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

DPC Case Reference: 03/SIU/2018

In the matter of Limerick City and 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

9th December 2021

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 provided Limerick City and County Council **("Council")** with the Draft Inquiry Report and the Final Inquiry Report.

1.2 The Council was provided with the Draft Decision on this inquiry on 1st November 2021 to give it a final opportunity to make submissions. I received submissions from the Council relating to the Draft Decision on 22nd November 2021. I have given consideration to these submissions in advance of arriving at a final Decision. This Decision is being provided to the Council pursuant to sections 116(1)(a) and 126(a) of the 2018 Act in order to give the Council notice of the Decision, the reasons for it, and the corrective powers that I have decided to exercise.

1.3 This Decision contains corrective powers under sections 115 and 127 of the Data Protection Act 2018 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. In this regard, the Council will be required to comply with these corrective powers and it is open to this office to serve an enforcement notice on the Council in accordance with section 133 of the Data Protection Act 2018.

2. Factual Background

2.1 Authorised Officers from the Special Investigations 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. On 15th 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 25th 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, using CCTV systems, Automated Number Plate Recognition, 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 Data Protection Act 2018 and/or the GDPR has been infringed and if so, whether corrective powers should be exercised.

2.4 The DPC received an acknowledgement of receipt of the notice from the Council on 15th June 2018.

2.5 On 25th 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 16th July 2018. A revised completed version of Questionnaire No. 1 was submitted to the DPC on 10th December 2018.

2.6 On 7th 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 Data Protection Act 2018. It explained that the Authorised Officers would meet with the Data Protection Officer before commencing site visits to the CCTV monitoring stations at [redacted]. It advised the Data Protection Officer that the Authorised Officers would first focus on the Smart CCTV Project and it signalled that there may be further phases which would deal with the replies to other questions in Questionnaire No. 1.

2.7 On 27th September 2018, the first inspection was carried out by the Authorised Officers at the monitoring centre in [redacted], Limerick. The Data Protection Officer, the Head of Digital Strategy and two representatives of the data processor, [redacted], were present.

2.8 The next inspection took place on 2nd October 2018. The first session of the morning involved an inspection by the Authorised Officers of the Traffic Management Centre at City Hall, Merchants Quay, Limerick. The Data Protection Officer and a member of the Council's Traffic Management unit were present at this inspection. The second session of the morning comprised of an inspection by the Authorised Officers of the monitoring centre at [redacted], Limerick. The Data Protection Officer and a representative of [redacted] were present at this inspection. The afternoon session involved an inspection by the Authorised Officers of CCTV cameras at Rathkeale and the monitoring hub at Rathkeale. The Data Protection Officer and the Head of Digital Strategy were present at this session.

2.9 Inspections of CCTV cameras were conducted by Authorised Officers on 4th October 2018 at the following towns: Castleconnell, Murroe, Cappamore, Caherconlish, Pallasgreen, Patrickswell, Adare, Croom, Kilmallock, Rathkeale, Newcastlewest and Abbeyfeale. On 10th December 2018, the final inspection by Authorised Officers took place at Askeaton and Foynes.

2.10 Over the course of the inspection dates, the Authorised Officers had a number of meetings with the Data Protection Officer and different officials from the Council and the data processor [redacted].

2.11 An investigation of Henry Street Garda Station was conducted as part of a separate inquiry conducted into An Garda Síochána. Some of the information gathered from this inquiry was relied upon by the Decision-Maker in the context of this Decision.

2.12 The Council submitted a number of other documents during the course of the inquiry including a copy of legal advice the Council obtained regarding 'Advices on the powers of local authorities in relation to CCTV' (this document was not sought or requested by the Authorised Officers but was voluntarily provided by the Council). On 8th February 2019, the Council submitted to the DPC an inventory detailing '*CCTV in Public Places*'. On 9th April 2019, the Council submitted a revised version of the CCTV inventory which gives an overall picture of the technologies the Council used for surveillance purposes. In summary the inventory shows that the Council deploys 401 CCTV cameras. The inventory lists:

- A total of 26 CCTV cameras feeding into the Traffic Management Centre at City Hall in Limerick City and County Council. At the time of the inspection phase of the inquiry these cameras also fed on a live basis into Henry Street Garda Station in Limerick.
- 13 CCTV cameras operate along a three kilometre bicycle and walkway route, this is referred to as the 'Smarter Travel' Walkway. At the time of the inspection phase of the

inquiry, these cameras also fed on a live basis into Henry Street Garda Station in Limerick.

- A total of 48 cameras that have been installed to date on the Smart CCTV Pilot Project across fourteen towns.
- The remaining 314 cameras are installed in various locations across Limerick City and County, including housing estates, traveller accommodation sites and public spaces.
- During the inspection phase of the inquiry, the inquiry team established that 128 of the 314 cameras fed directly into the [redacted] Monitoring Centre and were the subject of real time surveillance. 64 cameras fed directly into the [redacted] Monitoring Centre and were also subject to constant real time surveillance. Since the inspection phase, these two centres have now combined into one centre. Images from a total of 192 cameras are the subject of live full time surveillance in the new monitoring centre. If the feeds from the Smart CCTV Pilot Project are connected to the new [redacted] Monitoring Centre, the number of cameras under live full time surveillance is set to increase in the future.
- Separately, Limerick City and County Council has two drones in operation.
- By way of email on 21st June 2019 the Council confirmed that '*[t]here is a project in train to install CCTV in the vicinity of eight different halting sites. The overall purpose is to support the development of safer communities for the residents of the Sites. DPIA's are currently being finalised in respect of all locations.*'

2.13 The draft inquiry report was submitted to the Council's Data Protection Officer on 8th July 2019 and submissions were invited from the Council within twenty-eight days. On 6th August 2019, the Council sought an extension of time to make submissions. This request was granted and the deadline for receipt of submissions was extended to 20th September 2019.

2.14 The submissions from the Council were received by the DPC on 20th September 2019. Included in the submissions received, was a reference by the Council to section 49 of the Data Protection Act 2018 as a legal basis for processing. This was the first time this legal basis for processing was relied upon by the Council and the inquiry team sought further clarification on the Council's reliance on section 49. A reply was received from the Council on 30th October 2019 in respect of this point. The inquiry team decided to revise the draft inquiry report on foot of the submissions received from the Council.

2.15 The Authorised Officers completed a final Inquiry Report which they submitted to me as a Decision-Maker on 11th November 2019.

2.16 I am satisfied that the audit and inquiry were correctly conducted and that fair procedures were followed throughout including, but not limited to, notifications to the data controller and an opportunity for the data controller to comment on a draft inquiry report before it was submitted to me as Decision-Maker.

3. Legal regime pertaining to the inquiry and the Decision

3.1 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 is given further effect 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*'.

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

'*…to the processing of personal data by or on behalf of a controller*

where the processing is carried out—

(a) for the purposes of—

(i) the prevention, investigation, detection or prosecution of criminal

offences, including the safeguarding against, and the prevention of,

threats to public security, or

(ii) the execution of criminal penalties,

and

(b) by means that—

(i) are wholly or partly automated, or

(ii) where the personal data form part of, or are intended to form part of, a

relevant filing system, are not automated.'

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

'*(a) a competent authority that, whether alone or jointly with others,*

determines the purposes and means of the processing of personal data,

or

(b) where the purposes and means of the processing of personal data

are determined by the law of the European Union or otherwise by the

law of the State, a controller nominated—

(i) by that law, or

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

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

'(a) a public authority competent for the prevention, investigation,

detection or prosecution of criminal offences or the execution of criminal

penalties in the State, including the safeguarding against, and the

prevention of, threats to public security, or…'

3.5 The Council is a '*competent authority*' pursuant to this definition. It enjoys competence for the prevention, investigation, detection, and prosecution of certain offences under the Litter Pollution Act 1997. Furthermore, it enjoys a general competence regarding the prevention of crime, when performing its functions, under section 37(1) of the Garda Síochána Act 2005. Two criteria must be fulfilled for the LED, as incorporated by Part 5 of the 2018 Act, to apply to the processing of personal data. Firstly, the processing must be conducted by or on behalf of a '*controller*' as defined in section 69 of the 2018 Act. Secondly, pursuant to section 70 of the 2018 Act, the processing must be carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against, and the prevention of threats to public security, or the execution of criminal penalties.

3.6 The Council operates and is a controller of twenty-six CCTV cameras from City Hall. These cameras were set up by the Council for the purposes of traffic management (for example, taking actions to alleviate traffic congestion). Sometimes An Garda Síochána make use of the cameras for law enforcement purposes, but the primary purpose behind the cameras is for traffic management. Evidence of this can be garnered from the Council's '*CCTV Inventory*' dated 8th February 2019 where it states the purpose of the CCTV in the city centre is for '*Traffic Management*'. As the primary function of the cameras is for traffic management the GDPR is the applicable legal regime.

3.7 The LED is the applicable legal regime for the remainder of the CCTV cameras that form part of this inquiry. The Council has determined the means and purposes of these cameras. These cameras process personal data primarily for the purposes of prevention, investigation, detection or prosecution of criminal offences. This can be derived from the CCTV Inventory where the Council specifies the purposes as '*Law enforcement, Property protection, H&S*', "*[t]o ensure proper use of facility by public and prosecute any unauthorised dumping at site entrance when closed*" or "*Enforcement*" '. The submissions received by the inquiry team from the Council validated that these were the actual purposes of the CCTV cameras.

3.8 The LED is the applicable legal regime governing the Council's use of ANPR cameras. ANPR cameras are used by An Garda Síochána to search for a certain passage in CCTV footage. This footage is then used by An Garda Síochána for the investigation, detection

and prosecution of criminal offences. As the Council is the controller of the ANPR cameras and as the purposes fall under the LED, the LED is the applicable regime.

3.9 The LED is the applicable legal regime for the Council's use of drones. The Council is the controller of the drones and the drones are used to investigate, detect and prosecute crime. Images captured by the drones of natural persons illegally dumping waste can be used by the Council in a subsequent prosecution.

4. Data Controller

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

5. Personal Data

5.1 Article 3(1) of the LED defines '*personal data*' as '*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly*'. Article 4(1) of the GDPR mirrors this definition. Section 69 of the 2018 Act defines '*personal data*' under Irish law for the purposes of Part 5 of the Data Protection Act 2018 which implements the Law Enforcement Directive.[1]

5.2 I will now conduct a preliminary analysis to determine if the different surveillance technologies used by the Council process personal data.

A. Automatic Number Plate Recognition Technology

5.3 According to the Council's draft CCTV Policy 2019 ANPR processes personal data: '*It is accepted that ANPR data is 'personal data' within the meaning of the GDPR. A Vehicle Registration Number is not in itself 'personal data' however since local authorities can in most cases access data that links a person to the vehicle, for example the name of the registered keeper it is 'personal data' within the meaning of the GDPR.*'[2]

5.4 ANPR allows a particular car to be pinpointed in CCTV footage. It is then possible to identify a natural person, if the CCTV is sufficiently focused. Although ANPR results in the indirect identification of individuals, it nonetheless amounts to the processing of personal data. I therefore find the Council processes personal data in its use of ANPR.

B. CCTV Surveillance Systems

[1] Section 69 of the 2018 Act defines 'personal data' as:
'information relating to—
(a) an identified living individual, or
(b) a living individual who can be identified from the data, directly or indirectly, in particular by reference to—
(i) an identifier such as a name, an identification number, location data or an online identifier, or
(ii) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual'.

[2] Limerick City and County Council, Draft CCTV Policy (V O.12 09/12/2019) page 15 accessed on 10th August 2021.

5.5 The Council uses CCTV systems for different purposes. According to the Council, the CCTV cameras used for traffic management purposes do not process personal data. This is apparent from the Council's response to the ninth question of the Draft DPIA in respect of the Smart CCTV project:

> '*Do the images need to be able to identify individuals, or could the scheme use other images not capable of identifying individuals?*
>
> *Cameras used for Traffic Management are placed in locations, distances, zoom and angles that do not allow the capture of images that would be capable of identifying individuals.*'

5.6 This view, however, is at variance with the fact that the Garda Síochána, on occasion, make use of the footage on the traffic management CCTV cameras at City Hall, Limerick City for the purposes of investigating and prosecuting criminal offences. Moreover, in the DPIA for the Smart CCTV Project, the capabilities of many CCTV cameras employed are describing as having a '*[p]an, tilt and zoom function*.' Many cameras are also listed as having either a 180-degree or 360-degree panoramic view. It is clear from the advanced capabilities of the CCTV cameras used by the Council, that they are able to process personal data. I therefore find the Council processes personal data in its use of CCTV systems.

C. Drones

5.7 Drones are used by the Council for waste enforcement purposes. It was stated by the Council that it does not set out to use a drone to capture images of persons. However, the Council submitted that, in event an image of a person is caught in the act of dumping waste, this image will be used for the purpose of investigating the offence. I therefore find the Council processes personal data in its use of drones.

6. Analysis and findings

6.1 The Authorised Officers identified a total of 48 issues in the course of the inquiry. I have considered each in turn and I also considered the commonality of issues identified. Given that the Council is a controller in each and all of the issues identified, I will group my analysis and findings based on the commonality of issues arising.

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

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

a) CCTV Cameras

Inquiry Report Issue: 7, 10, 20, 32, 34, 36, 37, 40, 43

i) Section 38 of the Garda Síochána Act 2005 / S.I. No. 289/2006 - Garda Síochána (CCTV) Order 2006

6.3 Section 38 of the Garda Síochána Act 2005 **("2005 Act"**) and the secondary legislation made pursuant to it (**"2006 Order"**)[3], were frequently cited by the Council as the principal legal bases which governed their utilisation of CCTV systems in public places. The following authorisations were given by the Garda Commissioner to the Council to install CCTV pursuant to section 38(3)(c) of the 2005 Act:

- On 19th September 2006 the Garda Commissioner authorised the installation of five additional CCTV cameras to the existing CCTV system in [redacted]. There were one hundred and twenty-eight cameras feeding into [redacted] monitoring centre at the time of the inspection. These cameras captured views from Ballynanty, Thomondgate, St. Mary's Park and Kileely.
- On 5th March 2009 the Garda Commissioner authorised the installation and operation of CCTV at thirty-four locations in the Weston, Carew Park, Keyes Park and O'Malley Park areas of Limerick City. There were sixty four cameras feeding into [redacted]l monitoring centre at the time of the inspection. These cameras captured views from [redacted], Carew Park, Weston and Rathbane.
- On 11th December 2017 the Garda Commissioner authorised the installation and operation of forty-four CCTV cameras at fourteen locations in Castleconnell, Murroe, Cappamore, Caherconlish, Pallasgreen, Patrickswell, Adare, Croom, Kilmallock, Rathkeale, Newcastlewest, Abbeyfeale, Askeaton and Foynes. These cameras are linked to the Smart CCTV pilot project.

6.4 In respect of the CCTV cameras that were installed by the Council in public places, but which were not authorised by the Garda Commissioner at the time of the inquiry, the Council indicated its intention to seek such authorisation if the DPC determined the 2005 Act was an appropriate legal basis. For these reasons, it is necessary to consider whether section 38 of the 2005 Act, together with the 2006 Order, constitutes a valid lawful basis for the processing of personal data in public places via CCTV cameras.

6.5 Section 71(1) of the 2018 Act provides:

'*A controller shall, as respects personal data for which it is responsible, comply with the following provisions:*

(a) the data shall be processed lawfully and fairly…'

6.6 Section 71(2) further provides:

'*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…'

[3] S.I. No. 289/2006 - Garda Síochána (CCTV) Order 2006.

6.7 As was stated in *National Asset Management Agency v Commissioner for Environmental Information,* Irish legislation transposing an EU directive should be interpreted teleologically so as to achieve the purpose of the directive.[4] It follows that the 2018 Act should be interpreted alongside Article 8 of the LED which states:

'*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.'

6.8 Although the wording of Article 8(2) of the LED was not transposed directly into the 2018 Act, a teleological interpretation can be given to section 71(1)(a) of the 2018 Act so that it is read in light of Article 8(2). Henceforth in this section, when I refer to section 71(1)(a) of the 2018 Act this should have a coterminous meaning to Article 8(2) of the LED.

6.9 The requirement in section 71(1)(a) 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.

6.10 Recital 33 of the LED gives further guidance as to the form the Member State law being relied on as legal basis must take:

'*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.*'[5]

6.11 Recital 33 emphasises the importance of the legal basis relied upon for the purposes of processing data being clear, precise and its application foreseeable in accordance with the case-law of the European Court of Human Rights (**"ECtHR"**) and the Court of Justice of the European Union (**"CJEU"**).

[4] [2015] IESC 51 paragraph 10.

[5] Emphasis added.

I will accordingly summarise the case-law of the ECtHR and the CJEU on these concepts prior to making a finding on whether or not the 2005 Act and 2006 Order cumulatively provide a valid legal basis for the processing of personal data by way of CCTV cameras.

European Court of Human Rights

6.12 Article 8 of the European Convention of Human Rights provides:

'*1. Everyone has the right to respect for his private and family life, his home and his correspondence.*

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

6.13 The Court has held that interferences with a person's right to private life under Article 8(1) are only permissible, when such interferences are '*in accordance with the law*' and '*necessary in a democratic society*.'

6.14 One of the first cases to opine on the requirements of the phrase "*in accordance with the law*" under the Convention was *The Sunday Times v United Kingdom*.[6] The case concerned an alleged interference with the applicant's right to freedom of expression under Article 10 of the Convention. The Court considered the meaning of the wording of Article 10(2) that any interference with the applicant's right to freedom of expression should be "*prescribed by law*":

'*In the Court's opinion, the following are two of the requirements that flow from the expression* "*prescribed by law*" *. First, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a 'law' unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able—if need be with appropriate advice—to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail…*'[7]

6.15 Although, the words "*in accordance with the law*" as opposed to "*prescribed by law*" are used in Article 8(2), the Court held in *The Sunday Times* the expressions should be interpreted as similarly as possible.[8] Subsequent cases have given equivalent interpretations to the phrase "*in accordance with the law*" under Article 8(2).[9]

[6] (1979-80) 2 E.H.R.R. 245.
[7] Ibid paragraph 49.
[8] Ibid paragraph 48.
[9] See for example: *Huvig v France* (1990) 12 E.H.R.R. 528 paragraph 26 and *Fernández Martínez v Spain* (Application no. 56030/07*)* paragraph 117.

6.16 *De Tomasso v Italy* recently summarised the case-law regarding the meaning of the phrase "*in accordance with the law*" under the Convention:

'*The Court reiterates its settled case-law, according to which the expression "in accordance with law" not only requires that the impugned measure should have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the persons concerned and foreseeable as to its effects.*'[10]

6.17 A rationale for the interference being prescribed by legislation that is precise and foreseeable, is to ensure that the interferences with rights are not arbitrary.[11] If the legislation gives a broad discretion to an authority to allow interferences with a Convention right, it increases the likelihood the legislation has not been drafted with sufficient precision and that it does not provide protection against arbitrary interferences with rights.[12]

6.18 The level of precision required in a legislative measure depends '*on the content of the law in question, the field it is designed to cover and the number and status of those to whom it is addressed.*'[13] It was noted in *S v United Kingdom* that the application of the law should be '*be reasonably predictable, if necessary with the assistance of expert advice. But except perhaps in the simplest cases, this does not mean that the law has to codify the answers to every possible issue which may arise. It is enough that it lays down principles which are capable of being predictably applied to any situation*.'[14] Nonetheless, *Kopp v Switzerland* held that legal bases in respect of surveillance technologies should be '*particularly precise*', considering their invasiveness and the fact technology increases in sophistication over time.[15] Although, this point was expressed in cases regarding secret surveillance, the principle is equally applicable to other types of technology such as CCTV cameras with advanced capabilities such as ANPR, panoramic rotation and zoom facilities which are at issue in this case.

Court of Justice of the European Union

6.19 CJEU jurisprudence has also considered the requirements of clarity, precision and foreseeability in relation to laws which authorise the processing of personal data by state or public authorities. These requirements can be said to flow from the Charter of Fundamental Rights of the EU. Article 7 protects the right to one's '*private and family life, home and communications.*' Article 8 states:

---

[10] *De Tommaso v Italy* (2017) 65 E.H.R.R. 19 paragraph 106 citing *Khlyustov* (28975/05) at paragraph 68, 11 July 2013; *X* v *Latvia* (2014) 59 E.H.R.R. 3 at paragraph 58; *Centro Europa 7 Srl* v *Italy* (38433/09) at paragraph 140, 7 June 2012; *Rotaru v Romania* (28341/95) at paragraph 52, 4 May 2000; and *Maestri v Italy* (2004) 39 E.H.R.R. 38 at paragraph 30.)

[11] *S v United Kingdom* (2008) 48 E.H.R.R. 1169 paragraph 99 and *Demirtas v Turkey* (2019) 69 E.H.R.R. 27 paragraph 143.

[12] *Tommaso v Italy* (2017) 65 E.H.R.R. 19 paragraph 118.

[13] *De Tommaso v Italy* (2017) 65 E.H.R.R. 19 paragraph 108. See also *Peruzzo and Martens v Germany* (2013) 57 E.H.R.R. SE17 paragraph 35.

[14] *S v United Kingdom* (2008) 48 E.H.R.R. 1169 paragraph 99.

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

'*1. Everyone has the right to the protection of personal data concerning him or her.*

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.'

