An Coimisiún um Chosaint Sonraí
Data Protection Commission

Decision of the Data Protection Commission under Section 124 of the Data Protection Act 2018 in the Case of 01/SIU/2018

Own-Volition Inquiry under Section 123 Data Protection Act, 2018

on foot of Data Protection Audit Conducted under

Section 136 of the Data Protection Act 2018 regarding