6.20 The requirement that a legal basis permitting the processing of personal data be clear, precise and its application foreseeable, can in particular be said to derive from Article 52 of the Charter which states:

'*1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.*'

6.21 In C-362/14 *Schrems v Data Protection Commissioner* (**"*Schrems I*"**) the CJEU invalidated the Safe Harbour Agreement, which had until that point, provided the legal framework for data transfers from the EU to the US. In the case the CJEU commented on the need for a law permitting interference with rights under Article 7 and 8 of the Charter to be clear and precise:

'*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*.'[16]

6.22 In Case C-175/20 *SIA 'SS' v Valsts ieņēmumu dienests*, Advocate General Bobek indicated that if a legal basis lacks the requisite detail required by Article 8(2) of the Charter of Fundamental Rights of the European Union, an alternative means of clarifying the scope of the personal data to be processed is at an administrative level:

'*In other words, the two regulatory layers, namely the legislative and the administrative, making up the eventual legal basis for the data processing, operate jointly. At least one of them must be sufficiently specific and tailored to a certain type or a certain amount of personal data requested. The more there is at the legislative, structural level for such data transfers, the less there needs to be in the individual administrative request. The legislative layer might even be so detailed and comprehensive that it will be completely self-contained and self-executing. By contrast, the more generic and vague the legislative level, the more detail, including a*

[16] Case C-362/14 *Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650 paragraph 91.

clear statement of purpose which will thus delimit the scope, there will need to be at the level of the individual administrative request.'[17]

Application

6.23 In considering the legal principles identified above, section 38 of the 2005 Act and the 2006 Order, in of themselves, fall short in meeting the requirements of clarity, precision and foreseeability as specified in Recital 33 of the LED. A number of reasons can be given for this view. First, there are no explicit safeguards in section 38 of the 2005 Act which require the Garda Commissioner to be satisfied that the installation of CCTV cameras in particular areas are proportionate and necessary in light of the purpose of preventing, investigating, detecting and prosecuting criminal offences (although I accept this may be implicit in the section). Second, section 38 of the 2005 Act does not require the Garda Commissioner to specify the exact number of CCTV cameras that are being authorised in a particular authorisation nor does it require the Garda Commissioner to specify the exact locations of the cameras.[18] Third, no legally binding guidelines have been issued pursuant to section 38 which could provide guidance to the Garda Commissioner as to how his discretion should be exercised in a particular case. I do acknowledge, however, there is a Code of Practice in place which gives the Garda Commissioner guidance on how to exercise his discretion, but this Code of Practice is not legally binding.[19]

6.24 *'SS' v Valsts ieņēmumu dienests* makes clear, however, if the primary legislation permitting processing of personal data is generic and broad, clarity can be achieved if an administrative request is sufficiently specific.[20]Applying this here, if a Garda authorisation made pursuant to section 38 of the 2005 Act is sufficiently clear, precise and foreseeable in its application, this authorisation cumulatively with the safeguards in place in section 38 of the 2005 Act and the 2006 Order can provide a valid legal basis for the processing of personal data by CCTV cameras.

6.25 I find the Garda Commissioner authorisation dated 11th December 2017 provides sufficient detail (when interpreted alongside section 38 of the 2005 Act and the 2006 Order) to constitute a valid legal basis under section 71(1)(a) of the 2018 Act for the 44 CCTV cameras authorised pursuant to it. The authorisation provides the exact GPS co-ordinates for where the cameras should be located and this helps to reduce the risk of arbitrary interferences with data subjects' rights in respect of that scheme.

---

[17] Case C 175/20 *SIA 'SS' v Valsts ieņēmumu dienests* Opinion of Advocate General Bobek delivered on 2 September 2021 paragraph 82.

[18] The Garda Commissioner is only required to specify the '*areas*' the cameras are warranted under section 38(2) of the 2005 Act.

[19] Code of Practice for Community Based CCTV Systems < http://www.justice.ie/en/JELR/PD_001_Code_of_Practice_2019.pdf/Files/PD_001_Code_of_Practice_2019.pdf> accessed on 22nd October 2021.

[20] It may ultimately be preferable that the primary legislation would set down more detailed limitations on the discretion of the Garda Commissioner to approve and more particular criteria applicant councils would need to meet and I note these matters fall for consideration in the published An Garda Síochána (Digital Recording) Bill 2021.

6.26 I find the Council has infringed section 71(1)(a) of the 2018 by installing up to 75 CCTV cameras in the fourteen towns. The authorisation dated 11th December 2017 is clear in only permitting 44 CCTV cameras to be installed. It is immaterial that the Council sought authorisation for more CCTV cameras in its application to the Garda Commissioner.

6.27 The authorisations dated 5th March 2009 and 19th September 2006 lack sufficient detail to constitute a valid legal basis (cumulatively with section 38 of the 2005 Act and the 2006 Order) under section 71(1)(a) of the 2018 Act for the processing of personal data by CCTV cameras. The authorisation dated 19th September 2006 contains no detail as to the number of CCTV cameras the Commissioner authorised or the exact locations where the Council is granted permission to install cameras. The authorisation dated 5th March 2009 does not give details of the exact number of CCTV cameras the Commissioner is giving the Council permission to install or the exact locations where the Council is permitted to install CCTV cameras. I do acknowledge the 2009 authorisation gives some detail of the locations where the CCTV cameras should be installed, but the Council's failure to specify the precise GPS co-ordinates for the locations or the exact number of cameras the Council is permitted to install in these locations leads to a lack of clarity, precision and foreseeability as to the authorisation's scope. It appears in this case the Council erected 64 cameras on foot of the 2009 authorisation which fed into [redacted] monitoring centre. However, the authorisation could be interpreted to empower the Council to install more cameras at these locations if the Council wished and this is indicative of a lack of clarity in the terms of the authorisation. The Council is under an obligation to demonstrate that personal data is being processed lawfully by virtue of section 71(10) of the 2018 Act. I accordingly find the authorisations of 5th March 2009 and 19th September 2006 do not provide valid legal bases for the CCTV cameras authorised pursuant to them under section 71(1)(a) of the 2018 Act.

Findings

6.28 ***I find that the Garda Commissioner authorisation dated 11th December 2017 together with section 38 of the 2005 Act and the 2006 Order provide a lawful basis under section 71(1)(a) of the 2018 Act for the 44 cameras listed in the authorisation. I find the same authorisation does not provide a lawful basis for any cameras the Council installed in the relevant towns in excess of this number.***

6.29 ***I find the authorisations dated 5th March 2009 and 19th September 2006 do not provide lawful bases for the processing of personal data by CCTV cameras installed pursuant to these authorisations and the Council has infringed section 71(1)(a) of the 2018 Act by using these CCTV cameras to process personal data.***

ii) Section 65 of the Local Government Act 2001 in conjunction with Section 37(1) of the Garda Síochána Act 2005

6.30 In submissions made to the inquiry team, the Council noted that prior to the audit taking place, it believed that section 65 of the Local Government Act 2001 taken in conjunction with section 37(1) of the Garda Síochána Act 2005 gave the Council a legal basis to operate CCTV in public places. It referenced these sections as a legal basis in relation to the fifty-seven CCTV cameras the Estate Management Unit installed in Banogue, Garryowen, Deebert (Kilmallock), Lee Estate, Lismakeera (Askeaton), Churchview (Askeaton), Old Cratloe Road, Altimira, Bruff Playground, The Banks (Kings Island), Cluain Dubh, Abbeycourt Estate Rathkeale, Lord Edward Street Development, Riverview Estate Kilmallock, Watergate, Clonlong, Kilmallock Road, Sharwood & Castleview Estates Newcastle West, Fr. Casey Close and Abbeyfeale. It also referred to these sections as a legal basis for the nine CCTV cameras it installed by the Housing and Halting Site Maintenance Section at the following traveller accommodation sites: Dublin Road Halting Site, Clondrinagh Halting Site, Rhebogue Halting Site, Rathkeale, Rathbane Depot and Clonlong. The sections were also cited as a legal basis for the processing of personal data at the 'Smarter Travel' Walkway, a three kilometre bicycle and walkway route along the Guinness Canal and Plassey Walkway.

6.31 Section 65 of the Local Government Act 2001 provides:

'*(1) A local authority may do anything ancillary, supplementary or incidental to or consequential on or necessary to give full effect to, or which will facilitate or is conducive to the performance of, a function conferred on it by this or any other enactment or which can advantageously be performed by the authority in conjunction with the performance of such a function.*

(2) The reference in subsection (1) to a function conferred on a local authority shall be read as including—

(a) all such functions as may at any material time stand conferred on the local authority by or under any enactment (including this Act and any other enactment whether enacted before or after this Act),

(b) the provision of offices, equipment or the doing of anything else which is necessary for or related to the general operation, organisation or administration of the authority.

(3) Every enactment relating to a function of a local authority shall be read and have effect in accordance with this section.'

6.32 Section 37(1) of the Garda Síochána Act 2005 provides:

'*A local authority shall, in performing its functions, have regard to the importance of taking steps to prevent crime, disorder and anti-social behaviour within its area of responsibility.*'

6.33 In principle, it is possible for two legislative provisions cumulatively to provide a valid legal basis for the processing of personal data. This is permissible where the objects of the two legal bases are not incompatible with each other.[21] It follows from this it is

[21] Opinion of the Court (Grand Chamber) of 26 July 2017 (ECLI:EU:C:2017:592) paragraphs 77-78.

possible for section 65 of the Local Government Act 2001 and section 37(1) of the Garda Síochána Act 2005 to cumulatively provide a legal basis for the processing of personal data. The objects or the procedures of the legal provisions can work in parallel with each other.

6.34 However, these legislative provisions do not form a valid legal basis for the processing of personal data, as they fail to meet the requirements of clarity, precision and foreseeability set out above. The fact that neither provision expressly empowers the Council to carry out surveillance in public places via CCTV systems makes the operation of this legal basis manifestly unclear. Furthermore, the provisions do not impose any safeguards or conditions on the use of CCTV technology in order to ensure the use of such is proportionate and necessary to the specified purposes.

Findings

6.35 ***I find section 65 of the Local Government Act and section 37(1) of the Garda Síochána Act 2005, in of themselves, are not an adequate legal basis for the processing of personal data as required by Article 8(2) of the LED.***

6.36 ***I find that the Council infringed Section 71(1)(a) of the 2018 Act by unlawfully installing and operating CCTV systems pursuant to these Acts.***

iii) Section 66 of the Local Government Act 2001

6.37 The Council relied on section 66 of the Local Government Act 2001 as an alternative legal basis for the CCTV cameras installed on the 'Smarter Travel' walkway and the various CCTV cameras installed by the Estate Management Unit and Housing and Halting Site Maintenance Section of the Council described above.

6.38 Section 66(3) of the Local Government Act 2001 (as amended) provides:

'*(a) Subject to this section, a local authority may take such measures, engage in such activities or do such things in accordance with law (including the incurring of expenditure) as it considers necessary or desirable to promote the interests of the local community.*

(b) For the purposes of this section a measure, activity or thing is deemed to promote the interests of the local community if it promotes, directly or indirectly —

(i) social inclusion or the social, environmental, recreational, cultural or community development, or

(ii) the general development including enterprise and economic development,

of the administrative area (or any part of it) of the local authority concerned or of the local community (or any group consisting of members of it).'

6.39 It is possible for CCTV to fall within the remit of section 66(3)(a) of the Local Government Act 2001, in that it could be argued '*to promote the interests of the local community*' by facilitating the prevention, investigation, detection and prosecution of

crime. However, the fact that such a purpose is not expressly included in section 66(3)(b) means that section 66 alone cannot be taken as a valid legal basis for the processing of personal data via CCTV.

6.40 The Council posited, in the materials it submitted, that section 66 of the Local Government Act 2001 should be interpreted alongside section 67 of same. Section 67 provides:

'*(1) In accordance with and subject to section 66 , a local authority may take such measures, engage in such activities or do such things (including the incurring of expenditure) as it considers necessary or desirable to promote the interests of the local community in relation to the matters indicated in subsection (2).*

(2) (a) The matters referred to in subsection (1) are—

…

(viii) the promotion of public safety.'

6.41 I accept that sections 66 and 67 empower the Council to take measures to promote the interests of the local community, which includes the promotion of public safety. These statutory provisions are broadly pitched and it is possible that they could provide a basis for the Council to install CCTV or other surveillance technologies to achieve this. Nonetheless, I am of the view that sections 66 and 67 are invalid legal bases to justify the processing of personal data by way of CCTV systems. The identification of express legislative authorisation is not necessarily sufficient to constitute a valid legal basis.[22] There is a need for this legal basis to be clear, precise and foreseeable. The broad and expansive nature of the powers conferred on the Council by the sub-sections, taken together with their failure to expressly empower the Council to install CCTV, or to even process personal data at all, means the provisions fail to meet the requirements of clarity, precision and foreseeability.

6.42 Furthermore, as stated above, Article 8(2) of the LED requires the Member State law relied upon as the legal basis, to specify '*the objectives of the processing, the **personal data** to be processed and the purposes of the processing*.'[23] Neither statutory provision gives guidance as to what locations the CCTV can be installed in, how many CCTV cameras can be installed and what safeguards are in place to ensure the processing of data is necessary and proportionate to the purpose of promoting public safety. It can be derived from the absence of such detail, that the statutory provision fails to specify what personal data can be processed and is thus incompatible with Article 8(2).

Findings

6.43 ***I find section 66 of the Local Government Act, in of itself, is not an adequate legal basis for the processing of personal data as required by Article 8(2) of the LED.***

[22] See Case C 201/14 *Bara v Presedintele Casei Nationale de Asigurari de Sanatate* (ECLI:EU:C:2015:638).
[23] Emphasis added.

6.44 ***I find that the Council infringed section 71(1)(a) of the 2018 Act by unlawfully installing and operating CCTV systems pursuant to this Act.***

iv) Section 34 of the Limerick City and County Council Cemeteries Bye-laws 2015

6.45 The Council has installed three CCTV cameras at Mt. St. Lawrence Cemetery. The purpose for installing the CCTV cameras was to investigate any breaches of the County Council Cemeteries Bye-laws 2015. The Council relies on the Bye-laws as a legal basis for its use of CCTV cameras.

6.46 The only reference to CCTV in the Bye-laws is in section 34. Section 34 provides:

'*The use of still, cine and television cameras shall not be used to photograph mourners or any part of a funeral cortege within the cemetery, without the prior consent of the Council and the immediate family. This however, does not preclude the Council from installing and maintaining Close Circuit Television (CCTV) for the purposes of security and public safety.*'

6.47 *Boddignton v British Transport Police*[24] is of relevance as it discusses the legal status of bye-laws. The case concerned a man who had been convicted for smoking on a railway carriage which was contrary to the bye-law 20 of the British Railways Board's Byelaws 1965 which were made pursuant to section 67 of the Transport Act 1962. Lord Irvine considered the legal status of bye-laws:

'*Subordinate legislation , or an administrative act, is sometimes said to be presumed lawful until it has been pronounced to be unlawful. This does not, however, entail that such legislation or act is valid until quashed prospectively. That would be a conclusion inconsistent with the authorities to which I have referred. In my judgment, the true effect of the presumption is that the legislation or act which is impugned is presumed to be good until pronounced to be unlawful, but is then recognised as never having had any legal effect at all. The burden in such a case is on the defendant to establish on a balance of probabilities that the subordinate legislation or the administrative act is invalid.*'[25]

6.48 In summary, Lord Irvine clarifies that there is a presumption that a bye-law is a valid law, until it is declared by a court to be unlawful. If this occurs, it will be recognised as never having any legal force. The presumption that bye-laws are good laws, can be reconciled with Recital 33 of the LED which states that the legal basis for processing personal data '*does not necessarily require a legislative act adopted by a parliament*'.

6.49 Although, a bye-law, *stricto sensu*, is capable of providing a valid legal basis for the processing of personal data by CCTV, the Limerick City and County Council Cemeteries Bye-laws 2015 fail to provide such a legal basis. The reason for this is that it fails to meet the requirements of clarity, precision and foreseeability. Section 34 of the Cemeteries Bye-laws are unclear in respect of providing a lawful basis for the processing of personal data, as they do not expressly empower the Council to install

[24] [1999] 2 AC 143.
[25] Ibid.

CCTV for the purposes of security and public safety. Stating there is no prohibition on the Council installing CCTV, is distinct from giving the Council a positive right to do so. Even if the Cemeteries Bye-Laws did equip the Council with a positive right to install CCTV cameras, the fact the discretion is not circumscribed by permitting the Council to only install CCTV where it is necessary and proportionate to do so, renders the application of the Bye-Laws unforeseeable.

Findings

6.50 ***I find section 34 of the Limerick City and County Council Cemeteries Bye-laws 2015, in of itself, is not an adequate legal basis for the processing of personal data as required by Article 8(2) of the LED.***

6.51 ***I find that the Council infringed Section 71(1)(a) of the 2018 Act by unlawfully installing and operating CCTV systems pursuant to this Act.***

v) Housing (Miscellaneous Provisions) Act 1997 and Housing (Miscellaneous Provisions) Act 2009

6.52 The Estate Management Unit of the Council deploy fifty-seven CCTV cameras within the following council estates and public areas: Banogue, Garryowen, Deebert (Kilmallock), Lee Estate, Lismakeera (Askeaton), Churchview (Askeaton), Old Cratloe Road, Altimira, Bruff Playground, The Banks (Kings Island), Cluain Dubh, Abbeycourt Estate Rathkeale, Lord Edward Street Development, Riverview Estate Kilmallock, Watergate, Clonlong, Kilmallock Road, Sharwood & Castleview Estates Newcastle West and Fr. Casey Close Abbeyfeale.

6.53 In addition, the Housing and Halting Site Maintenance section of the Council deploy at least nine CCTV cameras at the following traveller accommodation sites: Dublin Road Halting Site, Clondrinagh Halting Site, Rhebogue Halting Site, Rathkeale and Rathbane Depot.

6.54 According to the Council, the Housing and Halting Site Maintenance section of the Council is empowered with law enforcement functions under sections 3, 18 and 20 of the Housing (Miscellaneous) Provisions Act 1997 (**"1997 Act"**) and sections 7-18 of the Housing (Miscellaneous Provisions) Act 2014 (**"2014 Act")**. It cannot be said, however, that the 1997 Act and/or the 2014 Act provides a valid legal basis for the processing of personal data via CCTV systems. The 1997 Act does not provide for the '*personal data to be processed*' as required by Article 8(2) of the LED. In not expressly providing that the Council could use CCTV or in nominating safeguards and conditions for its use, the 1997 Act and the 2014 Act cannot be said to amount to a legal basis which is clear, precise and foreseeable as specified by Recital 33 of the LED.

Findings

6.55 ***I find the Housing (Miscellaneous Provisions) Act 1997 and Housing (Miscellaneous Provisions) Act 2009 are not an adequate legal basis for the processing of personal data as required by Article 8(2) of the LED.***

6.56 ***I find that the Council infringed Section 71(1)(a) of the 2018 Act by unlawfully installing and operating CCTV systems pursuant to these Acts.***

b) ANPR

Regime: LED

Inquiry Report Issue: 42

6.57 In its application to the Garda Commissioner under section 38(3)(c) of the 2005 Act in 2017, the Council sought authorisation for CCTV cameras with ANPR facilities to install in fourteen towns in Limerick as part of the Smart CCTV Pilot Project. The Garda Commissioner's authorisation dated 11th December 2017 did not explicitly authorise the installation of CCTV cameras with ANPR functions. The authorisation only granted permission to the Council to install CCTV cameras.

6.58 CCTV cameras with ANPR facilities can potentially allow the Council to track data subjects over long distances. This still image can then be used to pinpoint the date and time that the registration plate was captured, and the footage from the other CCTV cameras for the same time and date can then be searched to examine the movement of the vehicle concerned. Therefore, each time a vehicle passes one of these ANPR cameras – regardless of whether or not these motorists are suspected of any wrongdoing – a precise record of this activity by date and time is logged and retained. This can potentially allow the controller to track the data subject over a sustained distance where subsequent ANPR cameras are in place.

6.59 *Kopp v Switzerland* is an authority for the proposition that legal bases for surveillance technologies must be particularly precisely worded. As neither section 38 of the 2005 Act, the 2006 Order or the Garda Commissioner authorisation dated 11th December 2017 explicitly permit 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.

Findings

6.60 ***I find the Council has infringed section 71(1)(a) of the 2018 Act by processing personal data with ANPR technology without having a valid lawful basis to do so.***

c) Live Feed from CCTV Cameras provided to An Garda Síochána

i) 'Smarter Travel' Walkway

6.61 The Council had provided a live feed to An Garda Síochána from the CCTV cameras erected at the 'Smarter Travel' Walkway. These cameras were not authorised by the Garda Commissioner pursuant to section 38(3)(c) of the 2005 Act. The Council was therefore not legally mandated by section 38(7) to provide An Garda Síochána with access to the cameras. The Council has failed to demonstrate what the legal basis is

which permits the Council to allow An Garda Síochána to process personal data via these cameras.

Findings

6.62 ***I find the Council has infringed section 71(1)(a) of the 2018 Act by supplying An Garda Síochána with a live feed to the CCTV cameras at the 'Smarter Travel' Walkway without having a legal basis to do so.***

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

a) CCTV cameras

i) Traffic Management CCTV cameras

Regime: GDPR

Inquiry Issue: 1

6.63 Twenty-six CCTV cameras were set up by the Council in Limerick City for the purposes of traffic management (for example, taking actions to alleviate traffic congestion). From time to time, An Garda Síochána make use of the cameras for law enforcement purposes, but the primary purpose behind the cameras is traffic management. The cameras accordingly fall under the GDPR.

6.64 For processing of personal data to be lawful under the GDPR, the processing must fall under Article 6 of the GDPR. The Council relies on Article 6(1)(e) as a lawful basis for processing of personal data for traffic management purposes. The Council contends the 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.

6.65 Article 6 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'.

6.66 Recital 45 of the GDPR gives guidance on how Article 6(1)(e) should be interpreted. It provides:

'*It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so*'.

6.67 Recital 45 suggests a processing operation carried out by a local authority will not fall within the ambit of Article 6(1)(e), unless Member State law has determined the local authority will be given the responsibility for carrying out the specified task in the

public interest. In other words, it is insufficient for the local authority to simply claim a processing operation is carried out by it in the public interest to fall within the ambit of Article 6(1)(e). This task must be required by Member State law.

6.68 In the Draft Decision, I provisionally found that section 2 of the Local Authorities (Traffic Wardens Act 1975 gave local authorities the competence of carrying out traffic management functions which was a task carried out in the public interest. However, I noted, demonstrating the processing falls within Article 6(1)(e) is only the first step in demonstrating the processing has a lawful basis under Article 6 of the GDPR. 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 purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.'

6.69 In short, 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) 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:

1. 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);

2. The legal basis may contain specific provisions to adapt the rules of the GDPR (as listed above);

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

6.70 In the Draft Decision, I considered whether section 2 of the Local Authorities (Traffic Wardens) Act 1975 met the requirements of Article 6(3). I found the first criterion had been satisfied by virtue of the processing being covered by Article 6(1)(e). I also found the third criterion has been satisfied insofar as functions performed by traffic wardens

meet an objective of public interest. I then considered the requirements of the second criterion. I noted that it was not prescriptive; the use of the word '*may*' implies there is discretion regarding whether and how a legal basis adapts the rules of the GDPR.

6.71 Nevertheless, for a legal basis to be valid it must meet the requirements of clarity, precision and foreseeability as set out in Recital 41 of the GDPR irrespective of whether it seeks to adapt the application of the rules of the GDPR. Including 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 (as detailed above) 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 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 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 protection of their personal data.

6.72 As section 2 of the Local Authorities (Traffic Wardens) Act 1975 contains no such detail, I provisionally found it did not constitute a valid legal basis for the purposes of processing of personal data by CCTV cameras for traffic management purposes. The reasons I gave for this provisional finding included that by not providing that the persons employed by the authority can make use of CCTV cameras for traffic management purposes, the Act 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. The data subject would not be able to foresee from the wording of section 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, this led me to the provisional conclusion that the Act is an insufficiently clear, precise and foreseeable to constitute a valid legal basis for the processing of personal data via CCTV. I remain of this view after considering the submissions made by the Council in respect of the Draft Decision.

6.73 In its submissions in respect of the Draft Decision, the Council sought to rely on a number of statutory provisions as a legal basis for the processing of personal data by CCTV cameras for traffic management purposes. The Council relied upon sections 2 and 13 of the Roads Act 1993, section 38 of the Road Traffic Act 1994 and section 31 of the Road Traffic Act 2004 as providing a legal basis for the processing of personal data by CCTV cameras for traffic management purposes. The Council also referenced

its functions under the Road Traffic Act 1961 and in particular section 85, section 94 and section 95.

6.74 As was noted above, it is possible for different legislative provisions, taken cumulatively, to provide a valid legal basis for the processing of personal data.[26] Accordingly in considering whether the Council has a lawful basis for traffic management CCTV cameras, I will consider whether all the legislative provisions relied upon by the Council taken cumulatively provide a legal basis.

6.75 The Council submitted that a power to use CCTV for traffic management purposes can be derived from section 2 of the Roads Act 1993 and the Council in particular laid emphasis on section 2(d). 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'

6.76 The question is whether this is an adequate legal basis for the processing of personal data under Article 6 of the GDPR. It was accepted above that section 2 of the Local Authorities (Traffic Wardens) Act 1975 gives the Council traffic management competences. Therefore the Council meets the criteria under Article 6(1)(e).

6.77 The next issue is whether section 2 of the Roads Act 1993 meets the criteria to provide a valid legal basis for processing under Article 6(3) of the GDPR. Section 2 of the Roads Act 1993 is a general definition. It is possible that under this definition a traffic management CCTV camera could be said to be a '*thing forming part of the road*' which is '*necessary for the safety convenience or amenity of road users… or* [for the] *management of the road or for the protection of the environment*.' Section 2, however, is only a definition of a "*road*" and does not serve to empower the Council to conduct surveillance by CCTV cameras. In circumstances where this section does not explicitly provide the Council with the power to use CCTV cameras on public roads, it has failed to meet the requirements of clarity, precision and foreseeability in respect of any use of CCTV on public roads. The use of video surveillance of this nature has significant potential to impact on the rights and freedoms of data subjects. In those circumstances, it is imperative that any lawful basis under Article 6(1)(e) must include provisions that meet the standards of clarity, precision and foreseeability before such CCTV is deployed. In the circumstances, the inclusion of a provision authorising the use of CCTV is the minimum requirement necessary for the Council's operation of CCTV to be foreseeable for road users. The legislation should also bring clarity to the conditions under which the devices could be deployed. For this reason, I find section 2 of the Roads Act 1993, in of itself, does not provide a legal basis for the processing of personal data by CCTV cameras for traffic management purposes.

[26] Opinion of the Court (Grand Chamber) of 26 July 2017 (ECLI:EU:C:2017:592) paragraphs 77-78.

6.78 The Council also relied upon section 13 of the Roads Act 1993 as providing a legal basis for the processing of personal data by traffic management cameras (in particular sections 13(7) and 13(8) of the Act). 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.'

6.79 In similar vein to my finding that section 2 of the Roads Act 1993 does not provide a valid legal basis for the processing of personal data under Article 6(3) of the GDPR, I also find that section 13 of the Roads Act 1993 does not provide a valid legal basis. The failure of the section to explicitly state that the Council has the power to process personal data using CCTV cameras for traffic management purposes, and to bring clarity to the conditions under which the devices could be deployed, leads to a lack of foreseeability for natural persons as the Council's surveillance powers are.

6.80 Section 38 of the Road Traffic Act 1994 is another legal basis relied upon by the Council for the traffic management CCTV cameras. Section 38(1) states: '*A road authority may, in the interest of the safety and convenience of road users, provide such traffic calming measures as they consider desirable in respect of public roads in their charge.*'

6.81 Sections 38(7) and 38(9) of the Act provide definitions for "*traffic calming measures*":

(7) A traffic calming measure provided under this section shall be deemed to be a structure forming part of the public road concerned and necessary for the safety of road users.

[…]

(9)
[…]

" traffic calming measures " means measures which —
(a) enhance the provision of public bus services, including measures which restrict or control access to all or part of a public road by mechanically propelled vehicles (whether generally or of a particular class) for the purpose of enhancing public bus services, or

(b) restrict or control the speed or movement of, or which prevent, restrict or control access to a public road or roads by, mechanically propelled vehicles (whether generally or of a particular class) and measures which facilitate the safe use of public roads by different classes of traffic (including pedestrians and cyclists),
and includes for the purposes of the above the provision of traffic signs, road markings, bollards, posts, poles, chicanes, rumble areas, raised, lowered or modified road surfaces, ramps, speed cushions, speed tables or other similar works or devices, islands or central reservations, roundabouts, modified junctions, works to reduce or modify the width of the roadway and landscaping, planting or other similar works.

6.82 A CCTV camera installed for traffic management purposes could constitute a '*traffic calming measure*' under sections 38(7) and 38(9). However, the failure to explicitly specify that the Council is empowered to install CCTV cameras for the purposes of traffic management means the scope of the power lacks foreseeability for data subjects. Although the list is not exhaustive, it is noteworthy that cameras was not listed as one of the traffic management measures included in section 38(9) and further reinforces the lack of clarity provided in the legal basis for using CCTV cameras for traffic management purposes, including the conditions under which such CCTV cameras could be deployed even if authorised by the legislation

6.83 Section 31 was also identified by the Council as a potential basis for processing personal data by way of traffic management cameras. Section 31(1) states:
'*A road authority may, with the consent of the Commissioner or at his or her request, provide and maintain on public roads in their charge any equipment or structure which the authority consider desirable for the detection of offences under the Road Traffic Acts 1961 to 2004.*'

6.84 The primary purpose of the twenty-six cameras the Council monitored from the Traffic Management Centre was to promote good traffic management as opposed to detecting offences. I therefore I find section 31(1) does not provide a lawful basis for the use of traffic management CCTV cameras. In any event, even if traffic management cameras were within the scope of section 31(1), the provision would not provide a legal basis as it fails to explicitly specify that the Council can install CCTV cameras on public roads, and fails to bring clarity to the conditions under which the devices could be deployed.

6.85 I have also considered sections 85, 94 and 95 of the Road Traffic Act 1961 to establish whether these statutory provisions provided a legal basis for traffic management CCTV cameras. As none of these statutory provisions explicitly empower the Council to use CCTV cameras for traffic management purposes, I find these provisions do not amount to a valid legal basis to process personal data under Article 6(3) of the GDPR. Similarly, I have considered the general powers local authorities have under sections 65, 66 and 67 of the Local Government Act 2001. As these sections do not explicitly empower the Council to use CCTV cameras for traffic management purposes, and do not bring clarity to the conditions under which the devices could be deployed, I find these sections do not constitute a valid legal basis for the processing of personal data by CCTV cameras for traffic management purposes.

Findings

6.86 ***I find that the Council has infringed Article 5(1)(a) of the GDPR by not having a lawful basis to process personal data with CCTV 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) of the GDPR.***

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

Regime: GDPR

Inquiry Issue: 1, 9

6.87 An investigation was conducted in Henry Street Garda Station, Limerick, as part of a separate inquiry by the Data Protection Commission relating to An Garda Síochána. It transpired during the inquiry, that a live feed of the twenty-six traffic management cameras installed by the Council was made available via live feed to Henry Street Garda Station. It was ascertained that there were no restrictions on access to the live feed in the Garda Station and that approximately six-hundred Gardaí working there had access to the live feeds.

6.88 An application for authorisation to the Garda Commissioner was not made under section 38 of the 2005 Act in respect of the twenty-six 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.

Findings

6.89 ***I find the Council has infringed Article 5(1)(a) of the GDPR by sharing the personal data captured by the traffic management CCTV cameras with An Garda Síochána despite not having a valid legal basis to do so.***

C. Appropriate signage and general transparency

i) CCTV cameras used for traffic management purposes

Regime: GDPR

Inquiry Issue: 3

6.90 The personal data of members of the public is captured by CCTV cameras installed for traffic management purposes and which are monitored from City Hall. At the time the audit took place on 2nd October 2018, it was established there was no signage in place in Limerick City to inform data subjects that CCTV cameras were in operation for traffic management purposes.

6.91 Article 5 of the GDPR provides:

‘ *1. Personal data shall be:*

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency') '.

6.92 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…The information shall be provided in writing, or by other means, including, where appropriate, by electronic means.*'

6.93 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 the most important information should be included in the first layer. For CCTV surveillance, the first layer normally will be a sign which is placed at a reasonable distance from where the monitoring occurs.[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]

6.94 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*

[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.

[29] Ibid page 22.

[30] Ibid page 26.

[31] Ibid.

[32] Ibid.

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]

6.95 As Decision Maker, I visited the website of the controller (www.limerick.ie/council) to ascertain if the Council provided the required information to data subjects in respect of the Traffic Management CCTV. On the homepage, there was no immediately visible link to a policy with the requisite information in relation to the Council's use of CCTV for traffic management purposes. However, I did find a generic privacy statement for the Council which gave the Data Protection Officer's email address.[34] There was also a section on the privacy statement entitled 'Detailed Privacy Statements in relation to specific Council Services'. This, however, did not contain any reference to the Council's CCTV policy.

6.96 I then decided to conduct a Google Search using the search phrase 'limerick city and county council cctv policy'. I found a document entitled "*Limerick City and County Council CCTV Policy*".[35] The Policy had a watermark indicating it was in draft form. This policy provided an overarching view of the Council's use of CCTV cameras. In relation to public CCTV systems, it noted the primary purpose was to secure public order and safety in public places. It also listed a number of secondary purposes of public CCTV cameras such as improving emergency response rates, promoting better traffic management and obtaining statistical data in relation to pedestrian flows.[36]

6.97 The CCTV policy also stated '*[n]o CCTV cameras should be operated without appropriate signage being in place.*'[37] It required the signage to include the identity of the data controller, the contact details of the data controller and the specific purposes of the CCTV camera at each location.[38]

6.98 It is unclear when the CCTV policy was first published. The Policy itself notes an '*Initial draft*' was prepared on 15th October 2017. However, the policy was issued to Limerick JPC on 9th December 2019 and this was the last date the document was revised.

6.99 The CCTV policy fails to specify the precise locations of the CCTV cameras put in place by the Council. In the policy the following link was provided:' *https://safercommunities.limerick.ie/*'. On this website there is a link which gives the proposed locations for where the cameras for the Smart CCTV Pilot Project will be

[33] Ibid page 27.
[34] Privacy Statement for Limerick City and County Council < https://www.limerick.ie/council/services/your-council/privacy-statement-limerick-city-and-county-council> first accessed on 5th August 2021.
[35] <https://www.limerick.ie/sites/default/files/media/documents/2019-12/Draft%20CCTV%20Policy.pdf> first accessed on 5th August 2021.
[36] Ibid page 7.
[37] Ibid page 16.
[38] Ibid page 16.

installed in fourteen towns.[39] I could find no reference on this website or in the Council's draft CCTV policy as to the specific location of the twenty-six traffic management cameras.

6.100 I find the Council has infringed Article 13(1) of the GDPR by failing to provide 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[40] at the time the personal data was processed by the traffic management cameras. 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 has failed to do.

6.101 Article 13(3) of the GDPR also requires the Council to provide information to data subjects when it uses the personal data for a purpose other than which it was collected. As the Garda Síochána made use of the personal data for law enforcement purposes, there was an obligation on the controller to notify the data subject of this at the time the personal data was collected. In not including this secondary purpose in the signs, I find the Council has infringed Article 13(3) of the GDPR.

6.102 I note the Council has included some of the required information under Article 13 in respect of its CCTV operations in its draft CCTV policy. For example, the policy refers to its general data retention period, the data subject's access request rights, the contact details of the Data Protection Officer, the identity of the controller and the various purposes of the processing.

6.103 Nonetheless, this draft CCTV policy is of little value to the data subject in seeking to exercise his or her rights.

6.104 Firstly, where the Council has failed to erect signage in the vicinity of the cameras, the data subject lacks knowledge as to who is the actual controller of the cameras. Although the data subject could reasonably suspect the local authority could be the controller of CCTV cameras in a public place, the data subject could also reasonably believe that the cameras were controlled by some other public entity such as An Garda Síochána or another government body. In short, it would have been unclear to the data subject whether the cameras were covered by the Council's CCTV policy.

6.105 Secondly, the draft CCTV policy fails to specify (or signpost to the data subject via a link) that the Council was the controller of the traffic management CCTV cameras. Although, the policy states the Council will use CCTV cameras for traffic management purposes, it would not have been self-evident to the data subject, in the absence of signage, that the twenty six traffic management cameras were under the aegis of the Council's draft CCTV policy.

---

[39] < http://opendata.limerick.ie/cctv.html> accessed on 28th September 2021.

[40] 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.

6.106 I therefore find the Council, by failing to provide a reference to the CCTV policy via signs in the vicinity of the cameras and by failing to specify the precise locations of the traffic management cameras in its draft CCTV policy, has infringed its obligation to provide the required information under Article 13(1) and Article 13(2) of the GDPR.

6.107 In addition to the infringements of Article 13(1), Article 13(2) and Article 13(3) of the GDPR, in failing to provide the required information under Article 13 '*in a concise, transparent, intelligible and easily accessible form, using clear and plain language*', the Council has also infringed Article 12(1) of the GDPR. The Council has infringed Article 12(1) of the GDPR in failing to locate a comprehensive CCTV policy on an easily accessible section of the Council's website.

Findings

6.108 ***I find the Council has infringed Articles 13(1), 13(2) and 13(3) of the GDPR in failing to erect signage or by providing the necessary information in respect of the traffic management CCTV cameras on its website.***

6.109 ***I find the Council has infringed Article 12(1) of the GDPR by failing to provide this information in a transparent and easily accessible form.***

ii) CCTV Cameras at the 'Smarter Travel' Walkway, [redacted] Monitoring Centre, [redacted] Monitoring Centre

Regime: LED

Inquiry Issue: 8, 14, 23

6.110 The Council has installed thirteen CCTV cameras along a three kilometre bicycle and walkway route which is known as the 'Smarter Travel' Walkway. One-hundred and twenty-four CCTV cameras have been installed in various areas around Limerick which were subject to monitoring from [redacted] monitoring centre. Sixty-four cameras have also been installed around various areas in Limerick which were monitored by [redacted] monitoring centre. The audit established that no signage has been erected at the locations notifying data subjects of the existence of such cameras.

6.111 As the CCTV cameras were installed for the purposes of preventing, investigating, detecting or prosecuting criminal offences, the LED is the applicable legal regime to apply. Recital 26 sets out the application of the principle of transparency under the LED:

'*Any processing of personal data must be lawful, fair and transparent in relation to the natural persons concerned, and only processed for specific purposes laid down by law. This does not in itself prevent the law-enforcement authorities from carrying out activities such as covert investigations or video surveillance. Such activities can be done 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, as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the natural person concerned…'

6.112 Although, Recital 26 permits the use of covert surveillance, this is only permissible where it is necessary and proportionate in a democratic society and the legitimate interests of natural persons have been taken into consideration. As the Council has not demonstrated that covert surveillance is proportionate and necessary with respect to the purposes for which the CCTV cameras were installed, the Council is required to adhere to the general principle of transparency.

6.113 It follows the Council is bound by the requirements of section 90 of the 2018 Act, that the information listed therein is made available to the data subjects whose data is being processed by the CCTV cameras. In contrast to Article 13 of the GDPR which requires this information to be made available to the data subject at the time the personal data is being processed, section 90(1) of the 2018 Act (which transposes the requirements of the LED) provides this information can be made available within a reasonable period after the data is processed. Section 90(3) provides the required information can be communicated to the data subject by publishing it on the website of the controller. The duty on the Council to make available the information in section 90 in a concise, intelligible and easily accessible form using clear and plain language is also applicable.

6.114 On the Council's website (in the search I described above) I found no evidence of the Council providing the information required under section 90 of the 2018 Act, in respect of the CCTV cameras on the 'Smarter Travel' Walkway or the CCTV cameras which feed into [redacted] monitoring centres. It follows the Council has infringed the requirements of section 93(1) by failing to provide the requisite information in an accessible form. I do acknowledge, however, the Council's submission that there was previously signage erected in respect of the CCTV cameras that fed into [redacted] monitoring centres which was taken down by unknown persons. I also accept the Council's submission in relation to the Draft Decision that it did have some signage in place at the 'Smarter Travel' Walkway. However, the signs only provided the logo for the Council and a picture of a camera. It provided no information as to the purpose of the camera, nor did it provide information in respect of the contact details of the DPO. For these reasons, I find the Council has infringed sections 90 and 93 of the 2018 Act in relation to its processing of personal data by CCTV cameras at the 'Smarter Travel' Walkway.

Findings

6.115 ***I find the Council has failed to meet its obligations under section 90(1) of the 2018 Act, to provide the information specified in section 90(2) in a reasonable period after the personal data was processed by the aforementioned CCTV cameras.***

6.116 ***I find the Council has infringed section 93(1) of the 2018 Act by failing to provide the information specified in section 90(2) in an accessible manner.***

iii) Smart CCTV Pilot Project

Regime: LED

Inquiry Issue: 44

6.117 The Smart CCTV pilot project introduces Smart CCTV and ANPR in the following fourteen towns in County Limerick: Castleconnell, Murroe, Cappamore, Caherconlish, Pallasgreen, Patrickswell, Adare, Croom, Kilmallock, Rathkeale, Newcastlewest, Abbeyfeale, Askeaton and Foynes. At the time of the inquiry, it was intended that these cameras would be monitored continuously on a real time basis from [redacted] monitoring centre. However, when the inquiry was conducted, monitoring via these cameras had yet to commence from [redacted] monitoring centre and in some towns there remained CCTV cameras to be erected.

6.118 In respect of each pole where a CCTV camera was erected, there was detailed signage notifying data subjects about the nature of the processing. It is important, however, that this signage should be supplemented by giving also details of the information required by section 90 on the Council's website.

Findings

6.119 ***I find the Council has not infringed section 90(1) of the 2018 Act as there is detailed signage in place in respect of the Smart CCTV cameras.***

iv) Drones

Regime: LED

Inquiry Issue: 48

6.120 It was established that the Council used drones on a number of occasions for the purposes of tackling waste and pollution. These drones processed personal data. Despite this, the Council made no efforts to provide the information required by section 90 of the 2018 Act at the time the personal data was processed by the drones, or after the processing occurred. This information could have been supplied on the Council's website.

Findings

6.121 ***I find the Council has infringed section 90 of the 2018 Act by failing to provide the information required by section 90 in respect of its processing of personal data using drones.***

D. Joint controller agreement

i) Traffic Management CCTV cameras

Regime: GDPR

6.122 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*'.

6.123 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.*'

6.124 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 Henry Street 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 monitoring 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.[41]

6.125 The 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*.'[42]

6.126 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*.'[43]

6.127 Applying these definitions, 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

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

6.128 ***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.***

ii) CCTV Cameras at 'Smarter Travel' Walkway

Regime: LED

Inquiry Issue: 7

6.129 There are thirteen cameras at the 'Smarter Travel' Walkway. No authorisation has been sought by the Council to install the CCTV from the Garda Commissioner under the 2005 Act. However, the Gardaí have a live feed of the walkway of the CCTV cameras in Henry Street Garda Station.

6.130 This arrangement should be covered by a joint controller agreement. The EDPB Guidelines state '*[d]etermining the purposes and the means amounts to deciding respectively the "why" and the "how" of the processing…A natural or legal person who exerts such influence over the processing of personal data, thereby participates in the determination of the purposes and means of that processing in accordance with the definition in Article 4(7) GDPR*'.[44]

6.131 The Council noted in its submission in response to the draft inquiry report that: '*Extensive public and stakeholder consultation was undertaken as part of the Planning process for this Smarter Travel Route. An Garda Síochána was heavily involved in the consultation.*' From the Council's submission it can be inferred that An Garda Síochána exercised a material influence over the decision to install CCTV cameras on the walkway. In this respect, it could be said the Council and An Garda Síochána exercised a '*common decision*' to install the CCTV on the walkway. It appears An Garda Síochána and the Council jointly determined the purpose of the CCTV, namely that it would be used to deter anti-social behaviour and crime on the walkway.

6.132 Although, there is no direct evidence of An Garda Síochána determining the means used, this can be inferred from the context, particularly where the Gardaí has access to the cameras via video feed.[45] The EDPB Guidelines state that the phrase determining the '*means*' of processing should be given a broad interpretation[46] and this gives further credence to the view the processing should be covered by a joint controller relationship.

6.133 Even if the live feed of the CCTV cameras to Henry Street Garda Station was discontinued, this does not negate the need for a joint controller agreement to be in

[44] Ibid page 13.

[45] The EDPB Guidelines emphasise the importance of conducting a factual rather than a formal analysis to discern whether there is a joint controller relationship. It is permissible to derive the existence of a joint controller relationship from the surrounding facts (ibid page 10).

[46] The EDPB Guidelines provide that determining the '*essential means*' of processing is a pre-requisite for an entity to be classified as a controller. Examples of '*essential means*' include the '*type of personal data which are processed ("which data shall be processed?"), the duration of the processing("for how long shall they be processed?"), the categories of recipients ("who shall have access to them?") and the categories of data subjects ("whose personal data are being processed?" '*(Ibid pages 13-14).

place. The *Jehovah's Witnesses* case[47] makes clear that it is not necessary for both controllers to have access to the personal data for a joint controller relationship to exist. Although the Jehovah's Witnesses Community was found not to collect personal data, the fact that the Community co-ordinated, encouraged and organised the collection of personal data in door-to-door preaching was sufficient for it to be a controller.

6.134 Section 79(1) of the 2018 Act provides:

'*Where 2 or more controllers jointly determine the purposes and means of the processing of personal data (in this Part referred to as "joint controllers"), they shall determine their respective responsibilities for compliance with this Part in a transparent manner by means of an agreement in writing between them*…'.

6.135 Section 79(2) requires the joint controller agreement to include a determination of the respective responsibilities of joint controllers with regard to the exercise of data subjects of their rights and with regard to providing information specified in section 90(2) of the 2018 Act. It is permitted for a single point of contact to be designated.

Findings

6.136 ***I find An Garda Síochána and the Council are joint controllers of the CCTV cameras at the 'Smarter Travel' Walkway. I find the Council has infringed section 79(1) of the 2018 Act by failing to have a joint controller agreement in place governing this surveillance.***

iii) CCTV cameras monitored via [redacted] monitoring centres

Regime: LED

Inquiry Issue: 10, 20

6.137 The Garda Commissioner has given authorisation pursuant to section 38(3)(c) of the 2005 Act for a number of CCTV cameras to be operated from [redacted] monitoring centres. The inquiry team wrote to An Garda Síochána in an attempt to clarify what CCTV cameras were authorised by the Garda Commissioner on 19th September 2006 for [redacted] monitoring centre. By reply dated 17th May 2019, An Garda Síochána stated that although the authorisation was not specific in terms of the number of CCTV cameras authorised, it appears authorisation was given in respect of five cameras. On 5th March 2009, the Garda Commissioner granted authorisation for CCTV at thirty-four locations in Weston, Carew Park, Keyes Park and O'Malley Park areas of Limerick City. These cameras were to be monitored from [redacted] monitoring centre.

6.138 Insofar as CCTV cameras have been authorised by the Garda Commissioner pursuant to section 38 of the 2005 Act, processing falls within a joint controller relationship and a joint controller agreement is required.

[47] *Jehovah's Witnesses case* (C-25/17) Judgment of the Court (Grand Chamber) delivered on 10 July 2018 ECLI:EU:C:2018:551 paragraph 23.

6.139 Article 3(8) of the LED defines 'controller' as meaning '*the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*'.

6.140 Section 38 designates both An Garda Síochána and the Council as controllers. Section 38(7) provides that Gardaí shall have access to the CCTV for the purpose of '*controlling the operation of the CCTV on behalf of the Garda Commissioner*'. Thus, the Act assigns An Garda Síochána as controller of this processing. The 2006 Order provides that applications for authorisations under section 38(3)(c) must include an undertaking '*by the local authority concerned that it will act as a data controller in respect of the CCTV*'.[48] Thus, the legislation provides that the Council must also undertake the role of controller.

6.141 Section 79 of the 2018 Act requires joint controllers to have an agreement in writing unless those responsibilities are determined by EU law or Member State law. Although the 2006 Order and section 38 of the 2005 Act give some details on the operation of the CCTV arrangement,[49] it does not provide for procedures on the respective responsibilities of the controllers to allow data subjects to exercise their rights under section 90 of the 2018 Act. A joint controller agreement governing this relationship is thus necessary.

6.142 Regarding the CCTV cameras which the Council has installed unilaterally and which are not covered by an authorisation from the Garda Commissioner, a joint controller agreement is not necessary as An Garda Síochána did not determine the purposes and means of the processing.

Findings

6.143 ***I find the Council has infringed section 79(1) of the 2018 Act by failing to implement an agreement in writing with An Garda Síochána in respect of the CCTV cameras authorised.***

iv) Miscellaneous CCTV cameras

Regime: LED

Inquiry Issue: 32, 33, 36, 37

6.144 In addition to the CCTV cameras described above, the Council has installed CCTV cameras in other parts of Limerick for the purposes of combatting crime and anti-social behaviour. These cameras include:

(1) Fifty-seven Cameras installed in following council estates and public areas: Banogue, Garryowen, Deebert (Kilmallock), Lee Estate, Lismakeera (Askeaton), Churchview (Askeaton), Old Cratloe Road, Altimira, Bruff Playground, The Banks

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

(Kings Island), Cluain Dubh, Abbeycourt Estate Rathkeale, Lord Edward Street Development, Riverview Estate Kilmallock, Watergate, Clonlong, Kilmallock Road, Sharwood & Castleview Estates Newcastle West and Fr. Casey Close Abbeyfeale.

(2) At least nine CCTV cameras at the following traveller accommodation sites: Dublin Road Halting Site, Clondrinagh Halting Site, Rhebogue Halting Site, Rathkeale and Rathbane Depot.

(3) Eleven CCTV cameras installed by the Estate Management Unit at Lord Edward Street.

(4) Three CCTV cameras at Mt. St. Lawrence Cemetery.

6.145 As these CCTV cameras were not authorised pursuant to section 38 of the 2005 Act and as it appears the Council has unilaterally determined the means and purposes of processing there is no requirement under section 79 of the 2018 Act for the Council to have a joint controller agreement with An Garda Síochána for these cameras.

Findings

6.146 ***I find section 79 of the 2018 Act was not infringed in respect of the aforementioned cameras as the Council unilaterally determined the means and purposes of processing.***

v) Smart CCTV Pilot Project

Inquiry Issue: 39, 42

6.147 As part of the Smart CCTV project, CCTV and ANPR cameras will be introduced in the following fourteen towns in County Limerick: Castleconnell, Murroe, Caherconlish, Pallasgreen, Patrickswell, Adare, Croom, Kilmallock, Rathkeale, Newcastlewest, Abbeyfeale, Askeaton and Foynes. On 11th December 2017, the Garda Commissioner authorised the installation of forty-four CCTV cameras at fourteen locations in these towns. The Council, however, intends to erect seventy-five cameras on foot of this authorisation at the fourteen locations. The Council's justification for this, was that in its application for authorisation pursuant to section 38 of the 2005 Act it sought to implement seventy-five cameras in forty-four locations in fourteen towns. Following the inquiry, the Council has re-submitted its application to the Garda Commissioner requesting express authorisation for these additional cameras.

6.148 As discussed above, where CCTV cameras are authorised by the Garda Commissioner pursuant to section 38 of the 2005 Act, a joint controller agreement is required under section 79 of the 2018 Act. The reason for this is that the 2006 Order and section 38 of the 2005 Act together designate the Council and An Garda Síochána as controllers of the CCTV. Moreover, if the Council obtains authorisation for the additional cameras which are currently not authorised, a joint controller agreement will also be required in respect of these cameras. I therefore find the Council has infringed section 79(1) of the 2018 Act by failing to have an agreement in writing in place with

An Garda Síochána detailing their respective responsibilities and obligations as joint controllers under the 2018 Act.

Findings

6.149 ***I find the Council has infringed section 79(1) of the 2018 Act by failing to have a joint controller agreement in place with An Garda Síochána determining their respective obligations towards data subjects under the 2018 Act.***

vi) Amalgamation of CCTV Operations to [redacted] Monitoring Centre

Regime: LED

Inquiry Issue: 47

6.150 It was established during the audit that the Council intended to move a considerable volume of its data processing operations to a new monitoring centre at [redacted]. The construction works for this building were underway at the time the inquiry took place. It was envisaged that the processing operations at the old [redacted] monitoring centre along with the processing operations in [redacted] monitoring centre would be amalgamated in the new monitoring centre. The Smart CCTV project would also be subject to real time continuous monitoring from this new centre.

6.151 As the processing had not commenced at the new centre at the time the inquiry finished, I cannot make findings with respect to the Council's compliance with section 79 of the 2018 Act. Nevertheless, if the Council seeks to process data from this new centre in the future, the requirements in respect of joint controllerships are equally applicable with respect to the processing operations at the new centre.

E. Processing arrangements

Regime: LED

Inquiry Issue: 10, 16, 25.

i) Lack of processing agreement and guarantee of appropriate technical and organisational measures

6.152 Section 69 of the 2018 Act defines a "*processor*" as meaning '*an individual who, or a legal person , public authority, agency or other body that, processes personal data on behalf of a controller, but does not include an employee of a controller who processes such data in the course of his or her employment*.'

6.153 The EDPB Guidelines note:

'Two basic conditions for qualifying as processor are:

a) being *a separate entity* in relation to the controller and

b) processing personal data *on the controller's behalf*.'[50]

[50] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Version 1.0 Adopted on 02 September 2020) page 4.

6.154 [redacted] is an independent entity from the Council. [redacted] also processes personal data on the Council's behalf. Section 69 of the 2018 Act which transposed the LED into Irish law defines "*processing*" as meaning '*an operation or a set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, including—(a) the collection, recording, organisation, structuring or storing of the data, (b) the adaptation or alteration of the data, (c) the retrieval, consultation or use of the data, (d) the disclosure of the data by their transmission, dissemination or otherwise making the data available, (e) the alignment or combination of the data, or (f) the restriction, erasure or destruction of the data…*' The activity carried out by [redacted] at [redacted] monitoring centres amounts to "*processing*" under this definition. For example, [redacted] collects and stores the personal data captured by the CCTV cameras at the monitoring centres. [redacted] did not determine the purposes of the processing. It is also clear that [redacted] processes the personal data on behalf of the Council. Therefore [redacted] falls within the definition of a "*processor*" under section 69 of the 2018 Act.

6.155 Section 80 of the 2018 Act sets out the safeguards the controller must adhere to when utilising the services of the processor. Section 80(1)(b) requires controllers to only use processors providing '*sufficient guarantees to implement appropriate technical and organisational measures*' so as to ensure compliance with Part 5 of the 2018 Act.

6.156 Section 80(1)(a) requires that such processing arrangements shall be governed by '*a contract in writing between the controller and the processor*'. Section 80(2) provides:

'*A contract entered into between a controller and a processor in accordance with subsection (1)(a) shall—*

(a) specify the subject matter, duration, nature and purpose of the processing to be carried out thereunder,

(b) specify the type of personal data to be processed thereunder and the categories of data subjects to whom the personal data relate,

(c) specify the obligations and rights of the controller in relation to the processing…'

6.157 Section 80(2)(d) provides the contract should set out that the processor shall:

'*(i) act only on instructions from the controller in relation to the processing, except in so far as the law of the European Union or the law of the State requires the processor to act otherwise,*

(ii) procure the services of another processor (in this section referred to as a "secondary processor") in relation to the processing only where authorised to do so in advance and in writing by the controller, which authorisation may be specific or general in nature,

(iii) ensure that any person authorised to process the personal data has undertaken to maintain the confidentiality of the personal data or is under an appropriate statutory obligation to do so,

(iv) assist the controller in ensuring compliance with this Part in so far as it relates to the exercise by a data subject of his or her rights,

(v) erase or return to the controller, at the election of the controller, all personal data upon completion of the processing services carried out by the processor on behalf of the controller and erase any copy of the data, unless the processor is required by the law of the European Union or the law of the State to retain the data, and

(vi) make available to the controller all information necessary to demonstrate compliance by the processor with this section.'

6.158 I acknowledge the Council has a data processing agreement in place with [redacted]. However, the processing agreement does not contain all of the information required by section 80(2) of the 2018 Act. The contract does not specify in detail the nature of the processing in contravention of section 80(2)(a) of the 2018 Act. For example, it does not state whether the monitoring is real time and continuous. The contract does not contain any reference to information required to be included by section 80(2)(d)(i), 80(2)(d)(ii), 80(2)(d)(iv) and section 80(2)(d)(vi). The contract has not been updated to reflect the coming into effect of the GDPR and the 2018 Act (the Data Protection Act 1988 and the Data Protection Act 2003 are referred to instead).

6.159 The lack of detail in the processing contract generates considerable uncertainty as to the operation of the arrangement. The Council's failure to set out in detail the information required by section 80(2), led to a scenario where data subjects' rights were put at risk and personal data was unlawfully processed. [redacted]. In these scenarios, the operators unlawfully processed personal data by monitoring private dwellings. Furthermore, although the CCTV cameras were installed for the purposes of countering anti-social behaviour and crime, it is by no means apparent that the system's function extended to assisting the investigation of motor tax offences. If the processing agreement was more specific as to what the purposes of the surveillance were, as required by section 80(2)(a) of the 2018 Act, this unlawful processing could have been avoided.

6.160 Section 80(1)(b) requires controllers to only use processors providing '*sufficient guarantees to implement appropriate technical and organisational measures*' so as to ensure compliance with Part 5 of the 2018 Act. The EDPB has given examples of

documentation which could fulfil this guarantee such as a '*privacy policy, terms of service, record of processing activities, records management policy, information security policy, reports of external audits, recognised international certifications, like ISO 27000 series*.'[51] The Council gave no evidence that it received such guarantees from the processor and has failed to demonstrate compliance with section 80(1)(b) of the 2018 Act.

Findings

6.161 ***I find the Council has infringed section 80(1)(a) of the 2018 Act by not having an agreement in writing which set out all the required matters referred to in section 80(2).***

6.162 ***I find the Council has infringed section 80(1)(b) of the 2018 Act by failing to receive sufficient guarantees from the controller to implement appropriate technical and organisational measures as required by the 2018 Act.***

ii) Appointment of a sub-processor

Regime: LED

Inquiry Issue: 31

6.163 Article 22(2) of the LED provides:

'*Member States shall provide for the processor not to engage another processor without prior specific or general written authorisation by the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes*.'

6.164 Article 22(2) of the LED has been indirectly transposed into Irish law in section 80 of the 2018 Act. In effect, section 80(2)(d)(ii) of the 2018 Act prohibits a processor engaging another processor without first having received specific or general written authorisation of the controller, by requiring such a clause to be inserted into the processing agreement.

6.165 Section 80(2)(d)(ii) provides a contract entered into between a controller and a processor shall provide that the processor shall only procure the services of another processor (a "*secondary processor*") '*in relation to the processing only, where authorised to do so in advance and in writing by the controller, which authorisation may be specific or general in nature.*'

6.166 I find the Council has infringed section 80(1)(a) by not having such a clause in its contract with the processor. I find the Council has infringed section 80 of the 2018 Act when the processor [redacted] engaged the sub-processor Wired Up without specific or general written authorisation being given by the controller. Wired Up in conducting maintenance work on the CCTV systems processes personal data as defined by section

[51] EDPB Guidelines, Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 1.0 (Adopted on 02 September 2020) 30.

69 of the 2018 Act. Section 69 defines "*processing*" as '*an operation or a set of operations that is performed on personal data or on sets of personal data, whether or not by automated means*…' Section 69 then goes on to list examples of operations which can be performed on personal data using the phrase '*including*'. The list of operations is not exhaustive and for this reason conducting maintenance on CCTV systems is sufficient to amount to processing of personal data as it is an '*operation*' performed on such. I find the controller has failed to demonstrate compliance with section 80 of the 2018 Act.

6.167 I welcome the submission made by the Council in response to the Draft Decision which indicated a contract is now in place with [redacted], which places an obligation on [redacted] not to appoint another processor without the prior written consent of the Council. However, as this clause was not in place at the time the inquiry was conducted I find the Council has infringed section 80(1) of the 2018 Act.

Findings

6.168 ***I find the Council has infringed section 80(1) of the 2018 Act by not having a contract in writing with the processor which sets out the conditions when the processor can engage another processor in accordance with section 80(2)(d).***

F. Excessive Data Collection/ Data Protection Impact Assessment

Regime: LED

Inquiry Issue: 13, 15, 20, 21, 41, 43

i) CCTV Surveillance via [redacted] monitoring centres

6.169 I find section 84(1) of the 2018 Act has been infringed by not carrying out a DPIA in respect of both monitoring centres and by not considering the risks that the surveillance poses to the freedoms and rights of individuals and any measures that could have been taken to mitigate such.

6.170 I find the system in place infringes section 71(1)(c) of the 2018 Act as it collects an excessive amount of personal data. It is impermissible to use the CCTV system to monitor private dwellings. For example, at St. Mary's Park, Limerick, a CCTV camera provides a full view of all activity in a small U-shaped housing estate. Once a resident of any of those houses opens their front door their activities are captured by a CCTV camera and they can be monitored in real-time at the monitoring centre. 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.

6.171 The fact that the monitoring from the CCTV systems at [redacted] monitoring centres is continuous and involves real-time monitoring also poses a high a risk to data subjects. Live monitoring takes place twenty-four hours a day and three-hundred and sixty five days a year at both of these centres. The Council has an onus of

accountability to ensure such surveillance is proportionate. On the spectrum of surveillance that could have been considered, continuous real time monitoring falls into a category which is particularly oppressive. Other solutions that should have been considered in the DPIA could have included installing CCTV cameras, but only accessing them on a retrospective basis where the need arises, or only having real-time monitoring at certain intervals where there is considerable evidence that higher levels of anti-social behaviour or crime are inclined to take place. Ultimately, the onus is on the Council to demonstrate that the system used is not excessive and proportionate in accordance with section 71(1)(c) of the 2018 Act and the Council has failed to satisfy this here.

6.172 The Council has also failed to implement appropriate safeguards to protect data subjects' rights as required by section 76(1). The inquiry established that operators in [redacted] monitoring centres were able to manually control the CCTV cameras and sometimes used this facility to monitor private dwellings. A safeguard to prevent this from happening could be to prohibit manual control of the CCTV cameras by operators of the centre. The referenced guidance note gives details on how this could be achieved.[52] For CCTV systems, it is proportionate for the data controller to implement a data protection policy governing the use of the system as required by section 75(3) of the 2018 Act. The controller and processor have also failed in their duty under section 72(2) to take:

'*all reasonable steps to ensure that—(a) persons employed by the controller or the processor, as the case may be, and (b) other persons at the place of work concerned, are aware of and comply with the relevant technical or organisational measures…*'.

6.173 Abiding by these provisions could have helped to prevent unlawful access to personal data that has occurred at the [redacted] monitoring centres. Although, the processing operations carried out at [redacted] monitoring centres, have been amalgamated at a new purpose built centre in [redacted], the above considerations are also relevant to the new centre.

6.174 In arriving at the findings, I have given regard to the Council's submissions in respect of the Draft Decision. I accept that the installation of the CCTV cameras was motivated by the desire to combat crime in the area.

Findings

6.175 ***I find the Council has infringed section 84 of the 2018 Act by failing to carry out a DPIA in advance of beginning surveillance operations using CCTV cameras at [redacted] monitoring centres.***

6.176 ***I find the Council has failed to demonstrate that the continuous real time monitoring operations that were conducted in [redacted] monitoring***

[52] <https://www.bsia.co.uk/zappfiles/bsia-front/pdfs/197-cctv-privacy-marking-02%20(2).pdf> accessed on 29th September 2021.

centres are not excessive and are necessary. Accordingly I find the Council has infringed section 71(1)(c) of the 2018 Act.

6.177 ***I find the Council has infringed section 76(1) of the 2018 Act by failing to implement appropriate technical and organisational measures to prevent private dwellings being monitored prior to operating CCTV cameras.***

6.178 ***I find the Council has infringed section 72(2) of the 2018 Act by failing to have an appropriate procedure and training measures in place to inform staff on the requirements of the GDPR and the 2018 Act.***

ii) Smart CCTV Pilot Project

6.179 The inquiry team was informed that the Council proposes to connect the CCTV hubs from all fourteen towns to the new purpose built monitoring centre at [redacted] for monitoring by trained CCTV operators in real-time on a continuous basis. The existing surveillance operations at [redacted] monitoring centres would be transferred to this new centre. Other isolated CCTV projects such as the CCTV cameras at Lord Edward Street Development would also be monitored from this centre. The same concerns stated above with the [redacted] monitoring centres apply with equal force to the intended operations to be carried out at this new monitoring centre. At the time of writing on the inquiry report, the DPIA remained in 'Draft' form.

6.180 Nonetheless, for the purpose of completeness, it is worthwhile making a number of observations on the draft DPIA. The questions on the draft DPIA, taken cumulatively, require the Council to consider the potential risks to the rights and freedoms of data subjects as a result of the proposed processing and any safeguards, security measures or mechanisms proposed to be implemented by the controller to mitigate any risks identified. This fulfils the requirements of sections 84(2)(b) and 84(2)(c) of the 2018 Act. Notwithstanding this, the questions in the DPIA should mirror more closely the wording of section 84. This would be appropriate in light of the Council's obligation to demonstrate compliance with the 2018 Act. For example, there is no question which satisfies the requirements of section 84(3)(a), namely that notwithstanding the adoption of safeguards and mechanisms to mitigate risks, whether, in the Council's opinion, there continues to be a high risk to the rights and freedoms of data subjects and the DPC should be notified.

6.181 There was one question which required the Council to consider less privacy-intrusive solutions, such as non-continuous CCTV surveillance or increased lighting. There was a brief reference to the fact that lighting was an inadequate solution. However, there was no consideration of using alternatives to continuous CCTV surveillance, such as only accessing the CCTV on a retrospective basis or having the cameras turned on at specified times. There was also no analysis of the necessity for operating particular CCTV cameras at each location.

6.182 The DPIA is deficient in describing safeguards that will be implemented to prevent unauthorised access. For example, one safeguard to prevent unauthorised access could be to install software which will encrypt CCTV footage once it is downloaded (for example, for the purposes of transferring it to An Garda Síochána). Article 20 of the LED places emphasis on *'pseudonymisation*' as a means of promoting '*data minimisation*'. I have considered the state of the art and the potential costs of implementation and I believe this would be a proportionate safeguard in the circumstances.

6.183 I welcome the aspects of the DPIA which envisage further consultations being undertaken with the local community as a way of mitigating the risks. For surveillance which poses a high risk to the rights and freedoms of data subjects, an important step in demonstrating such surveillance is proportionate and necessary is to obtain the feedback of the local community. It is noteworthy the Council received correspondence from a resident in Newcastle West which submitted to the Council, the erection of additional CCTV cameras in the area was not necessary.[53] Such submissions should be given weight by the Council in considering whether the erection of extra cameras is necessary.

6.184 I welcome the fact that the Council has taken some steps to mitigate the risks that such surveillance poses to data subjects. For example, in relation to CCTV in town centres the DPIA noted that privacy masking would be introduced to prevent the cameras recording footage from the first and upper floors of all buildings and into windows of buildings. The DPIA is opaque however, on whether the ground floors of buildings are subject to privacy masking. This concern was raised by one of the data subjects who owned a pub opposite one of the intended camera locations and where the data subject indicated he did not want the front door of the pub to be recorded.

6.185 However, in general, the DPIA is deficient in giving sufficient detail as to what safeguards the Council would implement to reduce the risks posed by the CCTV cameras. In response to Question 7 of the DPIA which asks if '*any privacy by design features been adopted to reduce privacy intrusion*' the Council answered:

- '*Privacy masking has been deployed on all CCTV cameras.*
- *Cameras have also been placed on peripheral areas of residential areas, as far away from private properties as possible or at locations that minimize the impact on privacy.*
- *Cameras have been chosen to fulfil surveillance requirements of public areas and at the same time, to facilitate restrictions on zoom levels and panning angles in order to provide effective coverage without being invasive*
- *CCTV monitoring staff are trained in all methods and good practices of CCTV monitoring.*'

[53] At the time the inquiry was conducted the Council intended to commence the operation of six CCTV cameras in an estate in Newcastle West.

6.186 This answer needs to be more specific. Details of the privacy masking that has been employed on all CCTV cameras must be given. For example, what are the restrictions on zoom levels and panning angles of the cameras or what precise training has been given to the staff operating the CCTV systems. In the section of the DPIA where it lists the capabilities of the cameras it does not give details of the privacy masking features. In fact, nineteen cameras are listed as having '*360-degree panoramic view. Pan, tilt and zoom function. Smart tracking.*'

6.187 In the DPIA, the Council also stated it would publish an online map of public CCTV cameras and its use in Limerick city and this could be found via the link: safercommunities.limerick.ie. I have followed this link and on the page there is a link entitled 'Map of CCTV Locations (currently under construction)'.[54] On selecting this link, the map fails to give details of the precise locations in Limerick city for the CCTV cameras. If the Council does intend to install the Smart CCTV cameras in the future, it is important that this map is operational so the Council is able to fulfil its transparency requirements to data subjects.

6.188 I accept, however, in its current form the DPIA demonstrates the necessity and proportionality of some form of surveillance in the areas where it intends to erect CCTV. It followed from a public consultation the Council undertook that a majority of respondents seemed to be in favour of installing CCTV in the areas proposed. The Council also referred to high crime statistics in the relevant areas. Although this demonstrates that some form of surveillance may be warranted, in addition it is important for the Council to satisfy that the means of surveillance chosen are necessary and proportionate.

Findings

6.189 ***I find the Council has infringed section 84 of the 2018 Act in failing to conduct a sufficiently robust assessment of the risks the Smart CCTV cameras posed to the rights and freedoms of individuals and how such risks could be mitigated.***

G. Special Category Data Collection/ Data Protection Impact Assessment

Regime: LED

Inquiry Issue: 32

6.190 Section 69 of the 2018 Act defines special categories of personal data as including '*personal data revealing the racial or ethnic origin of the data subject*'. Irish Travellers are an ethnic group. As discussed above, the Council deployed at least nine CCTV cameras at various traveller accommodation sites in Limerick. These cameras were not authorised by the Garda Commissioner pursuant to section 38(3)(c) of the 2005 Act. Therefore, this Decision finds that the CCTV cameras at these sites process special category personal data.

6.191 Section 73 of the 2018 Act provides that the processing of special category personal data shall be lawful only where section 71 is complied with and one of the nine

[54] < https://www.limerick.ie/safer-communities> last accessed on 26th August 2021.

conditions in section 73(1)(b) is met. This Decision finds that the CCTV cameras at the traveller accommodation sites are unlawful in the absence of a basis for the processing in Union or Member State law which is required by section 71(1)(a). Even if this camera had a basis in Union or Member State law that processing would still have to pass a necessity test for securing public order and safety by facilitating the deterrence, prevention, detection and prosecution of offences.

6.192 The Council has also failed to carry out a DPIA in respect of the CCTV at the traveller accommodation areas as is required by section 84 of the 2018 Act.

Findings

6.193 ***I find the Council has infringed section 71(1)(a) of the 2018 Act in failing to demonstrate it had a valid legal basis for the processing of data by way of CCTV cameras at traveller accommodation areas.***

6.194 ***I find the Council has infringed section 84 of the 2018 Act by failing to carry out a DPIA prior to installing the CCTV cameras.***

H. Data Protection Impact Assessments for Lord Edward Street Development and Clonlong Estate

Regime: LED

Inquiry Issue: 33, 34

6.195 Eleven CCTV cameras were installed by the Estate Management Unit at the Lord Edward Street Development in April 2018. I find the Council has infringed section 84 of the 2018 Act in failing to carry out a DPIA at the Lord Edward Street Development in respect of the CCTV cameras installed. Although, the CCTV was technically installed a month in advance of the GDPR and LED coming into effect, the Council has nonetheless infringed section 84. The reason for this is that the Council has a continuing duty of accountability to show compliance with the 2018 Act under section 71(10) and the Council has failed to satisfy this here.

6.196 In sessions the authorised officers attended on 25th October 2018 as part of the inquiry, it transpired that the Council intended to erect CCTV cameras at a halting site in Clonlong. It transpired at a session the authorised officers attended on 25th October 2018 that the Data Protection Officer of the Council was unaware of this proposed plan. Despite this matter being discussed with the authorised officers on 25th October 2018, the Council proceeded to erect the new CCTV system on 13th November 2018. Despite, requests by the authorised officers to the Council to furnish a DPIA for this new system, none was provided.

6.197 I find the Council has infringed section 88(4)(c)(iii) of the 2018 Act by failing to ensure the Data Protection Officer was involved, properly and in a timely manner in their decision to proceed with this CCTV system. The Council has also infringed section 84 of the 2018 Act by failing to carry out a DPIA in respect of this project.

Findings

6.198 ***I find the Council has infringed section 84 by failing to carry out a DPIA in respect of the CCTV cameras installed at the Lord Edward Street Development and the Clonlong halting site.***

6.199 ***I find the Council has infringed section 88(4)(c)(iii) of the 2018 Act by failing to ensure the Data Protection Officer was involved, properly and in a timely manner in the Council's decision to proceed with the CCTV system at Clonlong.***

I. Security Measures for Traffic Management CCTV

Regime: GDPR

Inquiry Issue: 2, 5, 6, 9

i) Access Logs

6.200 Section 82(1) of the 2018 Act provides:

'*...where a controller or processor carries out processing of personal data by automated means, the controller or processor, as the case may be, shall create and maintain a log ... of the following processing operations carried out in automated processing systems in respect of that processing:*

(a) the collection of personal data for the purposes of such processing and the alteration of any such data;

(b) the consultation of the personal data by any person;

(c) the disclosure of the personal data, including the transfer of the data, to any other person;

(d) the combination of the personal data with other data;

(e) the erasure of the personal data, or some of the data.

(2) Where a data log contains information specified in paragraph (b) or (c) of subsection (1), the controller or processor, as the case may be, shall ensure that the data log contains sufficient information to establish the following:

(a) the date and time of the consultation or disclosure, as the case may be;

(b) the reason for the consultation or disclosure, as the case may be;

(c) in so far as is possible, the identification of the person who consulted or disclosed, as the case may be, the personal data;

(d) the identity of any recipient to whom the personal data were disclosed.'

6.201 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.

6.202 The inquiry team on visiting Henry Street Garda Station, were supplied with a printout showing accesses to the traffic management CCTV system over a three day period by members of An Garda Síochána. The reason for the consultation or the identity of the person who accessed the CCTV were not set out in the access log in Henry Street Garda Station in contravention of Article 32(1) of the GDPR. In the access log in Henry Street Garda Station, the generic username 'Garda' was used instead of giving the specific identity of the name of the person who accessed it.

Findings

6.203 ***I find the Council, as the controller of the CCTV cameras which were connected via a live feed to Henry Street Garda Station, infringed Article 32(1) of the GDPR by failing to ensure the purpose of consulting the data and the identity of the persons who consulted the data were set out in the access log.***

ii) Security of Monitoring Screens

6.204 During the course of the audit, it was established at the Traffic Management Centre in City Hall that there was a corridor window from which passing staff could see into the monitoring room where there were live feeds to the twenty-six traffic management cameras. I find the Council, in failing to implement measures to prevent passing staff from looking into the monitoring room, has infringed Article 32(1) of the GDPR which requires data to be processed in a manner that ensures appropriate security of the data including the implementation of appropriate technical or organisational measures to protect against unlawful processing.

Findings

6.205 ***I find the Council has infringed Article 32(1) of the GDPR in failing to install an adequate security measure which would prevent passing staff looking into the monitoring room.***

J. Security Measures at [redacted] monitoring centres

Regime: LED

Inquiry issue: 11, 17, 18, 19, 22, 24, 26, 27, 28, 29, 30

i) Signage regarding phone use

6.206 An investigation conducted at [redacted] monitoring centre on 27th September 2018 revealed that there were no signs in place prohibiting staff or visitors from using personal audio or video recording devices to record images displayed on the monitoring screens. An investigation conducted at [redacted] monitoring centre on 2nd October 2018 revealed that there were a lack of signs prohibiting staff or visitors from using personal audio or video recording devices to record images displayed on the monitoring screens. The investigation also determined there were no data protection policies in place, governing what safeguards employees or agents of the Council should abide by while in the monitoring rooms.

Findings

6.207 ***I find the Council has infringed section 71(1)(f) of the 2018 Act by failing to process data in a manner that ensures the appropriate security of the data by neglecting to install signs regarding phone use in the monitoring rooms in [redacted] monitoring centres.***

6.208 ***I find the Council has infringed section 72(2) by failing to demonstrate that it took reasonable steps to bring to the employees' or agents' attention working in the monitoring centres about necessary security measures such as not using phones to record monitoring screens in the monitoring rooms.***

6.209 ***I find the Council has infringed section 75(3) by failing to implement a data protection policy in respect of processing operations at [redacted] monitoring centres.***

ii) Access logs and auditing of audit trails

6.210 The CCTV system operated by [redacted] at [redacted] monitoring centre has a facility which electronically logs all accesses to the CCTV footage. At the time of the inspection on 27th September 2018 it was established that arising from a system fault, all staff accesses to the CCTV footage were recorded under one common username. Consequently, it is impossible to identify the particular staff member who accessed CCTV footage on a particular day. It was established in an inspection of [redacted] monitoring system on 2nd October 2018 that the access log system is subject to the same defect.

6.211 The investigations of [redacted] monitoring centres ascertained there was no system in place which requires the controller or the processor to audit the audit trials. 'Auditing of audit trails' is a proportionate security measure considering the processing operations that take place at [redacted] monitoring centres. The onus is on the controller to demonstrate compliance with the GDPR and LED and this entails conducting reviews of the access logs. This is essential to confirm that personal data is being accessed for lawful purposes and to ensure the processing is carried out in accordance with the purpose limitation principle.

<u>Findings</u>

6.212 ***I find the Council has infringed section 82(2) of the 2018 Act by not having access logs in place at [redacted] monitoring centres which permitted the identification of persons who accessed the CCTV footage.***

6.213 ***I find the Council's failure to demonstrate that it carried out audits of the audit trails at both monitoring centres infringed section 71(1)(f) of the 2018 Act.***

iii) Informal disclosures of personal data to An Garda Síochána

6.214 In investigations of [redacted] monitoring centres it emerged that An Garda Síochána occasionally verbally requested that [redacted] conduct surveillance of certain individuals by observing their activities on the monitoring screens and keeping note of their movements. [redacted]

[redacted]. They would subsequently give verbal updates to An Garda Síochána, normally by telephone. There is no custom of An Garda Síochána making formal written requests seeking access to this information and [redacted] does not keep a formal record of the verbal disclosure of the personal data concerned. In order to ensure that personal data is collected by An Garda Síochána for a valid purpose it is necessary that the date and time, the purpose and the identity of the Garda member, as required by section 82, is recorded by the operative at the monitoring centre in an access log prior to divulging this information.

6.215 I find the Council has failed to demonstrate a legal basis which would allow it as controller (or a processor engaged by it) to conduct targeted surveillance on behalf of An Garda Síochána. Targeted surveillance is particularly invasive and it needs to have a particularly precise legal basis based on Union or Member State law for it to be compatible with section 71(1)(a) of the 2018 Act. Although, the cameras were authorised under section 38(3)(c) of the 2005 Act, this Act does not expressly empower local authorities to conduct targeted surveillance of individuals on behalf of An Garda Síochána.

<u>Findings</u>

6.216 ***I find the Council has infringed section 71(1)(a) in failing to demonstrate it had a legal basis to conduct targeted surveillance on behalf of An Garda Síochána.***

6.217 ***I find the Council has infringed section 82(1) of the 2018 Act by failing to maintain an access log in respect of verbal requests for disclosure of personal data captured by CCTV footage by members of An Garda Síochána.***

iv) Access by members of An Garda Síochána and Authorised Officers

6.218 It emerged during the inspection on 2nd October 2018 that a Garda based in the Technical Unit at Roxboro Road Garda Station in Limerick city has access at all times by means of a key fob to [redacted] monitoring centre. This arrangement pre-dates the commencement of real-time monitoring and it is ongoing for at least ten years. At the monitoring centre, the Garda concerned is permitted to review and download footage, unsupervised, from the CCTV system. The Garda does not provide the monitoring centre with written requests and an access log is not maintained detailing the record of his activities.

6.219 It emerged during the same inspection that a team of Gardaí are sometimes sent to [redacted] monitoring centre where they carry out live surveillance using the CCTV monitoring equipment. When such Garda operations occur, the staff of the monitoring centre are requested to leave the monitoring centre. Thus, these operations occur without operatives of the centre being present. An Garda Síochána also does not provide formal requests in respect of these operations, it is only where CCTV is subsequently downloaded that a formal written request is made by An Garda Síochána. It also transpired that the authorised officers of the Council have access at all times by

means of a key fob to [redacted] monitoring centre. These officers access the data on the CCTV cameras for law enforcement purposes.

6.220 It is important to note, that when members of An Garda Síochána access personal data at [redacted] monitoring centre this is permitted by section 38(7) of the 2005 Act which requires the local authority given authorisation to operate CCTV to:

'*ensure that members of the Garda Síochána have access at all times to the CCTV to which that authorisation relates for the purpose of—*

(a) supervising and controlling the operation of the CCTV on behalf of the Garda Commisioner, or

(b) retrieving information or data recorded by the CCTV.'

6.221 Although, for the reasons discussed above, section 38 is not a valid legal basis to process personal data under the LED, it is worth emphasising nonetheless that An Garda Síochána has statutory authority under Irish law.

6.222 The Council, however, has infringed section 82 of the 2018 Act by failing to keep an access log detailing the date and time, the purpose and the identity of the individual Garda member or the Garda teams which accessed personal data from the CCTV cameras at [redacted] monitoring centre. The requirement for the [redacted] operators to leave the monitoring room when a Garda team arrives on site also poses a risk to data subjects' rights. Under section 72(2) a controller or processor is required to take all reasonable steps to ensure that:
'*(a) persons employed by the controller or the processor, as the case may be, and (b) other persons at the place of work concerned, are aware of and comply with the relevant technical or organisational measures referred to in subsection (1).*'

6.223 These technical and organisational measures under section 72(1) include taking measures to prevent the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of personal data, in proportion with the harm that might result from such occurring. Accordingly, as the operatives are required to have knowledge on what technical and organisational measures have to be adhered to, it makes sense for at least some of the operatives to remain onsite while members of An Garda Síochána are carrying out surveillance. This would help to ensure that An Garda Síochána does not act in contravention of the 2018 Act in carrying out its surveillance operations.

6.224 As the Council's authorised officers are employees or agents of the Council, who is a controller of the CCTV system at [redacted] monitoring centre, there is no impediment in principle to the Council's authorised officers having access to the data for law enforcement purposes. In accordance with section 69 of the 2018 Act, the Council is a '*competent authority*' for the purposes of Part 5 of the Act and is thus entitled to

process personal data for law enforcement purposes. In its submission in response to the draft inquiry report the Council noted:

'The Council takes the point that Authorised Officers, who have been Garda Vetted and are acting on behalf of the Council as Data Controller, should still be subject to controls that protect them from allegations that they are acting, in any particular instance, without the authority of the Council. The functions of the [redacted] *Monitoring Centre, along with its staff, have moved to* [redacted] *and will operate under the controls in place in* [redacted]. [redacted] *is staffed on a continuous basis and any Authorised Officers who present will have to produce a written request for access to personal data associated with a specific case or incident certified by their supervisory officer. This will be logged and retained by* [redacted]*.'*

6.225 I agree that it is a necessary technical and organisational measure under section 75 to protect the security of personal data, that the Council's authorised officers or members of An Garda Síochána should not be permitted to access personal data without operatives of the monitoring centre being present. The presence of an operator should ensure that the purpose of the processing is recorded in access logs which is an essential safeguard to ensure the personal data is being processed lawfully.

Findings

6.226 ***I find the Council has infringed section 82(1) of the 2018 Act by not maintaining access logs in recording the site visits made by the Garda member from Roxboro Road Garda Station and various Garda teams at*** [redacted] ***monitoring centre.***

6.227 ***I find the Council has infringed section 75(1) of the 2018 Act by failing to have a measure in place which requires an operative of the monitoring centre to be present when a visit of a Garda member or an authorised officer takes place.***

K. Security Measures regarding Garda Síochána Access to Estate Management CCTV Cameras

Regime: LED

Inquiry Issue: 35

6.228 The Estate Management Unit of the Council is responsible for operating thirty-nine CCTV cameras at Banogue, Garryowen, Deebert (Kilmallock), Lee Estate, Lismakeera (Askeaton), Churchview (Askeaton), Old Cratloe Road, Altimira, Bruff Playground, The Banks (Kings Island) and Cluain Dubh. As discussed above, there was no evidence that An Garda Síochána determined the means and purposes of these cameras and it appears the Council installed them unilaterally. Accordingly, the cameras do not fall under a joint controller agreement with An Garda Síochána.

6.229 It was ascertained during the inquiry, that a Garda Communications Officer based in Henry Street Garda Station had direct access by remote dial-in on a retrospective basis to these cameras. According to the Council, the motive behind granting An Garda Síochána this access was:

'*to allow a faster response to complaints especially out of hours. It assisted in ensuring resources were not deployed to areas where there was no need for same. It was retrospective reviewing of issues albeit issues that may have occurred only 5 minutes previous.*'

6.230 Section 71(1)(a) of the 2018 Act requires that '*data shall be processed lawfully and fairly*'. In addition, section 71(1)(f) provides:
'*the data shall be processed in a manner that ensures appropriate security of the data, including, by the implementation of appropriate technical or organisational measures, protection against—*
(i) unauthorised or unlawful processing, and
(ii) accidental loss, destruction or damage.'

6.231 I find the Council has infringed this provision of the Act by granting the Garda member access to the data concerned. The arrangement does not fall under the aegis of a joint controller agreement with An Garda Síochána and An Garda Síochána accordingly does not have an automatic entitlement to view the personal data captured by these cameras under Irish law.

Findings

6.232 ***I find the Council has infringed section 71(1)(a) by failing to ensure that the personal data collected via the above-mentioned CCTV cameras was processed lawfully.***

L. Data Protection Policy

Regime: LED

Inquiry Issue: 38

6.233 In considering other issues raised by this inquiry, I have found that the Council has infringed its duty to implement a data protection policy under section 75(3) of the 2018 Act in respect of some processing operations.

6.234 As a stand-alone issue, the inquiry report noted that although the Council has a draft Data Protection Policy covering the use of CCTV systems, ANPR and drones, the Council is yet to finalise this policy. I have searched for this policy by way of a 'Google Search' and the most recent policy I could find is entitled '*Limerick City and County Council CCTV Policy*'.[55] This policy is dated 9th December 2019 and has a watermark with the word '*Draft*' imprinted on each page. The executive summary notes a separate policy applies for the Council's use of drones but I could find no such policy online. The inquiry team had previously been furnished with an earlier version of the Council's CCTV policy dated 15th July 2018.

6.235 Insofar, as the Council had no CCTV policy from 25th May 2018 until 15th July 2018 for its use of CCTV and ANPR surveillance, I find the Council infringed section 75(3) of the 2018 Act. Although, the Council did submit a draft drones policy to the DPC,

[55] Accessed on 10th August 2021.

this was dated 8th November 2018. Insofar, as the Council had no drones policy in place until 8th November 2018, I find the Council has infringed section 75(3) of the 2018 Act.

Findings

6.236 ***I find the Council has infringed section 75(3) of the 2018 Act by failing to implement a data protection policy in respect of its use of CCTV and ANPR until the 15th July 2018.***

6.237 ***I find the Council has infringed section 75(3) for failing to implement a data protection policy governing its use of drones until 8th November 2018.***

M. Smart CCTV pilot project access by a member of An Garda Síochána

Regime: LED

Inquiry Issue: 46

6.238 It was established that a Garda Communications Officer had direct access to stand-alone CCTV cameras in the following towns: Castleconnell, Murroe, Patrickswell, Croom and Pallasgreen. These cameras appear to have been authorised by the Garda Commissioner pursuant to section 38(3)(c) of the 2005 Act. These cameras form part of the Council's Smart CCTV project.

6.239 When CCTV cameras are authorised pursuant to section 38 of the 2005 Act, I note section 38(7) of the 2005 Act requires local authorities to give members of An Garda Síochána access at all times to the CCTV. However, for the reasons discussed above, it is my view that section 38 of the 2005 Act does not provide local authorities with valid legal basis to process personal data by way of CCTV cameras. Accordingly, I find the Council has infringed section 71(1)(a) of the 2018 Act by giving access to a member of An Garda Síochána to the aforementioned cameras.

Findings

6.240 ***I find the Council has infringed section 71(1)(a) of the 2018 Act by giving access to a member of An Garda Síochána to the Smart CCTV cameras in Castleconnell, Murroe, Patrickswell, Croom and Pallasgreen.***

N. Smart CCTV pilot project: Garda access to the new monitoring centre at [redacted]

Regime: LED

Inquiry Issue: 47

6.241 During the inspection of the new monitoring centre at [redacted] (which was under construction at the time of the inspection), the inquiry team observed there was a small room adjacent to the monitoring room. The inquiry team were advised that An Garda Síochána will use this room for the purpose of on-site reviewing and downloading of CCTV footage.

Findings

6.242 ***I can make no findings in respect of the new monitoring centre as processing had not commenced at the time the audit took place.***

O. Time Limits on the Storage of Personal Data

Regime: LED

Inquiry Issue: 12

6.243 Article 4(1) of the LED provides:

'*1. Member States shall provide for personal data to be:*

…

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed'.

6.244 Article 5 of the LED provides:

'*Member States shall provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Procedural measures shall ensure that those time limits are observed.*'

6.245 Section 71 of the 2018 Act provides:

'*(1) A controller shall, as respects personal data for which it is responsible, comply with the following provisions:*

…

(c) the data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed;

…

(7) A controller shall ensure, in relation to personal data for which it is responsible, that an appropriate time limit is established for—

(a) the erasure of the data, or

(b) the carrying out of periodic reviews of the need for the retention of the data.

(8) Where a time limit is established in accordance with subsection (7), the controller shall ensure, by means of procedural measures, that the time limit is observed.'

6.246 Section 81 provides:

'*(1) A controller shall create and maintain a record in writing containing the following information in relation to each category of processing activity for which it is responsible:*

…

(b) a description of—

…

(vii) where possible, the proposed time limit within which each category of personal data shall be erased'.

6.247 It was ascertained during the inquiry the data collected on CCTV cameras at [redacted] monitoring centre was not automatically deleted after a certain period. Instead footage is deleted when the hard drives are filled to capacity and an overwriting process occurs. This is in essence is a random data retention period. This is also inconsistent with the monitoring centre's own retention policy which prescribes personal data captured by the CCTV cameras will be deleted after a period of thirty days.

Findings

6.248 ***I find the Council is compliant with section 71(7) and section 81 of the 2018 Act in that it has prescribed a time limit for deleting personal data.***

6.249 ***However, I find the Council has infringed section 71(8) by failing to ensure that time limit is observed.***

6.250 ***I find section 71(1)(c) of the 2018 Act has been infringed by the Council, as it has not shown the retention of such data is necessary.***

P. Subject Access Requests Traffic Management Centre

Regime: GDPR

Inquiry Issue: 4

6.251 Article 15(1) of the GDPR confers on data subjects '*the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:*

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c)the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d)where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e)the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g)where the personal data are not collected from the data subject, any available information as to their source;

(h)the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.'

6.252 EDPB Guidelines elaborate on the requirements of a controller under Article 15 of the GDPR in relation to personal data collected via video surveillance:

'*A data subject has the right to obtain confirmation from the controller as to whether or not their personal data are being processed. For video surveillance this means that if no data is stored or transferred in any way then once the real-time monitoring moment has passed the controller could only give the information that no personal data is any longer being processed (besides the general information obligations under Article 13, see section 7 – Transparency and information obligations). If however data is still being processed at the time of the request (i.e. if the data is stored or continuously processed in any other way), the data subject should receive access and information in accordance with Article 15.*'[56]

6.253 Article 15(3) requires the controller to furnish the data subject with a copy of his or her personal data that was subject to processing. However, Article 15(4) of the GDPR provides:

'*[t]he right to obtain a copy [of one's personal data] shall not adversely affect the rights and freedoms of others*'.

6.254 In the context of processing subject access requests in relation to CCTV footage, the EDPB Guidelines note, if other persons have been captured by CCTV in the particular segment of footage sought, the controller is required to implement technical measures to anonymise the other data subjects in the footage.[57] This is essential to protect the rights and freedoms of the other data subjects. Examples of technical measures could include image-editing such as masking or scrambling.[58] The Guidelines clarify the presence of other data subjects in the footage does not absolve the controller from providing a data subject with a copy of his or her personal data when requested to do so.

[56] EDPB Guidelines 3/2019 on processing of personal data through video devices (adopted on 10th July 2019) pages 18-19.
[57] Ibid 19.
[58] Ibid.

6.255 The EDPB Guidelines also refer to Article 11(2) of the GDPR in relation to the processing of personal data by way of CCTV cameras. Article 11(2) of the GDPR provides Articles 15 to 20 of the GDPR will not apply where '*the controller is able to demonstrate that it is not in a position to identify the data subject…*'. The Guidelines note in relation to this:

'*If the video footage is not searchable for personal data, (i.e. the controller would likely have to go through a large amount of stored material in order to find the data subject in question) the controller may be unable to identify the data subject. For these reasons the data subject should (besides identifying themselves including with identification document or in person) in its request to the controller, specify when – within a reasonable timeframe in proportion to the amount of data subjects recorded – he or she entered the monitored area. The controller should notify the data subject beforehand on what information is needed in order for the controller to comply with the request. If the controller is able to demonstrate that it is not in a position to identify the data subject, the controller must inform the data subject accordingly, if possible.*'[59]

6.256 In short, where the data subject provides an estimated timeframe at which his or her personal data was processed, the controller of the CCTV cameras remains under an obligation to provide a copy of the personal data sought for the purposes of Article 15 of the GDPR.

6.257 Article 12 of the GDPR prescribes another exception to the data subject's right to access his or her personal data under Article 15:

'*In case of excessive or manifestly unfounded requests from a data subject, the controller may either charge a reasonable fee in accordance with Article 12 (5) (a) GDPR, or refuse to act on the request (Article 12 (5) (b) GDPR). The controller needs to be able to demonstrate the excessive or manifestly unfounded character of the request.*'[60]

6.258 At the time of the inspection of the traffic management centre on 2nd October 2018 it was established that all subject access requests for access to personal data contained in the CCTV footage captured by the traffic management cameras were rejected. The manager of the traffic management centre was unaware of the rights of data subjects to seek access by means of subject access requests to a copy of their personal data kept on recorded CCTV footage.

6.259 I have taken into account the Council's submission in respect of the Draft Inquiry Report that the general policy is to refer subject access requests to the Data Protection Officer and that the management team deals with any situations where a data subject access request is not referred.

6.260 I have considered the Council's submissions relating to the Draft Decision. I have given regard to the correspondence the Council submitted relating to subject access

[59] Ibid.
[60] Ibid.

requests made to the Council within the range of April 2015 and October 2017. The Council replied to two subject access requests stating that either the requester's personal data had been deleted or was not captured by the Council's CCTV cameras. No response to the third subject access requested was appended to the Council's submissions on the Draft Decision. I have also considered the Council's submission that in any case where relevant footage was available it was provided to the DPO for consideration. I have also considered the Council's comment that it was never articulated by the Traffic Management Unit that subject access requests would not be processed and if such a response was encountered it would have been addressed promptly by Council Management. I have also considered the Council's submission that '*[a]t the time of the above inspection, 24 data subject access requests under the GDPR had been received by the DPO and were processed in accordance with the relevant legislation.*'

6.261 Nonetheless, despite having considered these submissions, I remain of the view that the Council has infringed its obligations under Article 15 of the GDPR. It was established during the course of the inquiry that the manager of the Traffic Management Centre was unaware of their obligations in relation to procedures with regard to processing access requests. It was ascertained that the manager Traffic Management Centre rejected requests for access to footage made by individuals irrespective of whether the footage relates to drivers, cyclists or pedestrians. The Council is under an obligation to process all subject access requests irrespective of whether they are received by the DPO or not.

6.262 The Council has not demonstrated that any of the requests should not have been processed on foot of Article 11(2) or Article 12 of the GDPR.

Findings

6.263 ***I find the Council has infringed Article 15 by rejecting subject access requests in respect of processing at the Traffic Management Centre.***

Q. Smart CCTV Pilot Project: Subject Access Requests

Regime: LED

Inquiry Issue: 45

6.264 At the time of the inspection of the Rathkeale Hub (part of the Smart CCTV Pilot Project) on 2nd October 2018, it was established that data subjects who submit subject access requests for access to personal data contained in CCTV footage captured by the Smart CCTV cameras in Rathkeale and in the other thirteen towns are currently advised to contact An Garda Síochána. There was no evidence of a procedure being in place with details on how to deal with a data subject access request.

6.265 As discussed above, as the Smart CCTV Pilot Project has been subject to approval by the Garda Commissioner under section 38 of the 2005 Act, An Garda Síochána is a joint controller of this CCTV system. Section 79(2) of 2018 Act requires joint controllers to have an agreement in writing. The section states the agreement:

'*(a) shall include a determination of—*

(i) the respective responsibilities of the joint controllers concerned as regards the exercise by data subjects of their rights under this Part, and

(ii) the respective duties of the joint controllers concerned as regards the provision to a data subject of the information specified in section 90(2)

and

(b) may designate a single point of contact in respect of the processing concerned for the data subject to whom it relates, where such designation is not otherwise determined by the law of the State.'

6.266 Section 79(2) seems to envisage that one joint controller can be designated as the single point of contact for handling data subject access requests and this could be An Garda Síochána. However, the EDPB has noted:

'*Irrespective of the terms of the arrangement, data subjects may exercise their rights in respect of and against each of the joint controllers. Supervisory authorities are not bound by the terms of the arrangement whether on the issue of the qualification of the parties as joint controllers or the designated contact point.*'[61]

6.267 It follows from this, that even if An Garda Síochána was the designated contact point for handling subject access requests, the Council is not absolved of its responsibility to deal with a request when it is made directly to the Council. In any event, due to the absence of a joint controller agreement, it cannot be said that An Garda Síochána has been designated as the contact point for handling such requests. It follows that the Council has a responsibility to respond to all subject access requests in respect of the Smart CCTV project, where those requests are directed to the Council.

6.268 I have taken into account the Council's submission in respect of the Draft Inquiry Report that the general policy is to refer subject access requests to the Data Protection Officer and that the management team deals with any situations where a data subject access request is not referred.

6.269 I have also given consideration to following submission of the Council relating to the Draft Decision:

'*The Council has never been in a position whereby it relied on, or expected, An Garda Síochána to recover CCTV footage on our behalf and would not have directed any data subject to An Garda Síochána in this regard.* […]*This is the only circumstance under which a data subject is directed to An Garda Síochána and it is with a view to the investigation of an incident by An Garda Síochána rather than the data subject accessing their personal data via An Garda Síochána. Any such access request would be processed by the Council.*'

[61] EDPB Guidelines, Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 1.0 (Adopted on 02 September 2020) page 4.

6.270 Having considered the above submissions I find the Council has not infringed section 91 of the 2018 Act in failing to process subject access requests from Rathkeale Hub. It appears when access requests were made by data subjects to Rathkeale Hub, data subjects were only required to contact the Gardaí where their query pertained to the investigation and there was no blanket policy of referring subject access requests to An Garda Síochána.

Findings

6.271 ***I find the Council has fulfilled its responsibilities under section 91 of the 2018 Act in this instance.***

R. DPIA for drones

Regime: LED

Inquiry Issue: 48

6.272 The Commercial Waste Enforcement Section of the Council informed the investigators on 13th November 2018 that it used a drone on five occasions in 2018. It was stated that the Section does not set out to use the drone to capture images of persons but in the event that the drone captured the image of a person in the act of dumping waste, the Council would use the recorded footage in its investigation of the offence. Separately, the Water Monitoring Section of the Council uses drones to survey the waterways in the context of its law enforcement powers under the Water Pollution Acts. It may use any images it captures of suspected polluters for investigation and prosecution purposes.

6.273 The inquiry team found no evidence of a DPIA being carried out for drones pursuant to section 84 of the 2018 Act. Section 84(1) provides:

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

6.274 Drones are mobile recording devices which have a wide sphere of movement and have the capacity to record or take pictures of natural persons from a height. I find such technology, by its nature, poses a high risk to the rights and freedoms of individuals. In particular, the right to protection of personal data in Article 8 of the Charter of Fundamental Rights of the European Union can be cited. In failing to carry out a DPIA the Council has not fulfilled the requirements of section 84(1) of the 2018 Act.

Findings

6.275 ***I find the Council has infringed section 84 of the 2018 Act by not carrying out a DPIA prior to using drones.***

S. SMART CCTV Pilot Project Purpose Limitation

Inquiry Issue: 40

6.276 The Council informed the inquiry team that the primary purpose of the Smart CCTV project is to secure public order and safety in public places by facilitating the deterrence, prevention, detection and prosecution of offences. On 11th December 2017 authorisation was given by the Garda Commissioner for the installation of forty-four CCTV cameras at fourteen locations under section 38 of the 2005 Act.

6.277 The Council also indicated another purpose of the project would be to generate near real-time open statistical data relevant for the functions of the local authority such as traffic flows, pedestrian flows, line crossing and intrusion detection. It also indicated that it wants to use the project to help promote tourism and events organised in town centres (festivals, markets, parades, etc.) to an international audience by providing an online streaming service in a number of town centres and other suitable locations. The Council in its application for authorisation described the type of cameras it intended to install. One camera is described as an '*Internet Protocol Based Smart CCTV camera*' and it is stated as having the following features:

'A proprietary ANPR software shall be included for the number plate recognition at appropriate locations. These bullet type ANPR cameras shall also incorporate Smart CCTV functions and operate as Footfall Counters, Facial Detection, Intrusion Detection and Line Crossing Detection cameras respectively.'

6.278 The inquiry team queried whether the Council's intention to use the cameras for purposes other than the prevention, investigation, detection and prosecution of crime is compatible with purpose limitation principle.

6.279 Section 71(1)(b) of the 2018 Act provides a controller shall only collect personal data '*for one or more specified, explicit and legitimate purposes and shall not be processed in a manner that is incompatible with such purposes.*'

6.280 Section 38(1) of the 2005 Act states:

'*The Garda Commissioner may authorise the installation and operation of CCTV for the sole or primary purpose of securing public order and safety in public places by facilitating the deterrence, prevention, detection and prosecution of offences.*'

6.281 It does not envisage CCTV systems being used for purposes other than the deterrence, prevention, detection and prosecution of offences.

6.282 The EDPB Guidelines in respect of video surveillance elaborate on the requirements the purpose limitation principle under Article 5(1)(b) of the GDPR (which is the analogue of Article 4(1)(b) of the LED and section 71(1)(b) of the 2018 Act). The Guidelines provide that before processing takes place '*the purposes of processing have to be specified in detail*'. For example, the Guidelines note: '*Video surveillance based on the mere purpose of "safety" or "for your safety" is not sufficiently specific*'. In

addition the Guidelines note video surveillance poses particular challenges to the purpose limitation principle:

'*While individuals might be comfortable with video surveillance set up for a certain security purpose for example, guarantees must be taken to avoid any misuse for totally different and – to the data subject – unexpected purposes (e.g. marketing purpose, employee performance monitoring etc.). In addition, many tools are now implemented to exploit the images captured and turn traditional cameras into smart cameras. The amount of data generated by the video, combined with these tools and techniques increase the risks of secondary use (whether related or not to the purpose originally assigned to the system) or even the risks of misuse.*'

6.283 As the Council had not used the Smart CCTV cameras to process data for purposes other than that of countering crime at the time the inquiry took place, I find the Council has not infringed the purpose limitation principle stated in section 71(1)(b) of the 2018 Act.

6.284 However, as an observation, it is important to note that if the Council did proceed to process data for the other purposes apart from countering crime mentioned above, it is necessary for the Council to clearly express these other purposes and make them known to data subjects. This is required by the principle of transparency expressed in Recital 26 of the LED. In addition, the Council would have demonstrate that it has a legal basis for the processing of personal data for these additional purposes. In this regard, the Council has adduced no such legal basis to date.

Findings

6.285 ***I find the Council has not infringed section 71(1)(b) of the 2018 Act in respect of the forty-four CCTV cameras which were authorised under section 38 of the 2005 Act.***

7. Decision on Corrective Powers

7.1 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: Installing more CCTV cameras than permitted in the Garda Commissioner authorisation dated 11th December 2017 for the Smart CCTV Project without having a lawful basis to do so; Installing 128 cameras feeding views from from Ballynanty, Thomondgate, St. Mary's Park and Kileely into [redacted] monitoring centre without providing evidence of a detailed Garda Commissioner authorisation dated 19th September 2006; Installing 64 cameras feeding views from [redacted], Carew Park, Weston and Rathbane into [redacted] monitoring centre without having a legal basis to do so;

	Installing 57 cameras in Banogue, Garryowen, Deebert (Kilmallock), Lee Estate, Lismakeera (Askeaton), Churchview (Askeaton), Old Cratloe Road, Altimira, Bruff Playground, The Banks (Kings Island), Cluain Dubh, Abbeycourt Estate Rathkeale, Lord Edward Street Development, Riverview Estate Kilmallock, Watergate, Clonlong, Kilmallock Road, Sharwood & Castleview Estates Newcastle West and Fr. Casey Close Abbeyfeale without having a legal basis to do so; Installing 9 cameras at traveller accommodation sites including Dublin Road Halting Site, Clondrinagh Halting Site, Rhebogue Halting Site, Rathkeale, Rathbane Depot and Clonlong without having a legal basis to do so; Installing 13 cameras at the 'Smarter Travel' walkway without having a legal basis to do so; Installing 3 cameras at Mt. St. Lawrence Cemetery without having a legal basis to do so; Using ANPR technology as part of the Smart CCTV Pilot Project without having a legal basis to do so; Supplying An Garda Síochána with a live feed to the CCTV cameras at the 'Smarter Travel' Walkway without having a legal basis to do so; Failing to demonstrate that it had a legal basis to conduct targeted surveillance on behalf of An Garda Síochána at [redacted] and [redacted] monitoring centres; Giving a Garda Communications Officer based in Henry Street Garda Station direct access by remote dial-in to CCTV cameras in Banogue, Garryowen, Deebert (Kilmallock), Lee Estate, Lismakeera (Askeaton), Churchview (Askeaton), Old Cratloe Road, Altimira, Bruff Playground, The Banks (Kings Island) and Cluain Dubh without having a lawful basis to do so; Giving a Garda Communications Officer access to Smart CCTV cameras in Castleconnell, Murroe, Patrickswell, Croom and Pallasgreen without having a lawful basis to do so.
Article 5(1)(a) of the GDPR	I have found the Council has infringed this Article by: Operating 26 traffic management cameras without having a legal basis to do so;

	Sharing the personal data captured by the traffic management CCTV cameras with An Garda Síochána despite not having a legal basis to do so.
Article 13 of the GDPR	I have found the Council has infringed Article 13 of the GDPR in failing to erect signage or provide the necessary information on its website in relation to its processing of personal data by traffic management CCTV cameras.
Article 12 of the GDPR	I have found the Council has infringed Article 12(1) by failing to provide the information required by Article 13 of the GDPR in a transparent and easily accessible form.
Section 90 of the 2018 Act	I have found the Council has infringed section 90(1) of the 2018 Act in failing to meet its obligations to provide the information specified in section 90(2) in a reasonable period after the personal data was processed by the CCTV cameras at the 'Smarter Travel' Walkway, [redacted].
Section 93 of the 2018 Act	I have found the Council has infringed section 93(1) of the 2018 Act by failing to provide the information specified in section 90(2) in an accessible manner in respect of the CCTV cameras at the 'Smarter Travel' Walkway, [redacted] monitoring centre and [redacted] monitoring centre.
Section 79 of the 2018 Act	I have found the Council has infringed section 79(1) of the 2018 Act by: Failing to have a joint controller agreement in place governing the CCTV camera surveillance at the 'Smarter Travel' Walkway; Failing to have a joint controller agreement in place governing CCTV cameras monitored via [redacted] monitoring centres; Failing to have a joint controller agreement in place governing CCTV cameras forming part of the Smart CCTV Pilot Project.
Section 80 of the 2018 Act	I have found the Council has infringed: Section 80(1)(a) of the 2018 Act by not having an agreement in writing which set out all the required matters referred to in section 80(2); Section 80(1)(b) of the 2018 Act by failing to receive sufficient guarantees from the controller to implement appropriate technical and organisational measures as required by the 2018 Act; Section 80(1) of the 2018 Act by not having a contract in writing with the processor which sets out the conditions when the processor can engage another processor in accordance with section 80(2)(d).

Section 84 of the 2018 Act	I have found the Council has infringed section 84 of the 2018 Act by failing to carry out a DPIA in advance of beginning surveillance operations using CCTV cameras: At [redacted] monitoring centres; As Part of the Smart CCTV Pilot Project; At traveller accommodation areas; At the Lord Edward Street development. I have also found the Council has infringed section 84 of the 2018 Act by not carrying out a DPIA prior to using drones.
Section 71(1)(c) of the 2018 Act	I have found the Council has infringed section 71(1)(c) of the 2018 Act by failing to demonstrate that the continuous real time monitoring operations that were conducted in [redacted] monitoring centres are not excessive and are necessary. I have found the Council has infringed section 71(1)(c) by failing to show the retention of data at [redacted] monitoring centre is necessary.
Section 76 of the 2018 Act	I have found the Council has infringed section 76(1) of the 2018 Act by failing to implement appropriate technical and organisational measures to prevent private dwellings being monitored prior to operating CCTV cameras.
Section 72 of the 2018 Act	I have found the Council has infringed section 72(2) of the 2018 Act by failing to have an appropriate procedure and training measures in place to inform staff on the requirements of the GDPR and the 2018 Act.
Section 88 of the 2018 Act	I have found the Council has infringed section 88(4)(c) of the 2018 Act by failing to ensure the Data Protection Officer was involved, properly and in a timely manner in the Council's decision to proceed with the CCTV system at Clonlong.
Article 32(1) of the GDPR	I have found the Council has infringed Article 32(1) of the GDPR by failing: To ensure the purpose of consulting the data and the identity of the persons who consulted the data captured by the traffic management CCTV cameras were set out in the access log in Henry Street Garda Station;

	To install an adequate security measure which would prevent passing staff looking into the monitoring room at the Traffic Management Centre.
Section 71(1)(f) of the 2018 Act	I have found the Council has infringed section 71(1)(f) of the 2018 Act by: Failing to process data in a manner that ensures the appropriate security of the data by neglecting to install signs regarding phone use in the monitoring rooms in [redacted] monitoring centres; Failing to demonstrate that it carried out audits of the audit trails at [redacted] monitoring centres.
Section 72 of the 2018 Act	I have found the Council has infringed section 72(2) of the 2018 Act by failing to demonstrate that it took reasonable steps to bring to the employees' or agents' attention working in the monitoring centres about necessary security measures such as not using phones to record monitoring screens in the monitoring rooms.
Section 75 of the 2018 Act	I have found the Council has infringed section 75(3) by failing to implement a data protection policy in respect of its: Processing operations at [redacted] monitoring centres; Use of CCTV and ANPR until 15th July 2018; Use of drones until 8th November 2018 I have found the Council has infringed section 75(1) of the 2018 Act by failing to have a measure in place which requires an operative of the monitoring centre to be present when a visit of a Garda member or an authorised officer takes place.
Section 82 of the 2018 Act	I have found the Council has infringed section 82(2) of the 2018 Act by not having access logs in place at [redacted] monitoring centres which permitted the identification of persons who accessed the CCTV footage. I have found the Council has infringed section 82(1) by not maintaining access logs in recording the site visits made by the Garda member from Roxboro Road Garda Station and various Garda teams at [redacted] monitoring centre.
Section 71(8) of the 2018 Act	I have found the Council has infringed section 71(8) by failing to ensure it observed the time limit for deleting personal data at [redacted] monitoring centre.
Article 15 of the GDPR	I have found the Council has infringed Article 15 by rejecting subject access requests in respect of processing at the Traffic Management Centre.

7.2 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 8 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.	Finding Number	Action	Time Scale
1.		CCTV Cameras located at the 'Smarter Travel' Walkway 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 the 'Smarter Travel' Walkway. I impose a temporary ban on the Council's use of CCTV at this location. This processing must not resume unless, and until, there is a basis for it in EU or Member State Law, 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. I find that there is no lawful basis for the Council providing An Garda Síochána with a live feed to the 'Smarter Travel' Walkway CCTV cameras. I impose a temporary ban on the Council providing this live feed to An Garda Síochána. The provision of the live feed should 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	The Council is required to confirm to the Data Protection Commission within 90 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.

		section 38(3)(c) of the 2005 Act that regulates such processing in accordance with Article 8(2) of the LED.	
2.		Traffic Management CCTV Cameras at City Hall, Limerick 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 for traffic management purposes. This processing must not resume unless, and until, there is a basis for it in EU or Member State Law, for example an Act of the Oireachtas that regulates such processing 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 to An Garda Síochána. The provision of the live feed should 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.	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.
3.		CCTV cameras installed by the Estate Management Unit of the Council in Banogue, Garryowen, Deebert (Kilmallock), Lee Estate, Lismakeera (Askeaton),	The Council is required to confirm to the Data Protection Commission within 90 days of receiving this Decision that the cameras are switched off,

		Churchview (Askeaton), Old Cratloe Road, Altimira, Bruff Playground, The Banks (Kings Island), Cluain Dubh, Abbeycourt Estate Rathkeale, Lord Edward Street Development, Riverview Estate Kilmallock, Watergate, Clonlong, Kilmallock Road, Sharwood & Castleview Estates Newcastle West, Fr. Casey Close and Abbeyfeale. CCTV cameras installed by the Housing and Halting Site Maintenance Section of the Council at Dublin Road Halting Site, Clondrinagh Halting Site, Rhebogue Halting Site, Rathkeale, Rathbane Depot and Clonlong. 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 the abovementioned locations. 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 such processing in accordance with Article 8(2) of the LED.	unless another legal basis for the processing can be pinpointed in the meantime.
4.		CCTV cameras at Mt. St. Lawrence Cemetery 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 the abovementioned location. 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 such processing in accordance with Article 8(2) of the LED.	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.
5.		Smart CCTV Pilot Project across fourteen towns 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 Smart CCTV cameras at the fourteen towns apart from the 44 CCTV cameras which were authorised by the Garda Commissioner in the authorisation dated 11th December 2017. I impose a temporary ban on the Council's use of Smart CCTV cameras, in excess of the number authorised in the authorisation dated 11th December 2017, at these locations. This processing must not resume unless, and until, there is a basis for it in EU or Member State Law, for example an authorisation received from the Garda Commissioner pursuant to section 38(3)(c) of the 2005 Act that regulates such processing in accordance with Article 8(2) of the LED. I find there is no lawful basis for the Council's processing of personal data by means of ANPR technology at the fourteen towns	The Council is required to confirm to the Data Protection Commission within 90 days of receiving this Decision that the cameras (apart from the 44 authorised in the authorisation dated 11th December 2017) are switched off, unless another legal basis for the processing can be pinpointed in the meantime. In respect of any CCTV cameras which were authorised by the Garda Commissioner in the authorisation dated 11th December 2017 which have ANPR facilities, these ANPR facilities should be switched off within 90 days of receiving this Decision, unless another legal basis for the processing can be pinpointed in the meantime.

		which were part of the Smart CCTV Pilot Project. I impose an order requiring the Council to switch off the ANPR facilities on any cameras which were authorised by the Garda Commissioner in the authorisation dated 11th December 2017, unless another legal basis for the processing can be pinpointed in the meantime.	
6.		128 CCTV cameras linked to [redacted] monitoring centre capturing views from Ballynanty, Thomondgate, St. Mary's Park and Kileely providing real time surveillance at the time of the inspection. 64 cameras linked to [redacted] monitoring centre providing real time surveillance at the time of the inspection capturing views from [redacted], Carew Park, Weston and Rathbane. 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 the CCTV cameras at the abovementioned areas. I impose a temporary ban on the Council's processing of personal data with the 128 CCTV cameras linked to [redacted] monitoring centre and the 64 cameras linked to [redacted] monitoring centre at the time the inspections took place. This processing must not resume unless, and until, there is a basis for it in EU or Member State Law, for example an authorisation received from the Garda Commissioner pursuant to section 38(3)(c) of the 2005 Act that regulates such processing in accordance with Article 8(2) of the LED.	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.

		I find that there is no lawful basis for the Council to conduct targeted surveillance of individuals on behalf of the Garda Síochána from [redacted] monitoring centres. I impose a temporary ban on the Council conducting targeted surveillance of individuals. This targeted surveillance 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 8(2) of the LED.	

ii. <u>Transparency</u>

No.	Finding Number	Proposed Action	Proposed Time Scale
7.		Traffic Management CCTV Cameras at City Hall, Limerick Article 12(1)/Article 13 GDPR I order the Council to bring its processing by means of CCTV cameras into compliance with Articles 12(1) and 13 of the GDPR by ensuring that all data subjects are provided with all the information required by Article 13 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. A reference to 'Limerick.ie' (the Council's website) must be included on the signs. The Council is required to update 'Limerick.ie' by making the	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 7 must be complied with.

		information required by Article 13 easily accessible to data subjects. This could be achieved by placing in an easily accessible location of the website a detailed CCTV policy which gives information on the locations of the CCTV cameras and the relevant information required by Article 13.	
8.		Transparency for Law Enforcement CCTV Cameras referred to at Numbers 1, 3,4, and 6 of this table Sections 90(1) and 93(1) of the 2018 Act I order the Council to bring its processing by means of CCTV cameras used primarily for the purposes of law enforcement into compliance with sections 90(1) and 93(1) of the 2018 Act by ensuring that all data subjects are provided with all the information required by section 90 of the 2018 Act. This may be achieved by installing signage in the vicinity of where the CCTV cameras are operating which gives data subjects advanced notice of the processing, the purposes of the processing and the identity of the controller. A reference to 'Limerick.ie' (the Council's website) must be included on the signs. The Council is required to update 'Limerick.ie' by making the information required by section 90 easily accessible to data subjects. This could be achieved by placing in an easily accessible location of the website a detailed CCTV policy which gives information on the locations of the CCTV cameras and the	If the Council identifies an appropriate legal basis and intends to recommence processing personal data with CCTV cameras used primarily for law enforcement purposes, prior to commencing processing Order 8 must be complied with.

		relevant information required by section 90.	
9.		Transparency for Drones Section 90 and 93(1) of the 2018 Act I order the Council to bring its processing by means of drones used primarily for the purposes of law enforcement into compliance with section 90(1) of the 2018 Act by ensuring that all data subjects are provided with all the information required by section 90 of the 2018 Act. The Council is required to update 'Limerick.ie' by making the information required by section 90 easily accessible to data subjects. This could be achieved by placing in an easily accessible location of the website a detailed Drones policy which gives information on the locations where drones will be operated and the relevant information required by section 90.	If the Council intends to recommence processing personal data with drones used primarily for law enforcement purposes, prior to commencing processing Order 9 must be complied with.

iii. <u>Joint Controller Agreement</u>

No.	Finding Number	Proposed Action	Proposed Time Scale
10.		Joint Controller Agreements for CCTV cameras Section 79 of the 2018 Act I order that the Council make a joint controller agreement with An Garda Síochána governing their respective responsibilities under section 79 of the 2018 Act in respect of the CCTV cameras at the 'Smarter Travel' Walkway, the CCTV cameras which were subject to surveillance at [redacted] monitoring centres at the	If the Council identifies an appropriate legal basis and intends to recommence processing personal data with the described CCTV cameras, prior to commencing processing Order 10 must be complied with. In respect of the CCTV cameras which form part of the Smart CCTV Pilot Project and were authorised by the Commissioner on 17th December 2021 the Council has 90 days from the date of

		time of the inquiry and the CCTV cameras which formed part of the Smart CCTV Pilot Project.	this Decision to enter a joint controller agreement with An Garda Síochána.

iv. Processing Agreement

No.	Finding Number	Proposed Action	Proposed Time Scale
11.		Processing Agreement with [redacted] Section 80 of the 2018 Act I order that the Council make a processing agreement with [redacted] in writing which includes all the information required by section 80 of the 2018 Act.	If the Council identifies an appropriate legal basis and intends to recommence processing personal data with the CCTV cameras which were the subject of surveillance by [redacted] monitoring centres, prior to [redacted] recommencing monitoring of the cameras, the Council is required to make a processing agreement in writing with [redacted].

v. Technical and Organisational Measures/Data Protection Impact Assessments

No.	Finding Number	Proposed Action	Proposed Time Scale
12.		Data Protection Impact Assessments/Technical and Organisational Measures [redacted] monitoring Centres/ Training Measures Sections 84, 76 and 72(2) of the 2018 Act I order the Council to carry out a DPIA in respect of CCTV cameras which were subject to surveillance at [redacted] monitoring centres in accordance with section 84 of the 2018 Act in advance of recommencing processing. I order the Council to integrate appropriate technical and organisational measures as required by section 76 of the	If the Council identifies an appropriate legal basis and intends to recommence processing personal data with the CCTV cameras which were the subject of surveillance by [redacted] monitoring centres, prior to recommencing processing the Council is required to comply with Order 12.

		2018 Act in respect of the CCTV cameras which were subject to surveillance at [redacted] monitoring centres. These technical and organisational measures could include privacy masking and/or preventing manual control of the CCTV cameras by operators of the monitoring centres. I order the Council to implement appropriate procedures and training measures for staff working in the monitoring centres so as to promote compliance with the 2018 Act.	
13.		Data Protection Impact Assessments at Dublin Road Halting Site, Clondrinagh Halting Site, Rhebogue Halting Site, Rathkeale, Rathbane Depot, Clonlong Halting Site, Lord Edward Street Development, Section 84 of the 2018 Act I order the Council to carry out a DPIA in respect of CCTV cameras at these locations in advance of recommencing processing.	If the Council identifies an appropriate legal basis and intends to recommence processing personal data with the CCTV cameras at these locations, prior to recommencing processing the Council is required to comply with Order 13.
14.		Security Measures in relation to Traffic Management Cameras at City Hall I order the Council to bring its processing into compliance with the GDPR by requiring the controller to ensure persons who access personal data leave their identity and the purpose for which they accessed the data in the log book. I order the Council to implement a security measure at the corridor window of the Traffic	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 14 must be complied with.

		Management Centre in City Hall to prevent passersby from viewing the CCTV monitoring screens in accordance with Article 32(1) of the GDPR.	
15.		Security measures at [redacted] monitoring centres Sections 71(1)(f), 72(2), 82(2), 82(1) I order the Council to install signs prohibiting staff from using their phones or other devices to take pictures or video or audio recordings of the CCTV monitoring screens in the monitoring centres to ensure compliance with section 71(1)(f) of the 2018 Act. I order the Council to bring its processing into compliance with section 82(2) of the 2018 Act by requiring the controller to ensure persons who access personal data 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 which were monitored via [redacted] monitoring centres at the time of the inquiry, prior to commencing processing Order 15 must be complied with.
16.		Garda Communications Officer access to CCTV cameras Section 71(1)(a) of the 2018 Act I order the Council to remove access by the Garda Communications Officer based in Henry Street Garda Station to the thirty nine CCTV cameras at Banogue, Garryowen, Deebert (Kilmallock), Lee Estate, Lismakeera (Askeaton), Churchview (Askeaton), Old	The Council is required to confirm to the Data Protection Commission within 90 days of receiving this Decision that the access to the Garda Communications Officer has been removed.

		Cratloe Road, Altimira, Bruff Playground, The Banks (Kings Island) and Cluain Dubh.	
17.		Garda Communications Officer access to CCTV cameras Section 71(1)(a) of the 2018 Act I order the Council to remove access by the Garda Communications Officer based in Henry Street Garda Station to the CCTV cameras in Castleconnell, Murroe, Patrickswell, Croom and Pallasgreen.	The Council is required to confirm to the Data Protection Commission within 90 days of receiving this Decision that the access to the Garda Communications Officer has been removed.
18.		Time Limits on the Storage of Personal Data Sections 71(8) and 71(1)(c) of the 2018 Act I order the Council to delete personal data captured by CCTV cameras monitored via [redacted] monitoring centre after 30 days in accordance with its own data retention policy.	The Council is required to confirm to the Data Protection Commission within 45 days of receiving the final Decision that this 30 day retention policy is being adhered to.
19.		Data Protection Impact Assessment Smart CCTV Pilot Project Section 84 of the 2018 Act I order the Council to complete a revised DPIA in respect of the cameras installed pursuant to the Smart CCTV Pilot Project. If in light of the DPIA the Council is of the view some of the cameras installed are not proportionate and necessary for their intended purposes the Council should switch off these cameras.	The Council is required to confirm that a revised DPIA has been carried out within 90 days from the date of this Decision for the 44 CCTV cameras authorised by the Garda Commissioner in the authorisation dated 11th December 2017. If the Council identifies a legal basis to install more cameras under the Smart CCTV project (such as a further authorisation from the Garda Commissioner under section 38(3)(c) of the 2005 Act) a revised DPIA must be completed in advance of commencing such processing.
20.		Data Protection Impact Assessment Drones	N/A

		Section 84 of the 2018 Act I order the Council to complete a revised DPIA in advance of recommencing processing of personal data with drones.	

vi. Miscellaneous

No.	Finding Number	Proposed Action	Proposed Time Scale
21.		Failure to ensure the Data Protection Officer was consulted in a timely manner prior to installing a CCTV system at Clonlong/Failure to complete a DPIA in advance of installing a CCTV system at Clonglong Sections 88(4)(c) and 84 of the 2018 Act I issue a reprimand to the Council for failing to ensure that the Data Protection Officer was involved in a timely manner in installing the CCTV system at Clonlong. I issue a reprimand to the Council for failing to carry out a DPIA in advance of installing a new CCTV system in Clonlong.	N/A
22.		Drones Policy Section 75(3) of the 2018 Act I issue a reprimand to the Council for failing to publish a data protection policy on drones prior to conducting surveillance with drones for law enforcement purposes.	N/A

8. Decision to Impose an Administrative Fine

8.1 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.

8.2 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.[62] 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 5(1)(a), 12(1), 13(1), 13(2), 13(3) and 15 of 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) <u>Article 5(1)(a):</u> Lack of lawful basis for processing of personal data by way of traffic management cameras in public places and for sharing a live feed of the cameras with members of An Garda Síochána

8.3 The requirement on a controller to demonstrate that it has a lawful basis to process personal data is a fundamental requirement of the GDPR. A clear, precise and foreseeable legal basis upholds persons' fundamental right to the protection of their personal data under Article 8 of the Charter of Fundamental Rights of the European Union in ensuring the data is not processed in an arbitrary or abusive manner. It is a necessary counterweight on the power of the state and private entities.

8.4 Accordingly, the Council's infringement of Article 5(1)(a) of the GDPR in failing to demonstrate that it has a lawful basis for the processing of personal data by way of traffic management CCTV cameras and for sharing it with a third party is of a serious nature and gravity. The infringement is of a significant duration continuing from the date the GDPR came into effect on 25th May 2018 at least until the inquiry report was completed on 11th November 2019 (I do acknowledge on receipt of the inquiry report the Council indicated in its submissions that it had discontinued the live feed to Henry Street Garda Station).

8.5 The nature and scope of the processing are broad. The twenty-six cameras are based in a central location in Limerick City and these cameras would have processed a voluminous quantity of personal data. It follows from the fact that the CCTV cameras were shared with Henry Street Garda Station that up to six-hundred members had access to the personal data despite not having a lawful basis to do so.

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

8.6 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) <u>Articles 13(1), 13(2), 13(3):</u> Lack of signage and general transparency in relation to the Council's use of CCTV cameras for traffic management purposes

8.7 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.

8.8 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 either via signage or on the Council's website.

8.9 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 of the GDPR. The Council has failed, at the time the personal data was processed to provide:

- the identity and contact details of the controller;[63]
- the contact details of the data protection officer;[64]
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;[65]
- the period for which personal data will be stored (or at least the criteria which will be used to determine this period);[66]
- the existence of the right to request from the controller access to and rectification or erasure of personal data;[67]
- the right to lodge a complaint against a supervisory authority.[68]

8.10 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.

[63] GDPR, Article 13(1)(a).
[64] GDPR, Article 13(1)(b).
[65] GDPR, Article 13(1)(c).
[66] GDPR, Article 13(2)(a).
[67] GDPR, Article 13(2)(b).
[68] GDPR, Article 13(2)(d).

8.11 The infringement is of a significant duration continuing from the date the GDPR came into effect on 25th May 2018 at least until the inquiry report was completed on 11th November 2019.

8.12 The nature and scope of the processing are broad. The twenty-six cameras are based in a central location in Limerick City and these cameras would have processed a voluminous quantity of personal data. It follows from the fact that the CCTV cameras were shared with Henry Street Garda Station that up to six-hundred members had access to the personal data.

iii) Article 12(1): Failure to take appropriate measures to make the information in the Draft CCTV policy transparent and easily accessible

8.13 The Council's CCTV inventory dated 8th February 2019 notes the CCTV cameras monitored in Limerick city centre were installed for the purposes of 'traffic management'. The Council's draft CCTV policy covers CCTV cameras which have as their purpose to promote 'traffic management'. This policy is thus capable of covering the Council's use of CCTV cameras for traffic management purposes.

8.14 The nature of the infringement of Article 12(1) is moderate. As discussed earlier in this Decision, when I visited the Council's website (www.limerick.ie/council) there was no visible link to the Council's draft CCTV policy. I did find a generic privacy statement for the Council which gave the Data Protection Officer's email address.[69] There was also a section on the privacy statement entitled 'Detailed Privacy Statements in relation to specific Council Services'. This, however, did not contain any reference to the Council's CCTV policy.

8.15 The layout of the Council's website did not make the draft CCTV policy easily accessible for data subjects. In including links to other data protection policies in this section, but not to the Council's draft CCTV policy, the lack of transparency is aggravated. A data subject on visiting this section of the website and in reading these data protection policies which make no reference to the Council's processing operations by CCTV cameras, it may be reasonable for a data subject to conclude in the circumstances that the Council is not the controller of CCTV cameras. This is compounded by the lack of signage notifying data subjects the Council is the controller of these cameras.

8.16 As discussed earlier in this Decision, I did not end my search here but I then decided to conduct a Google Search using the search phrase 'limerick city and county council cctv policy'. I found a document entitled "*Limerick City and County Council CCTV Policy*"[70] in draft form. The reason why I am classifying the Council's infringement of Article 12(1) as moderate as opposed to severe, is that this policy was available to data subjects if they conducted a specific Google Search for the Council's CCTV policy.

[69] Privacy Statement for Limerick City and County Council < https://www.limerick.ie/council/services/your-council/privacy-statement-limerick-city-and-county-council> first accessed on 5th August 2021.
[70] <https://www.limerick.ie/sites/default/files/media/documents/2019-12/Draft%20CCTV%20Policy.pdf> first accessed on 5th August 2021.

The fact that such a search was needed to find the policy is indicative of a lack of transparency on the Council's part. The need to use a key word search on a search engine to find the policy also means the policy cannot be considered easily accessible.

8.17 The Council's failure to specifically signpost in the draft CCTV policy that it was the controller of the twenty six traffic management cameras in the city centre and the Council's failure to specify the locations of the cameras infringes Article 12(1) of the GDPR. The opacity in the policy on these points means the Council has failed to fulfil the requirements of the principle of transparency when processing personal data.

8.18 The infringement is of a significant duration continuing from the date the GDPR came into effect on 25th May 2018 until the date of this Decision.

8.19 The infringements pertain to the Council's failure to transparently provide the information required by Article 13 in the Council's CCTV policy and to make such a policy easily accessible. The twenty-six cameras are based in a central location in Limerick City and these cameras would have processed a voluminous quantity of personal data. It follows numerous data subjects who had their data processed by the CCTV cameras would have suffered damage as a result of not being able to access the Council's draft CCTV policy, which could have been avoided if it were more easily available.

iv) <u>Article 15:</u> Rejection of subject access requests at traffic management centre

8.20 The Council's infringement of Article 15 of the GDPR can be characterised as serious in nature. The reason for this is that the Council failed to provide any of the information required to be given to data subjects by Article 15. The Council infringed the requirement to give the data subject a copy of the personal data where that was available

8.21 It was a general practice of the manager of the traffic management centre to reject all subject access requests. This suggests a number of data subjects were prevented from exercising their rights under Article 15. The twenty-six CCTV cameras would have captured a considerable volume of personal data. It follows that potentially a large number of data subjects were affected by the practice of the manager of the traffic management centre to refuse data subject access requests.

v) <u>Article 32(1)</u>Traffic Management CCTV cameras: Lack of detailed access log/ lack of adequate security measure

8.22 The nature of the infringement of Article 32(1) by not maintaining an access log which contains specific details of the identity of the Garda member and the purpose for which the personal data was accessed is a moderate infringement of the GDPR. An access log is essential to ensure the purpose limitation principle is being adhered to and that personal data is being processed lawfully. As Henry Street Garda Station had some form of an access log, the infringement constitutes a moderate, rather than a severe, infringement on the spectrum.

8.23 The failure to implement appropriate security measures at the corridor window constitutes a minor infringement of Article 32(1) of the GDPR. A limited number of passersby would have been able to see the monitoring screens and likely only for a short duration.

(b) the intentional or negligent character of the infringement;

i) <u>Article 5(1)(a):</u> Lack of lawful basis for processing of personal data by way of traffic management cameras in public places and for sharing a live feed of the cameras with members of An Garda Síochána

8.24 The operation by the Council of traffic management cameras at City Hall, Limerick City, without a lawful basis was not of an intentional or negligent character. As submitted by the Council, prior to the inquiry being conducted, the Council believed that section 65 of the Local Government Act 2001 and section 37(1) of the 2005 Act provided a general lawful basis for the processing of personal data by way of CCTV cameras. In this Decision, I have found that section 65 of the Local Government Act 2001 and section 37(1) of the 2005 Act do not provide a lawful basis for the processing of personal data by CCTV cameras in public places. However, I acknowledge the Council had no knowledge that section 65 and section 37(1) did not provide a valid lawful basis prior to the inquiry.

8.25 The infringement of Article 5(1)(a) of the GDPR by providing a live feed to members of An Garda Síochána at Henry Street Garda Station without a legal basis could also be said to not be negligent or intentional for the same reason.

ii) <u>Articles 13(1), 13(2) and 13(3):</u> Lack of signage and general transparency in relation to the Council's use of CCTV cameras for traffic management purposes

8.26 I find the Council's infringement of Article 13 of the GDPR was of a negligent character. The Council has provided no explanation for its failure to erect signage in respect of the CCTV cameras. Even if there was a sign in place referring to the Council's draft CCTV Policy, the Council was negligent in failing to specify the policy covered the traffic management cameras in issue by neglecting to include a reference to the locations of the cameras in the draft CCTV policy.

iii) <u>Article 12(1):</u> Failure to take appropriate measures to make the information in the Draft CCTV Policy transparent and easily accessible

8.27 I find the Council's infringement of Article 12(1)(a) was of a negligent character. The Council has provided no explanation for why the draft CCTV policy was not included on the same section of the website with the other data protection policies.

iv) <u>Article 15:</u> Rejection of subject access requests at traffic management centre

8.28 I find the Council's rejection of subject access requests at the traffic management centre was of an intentional character. The subject access requests were not rejected by the manager of the traffic management centre due to inadvertence or negligence, but rather due to a wilful act. It was the practice of the traffic management centre to reject all subject access requests.

v) <u>Article 32(1)</u> Traffic Management CCTV cameras: Lack of detailed access log/ lack of adequate security measure

8.29 The Council was negligent in giving a live feed to Henry Street Garda Station without having a valid lawful basis to do so. As the traffic management CCTV cameras were not authorised pursuant to section 38 of the 2005 Act, the Council was under no legal obligation to share the footage taken by the cameras with An Garda Síochána. However, as An Garda Síochána was responsible for managing the access log, my view is that the Council bears limited culpability for the failure to maintain a detailed access log in Henry Street Garda Station.

8.30 In respect of the lack of an adequate security measure at the corridor window by the Council, this seems to be a genuine oversight and the Council bears a limited degree of negligence for failing to erect such a measure.

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

i) <u>Article 5(1)(a):</u> Lack of lawful basis for processing of personal data by way of traffic management cameras in public places and for sharing a live feed of the cameras with members of An Garda Síochána

8.31 I note in the Council's submissions made on receipt of the Draft Decision, the Council confirmed that this live feed has been disconnected. Although I welcome this submission, this action relates to the duration of the infringement, rather than action taken to mitigate damage already suffered by data subjects.

.ii) <u>Articles 13(1), 13(2) and 13(3):</u> Lack of signage and general transparency in relation to the Council's use of CCTV cameras for traffic management purposes

8.32 I note in the Council's submissions made on receipt of the Draft Decision, the Council noted it had erected the necessary signage in respect of the CCTV cameras. Although I welcome this submission, this action relates to the duration of the infringement, rather than action taken to mitigate damage already suffered by data subjects.

8.33 I acknowledge the Council has a general Privacy Statement on its website which gives the identity of the controller and the contact details of the Data Protection Officer[71] and also a draft CCTV Policy which was publically available.[72] However, at the time the personal data was processed there was no visible indicator, which would allow the data subject to form a nexus that the Council was the controller of the cameras and that his or her rights under Article 13 could be exercised by contacting the Data Protection Officer of the Council. Nonetheless, the draft CCTV Policy, in particular,[73] amounts to a *bona fide* attempt by the Council to address its obligations under Article 13 in respect

[71] https://www.limerick.ie/council/services/your-council/privacy-statement-limerick-city-and-county-council accessed on 27 September 2021.

[72] Limerick City and County Council, Draft CCTV Policy (V O.12 09/12/2019) page 15 accessed on 10th August 2021.

[73] I find the general Privacy Statement has little weight as a mitigating factor as it provides sparse information on the Council's use of CCTV cameras.

of the CCTV cameras it was the controller for. Accordingly, I find the existence and publication of the draft CCTV policy to be a mitigating factor.

iii) <u>Article 12(1):</u> Failure to take appropriate measures to make the information in the Draft CCTV Policy transparent and easily accessible

8.34 Although, the draft CCTV policy was not easily accessible, it could be accessed by a data subject on entering the correct search terms on an online search engine. I find the act of the Council making the policy publically available constitutes a mitigating factor.

iv) <u>Article 15:</u> Rejection of subject access requests at traffic management centre

8.35 The Council in its submissions on receipt of the inquiry report submitted: '*During all this period, to date, applications for access to personal data, including that contained on CCTV footage, received from data subjects, have been directed to and dealt with by the relevant Data Protection Officer. Should any particular Department have refused access to personal data, contrary to the data subjects' rights under data protection legislation, this issue would have been resolved through the Council's management structure.*'

8.36 It is my view, the Council in its submissions has not demonstrated it has taken any action which could have mitigated the effects of the infringement of Article 15.

v) <u>Article 32(1)</u> Traffic Management CCTV cameras: Lack of detailed access log/ lack of adequate security measure

8.37 Following the inquiry, the Council has discontinued the live feed to Henry Street Garda Station from the traffic management centre. The Council has also expressed willingness to erect an adequate security measure outside the traffic monitoring room at City Hall. However, as the Council is legally obliged to adopt these positions, they cannot be given credit as mitigating factors.

(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;

8.38 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

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

8.39 The Council has no previous infringements since the GDPR came into effect on 25th 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;

i) <u>Article 5(1)(a):</u> Lack of lawful basis for processing of personal data by way of traffic management cameras in public places and for sharing a live feed of the cameras with members of An Garda Síochána

8.40 The Council has co-operated with the Data Protection Commission by discontinuing the live feed to Henry Street Garda Station. This cannot be taken into account as a mitigating factor, as the Council is under a legal obligation to ensure it has a lawful basis for the processing of personal data via CCTV cameras.

ii) Articles 13(1), 13(2) and 13(3): Lack of signage and general transparency in relation to the Council's use of CCTV cameras for traffic management purposes

8.41 The Council has co-operated with the Data Protection Commission by agreeing to erect signage in the vicinity of the traffic management cameras. However, as the Council is under a legal obligation to do this by virtue of Article 13 of the GDPR I cannot take this into account as a mitigating factor.

iii) Articles 12(1): Failure to take appropriate measures to make the information in the Draft CCTV policy transparent and easily accessible

8.42 As already referred to above, I find the act of the Council making the policy publically available constitutes a mitigating factor.

iv) Article 15: Rejection of subject access requests at traffic management centre

8.43 There is no evidence of any actions taken by the Council which would act as a mitigating or aggravating factor in respect of this infringement.

v) Article 32(1)Traffic Management CCTV cameras: Lack of detailed access log/ lack of adequate security measure

8.44 As mentioned above, the Council has discontinued access to Henry Street Garda Station and has expressed its willingness to erect the required security measure outside the traffic monitoring room at City Hall. However, as the Council is legally obliged to take these actions, I can give these actions little credit as mitigating factors.

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

8.45 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.*'[74]

8.46 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.

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

(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;

8.47 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 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;

8.48 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

8.49 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.

i) <u>Article 5(1)(a):</u> Lack of lawful basis for processing of personal data by way of traffic management cameras in public places and for sharing a live feed of the cameras with members of An Garda Síochána

8.50 I can identify no other aggravating or mitigating factor in respect of this infringement.

ii) <u>Articles 13(1), 13(2) and 13(3):</u> Lack of signage and general transparency in relation to the Council's use of CCTV cameras for traffic management purposes

8.51 I can identify no other aggravating or mitigating factor in respect of this infringement.

iii) <u>Articles 12(1):</u> Failure to take appropriate measures to make the information in the Draft CCTV Policy transparent and easily accessible

8.52 I can identify no other aggravating or mitigating factor in respect of this infringement.

iv) <u>Article 15:</u> Rejection of subject access requests at traffic management centre

8.53 I can identify no other aggravating or mitigating factor in respect of this infringement.

<u>v) Article 32(1)</u>Traffic Management CCTV cameras: Lack of detailed access log/ lack of adequate security measure

8.54 I can identify no other aggravating or mitigating factors in respect of these infringements.

B. Decision to Impose an Administrative Fine

Methodology

8.55 In the absence of specific EU-level guidelines on the calculation of fines, I am not bound to apply any particular methodology.[75] In practical terms, this means that I am not bound to use a base figure or fixed financial starting point for the assessment of the fine. Therefore, in calculating the fine I will identify the amount of the administrative fine to be imposed on the Council on a general basis and by reference to the factors to which I am required to have due regard in accordance with Article 83(2) and which I have already applied to the circumstances of this case in detail above. In doing so, I must also ensure that, in accordance with the obligation on supervisory authorities under Article 83(1), the administrative fine imposed in this case is effective, proportionate and dissuasive.

8.56 In considering the application of the principles of effectiveness, proportionality and dissuasiveness of the administrative fine, I consider that a fine cannot be effective if it does not have significance relative to the financial resources of the data controller. Moreover, the principle of proportionality cannot be adhered to if the infringement is considered in the abstract, regardless of the impact on the controller. This is compounded by the fact that future infringements need to be deterred. In this regard, I consider that a fine cannot be dissuasive if it will not be of any financial significance. I am bound by the fining cap stated in section 141(4) of the 2018 Act in respect of imposing fines on local authorities.

8.57 The Draft Decision set out a proposed range for the administrative fine and the factors to be considered, and the methodology to be used when calculating the fine, in order to provide the Council with the opportunity to comment in accordance with fair procedures. The Council made various submissions in respect of Draft Decision as I outlined in the above paragraphs. The Council did not make any comments on the quantum of the fine but it did make a number of submissions in relation to my views that Article 15 of the GDPR had been infringed by failing to process subject access requests in the Traffic Management Centre. I have not changed my view that Article 15 has been infringed, as I outlined above.

a) Decision to impose an administrative fine for each infringement

i) <u>Article 5(1)(a):</u> Lack of lawful basis for processing of personal data by way of traffic management cameras in public places and for sharing a live feed of the cameras with members of An Garda Síochána

8.58 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 5(1)(a) of the

[75] See by analogy Case T 332/09, *Electrabel v Commission,* judgement of 12 December 2012 (ECLI:EU:T:2012:672), paragraph 228; Case T-704/14, *Marine Harvest ASA v Commission*, judgement of 26 October 2017 (ECLI:EU:T:2017:753), paragraph 450.

GDPR by processing personal data by way of traffic management cameras in public places and for sharing a live feed of the cameras with members of An Garda Síochána without having a lawful basis to do so. The fact the Council had a genuine belief at the time the inquiry was conducted that it did have a lawful basis for operating CCTV cameras pursuant to section 65 of the Local Government Act 2001 led me to the conclusion it would be disproportionate to impose a fine for the infringement.

ii) <u>Articles 13(1), 13(2) and 13(3):</u> Lack of signage and general transparency in relation to the Council's use of CCTV cameras for traffic management purposes

8.59 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.

8.60 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), (2) 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.

8.61 Although, the Council's draft CCTV policy does not fulfil the requirements of Articles 13(1), 13(2) and 13(3) of the GDPR, I accept it does constitute a mitigating factor, insofar as the Council made a *bona fide* attempt to satisfy the requirements of these provisions.

8.62 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 have also had regard to the weight of the Council's CCTV policy as a mitigating factor. I therefore consider that a fine of **€50,000** is appropriate in the circumstances of this case. I consider that this fine is an effective, proportionate and dissuasive figure as required by Article 83(1).

iii) <u>Article 12(1):</u> Failure to take appropriate measures to make the information in the Draft CCTV policy transparent and easily accessible

8.63 The infringement of Article 12(1) amounts to a moderate infringement, in that the Council fails to make its draft CCTV policy easily accessible and the fact that it is the controller of the twenty six traffic management cameras transparent. Although, the Council's draft CCTV policy does not fulfil the requirements of Article 12(1) of the GDPR, I accept it does constitute a mitigating factor, insofar as the Council made the draft CCTV policy publically available.

8.64 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 have also had regard to the Council's CCTV policy being publically

available as a mitigating factor. I consider that a fine of **€25,000** is appropriate in the circumstances of this case. I consider that this fine is an effective, proportionate and dissuasive figure as required by Article 83(1).

iv) Article 15: Rejection of subject access requests at traffic management centre

8.65 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 infringements of Article 15 of the GDPR.

8.66 In arriving at the decision to impose the fine, I have been particularly influenced by the intentional character of the infringement. The reason the subject access requests were not accepted, was not on the grounds of inadvertence, but rather due to a wilful decision of the manager of the traffic management centre. Furthermore, the blanket refusal to provide the information required by Article 15 of a serious gravity and a high level of severity.

8.67 Having considered the criteria under Article 82(2) and the fining cap I am bound by under section 141(4) of the 2018 Act, I have decided to impose a fine of **€35,000** on the Council for the infringement of Article 15 of the GDPR. I consider that this fine is an effective, proportionate and dissuasive figure as required by Article 83(1).

v) Article 32(1) Traffic Management CCTV cameras: Lack of detailed access log/ lack of adequate security measure

8.68 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 infringements of Article 32(1). The Council was negligent in sharing a live feed with An Garda Síochána of the traffic management cameras without having a lawful basis to do so. However, once the live feed was made available, it was outside of the Council's power to ensure an adequate access log was maintained at Henry Street Garda Station in accordance with Article 32(1) of the GDPR. Having regard to all the circumstances of this infringement, I do not consider it necessary to impose an administrative fine.

b) Total value of the proposed administrative fine

8.69 Article 83(3) of the GDPR states:

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

8.70 In a recent decision, the EDPB held that the reference to '*gravest infringement*' in Article 83(3) did not relate to gravest infringement identified in a particular inquiry, but rather referred to the fining caps referred to in Articles 83(4) and Article 83(5) of the GDPR.[76] Accordingly, as Decision Maker I am not restricted to only imposing an administrative fine for the most serious infringement of the GDPR in this case.

[76] Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR (Adopted on 28th July 2021).

8.71 Considering the severity of each of the infringements of the GDPR which in my view justify the imposition of administrative fines under Article 83 and considering the requirement under Article 83(1) for the administrative fines to be imposed to be '*effective, proportionate and dissuasive*' I am of the view it is necessary to impose the three administrative fines I listed above.

8.72 Therefore, the total quantum of the administrative fines that I impose is **€110,000**.

8.73 I consider that the above administrative fines cumulatively meet 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 infringements require significant fines in order 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 fines 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 fines do 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 fines would be effective, proportionate and dissuasive, taking into account all of the circumstances of the case.

9. Right of Appeal

9.1 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 the 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

10. Appendices

Materials considered

10.1 The Authorised Officers delivered the Inquiry Report to me on 11th November 2019. I was provided with all the submissions received in compiling the report including:

i. The completed Data Protection Audit Questionnaire;
ii. The revised Data Protection Audit Questionnaire;

iii. CCTV Inventory February 2019;
iv. Revised CCTV Inventory March 2019;
v. MCEC Monitoring Contract 2008;
vi. Pobal Letter Section 38(3)(c) scheme dated 2006;
vii. Garda Commissioner Authorisations under Section 38(3)(c) dated 19th September 2006, 5th March 2009 and 11th December 2017;
viii. Legal advice submitted by Council dated March 2019;
ix. Traffic Management Centre – Access Log;
x. SMART CCTV Project;
xi. Maps & images of locations (14 towns);
xii. DPIA (Smart CCTV Project);
xiii. Revised DPIA (Smart CCTV Project);
xiv. Draft data processor agreement with [redacted]
xv. Draft CCTV Policy dated 15th July 2018;
xvi. Draft Drone Policy dated 8th November 2018;
xvii. Submissions on Draft Inquiry Report dated 20th September 2019;
xviii. Submissions on Draft Inquiry Report dated 30th October 2019;
xix. Formal protocol for An Garda Síochána requests to access traffic management footage;
xx. Legal advice submitted to DPC by Council on 5th March 2019;
xxi. Copy of An Garda Síochána reply dated 17th May 2019;
xxii. Copy of email extract of 5th March 2019 re: An Garda Síochána access;
xxiii. Copy of Garda Authorisation dated 11th December 2017;
xxiv. Appendices submitted by Council in respect of Smart CCTV Project;
xxv. Smart CCTV Project – Table.
xxvi. Submissions on the Draft Decision dated 22nd November 2021 and appended correspondence.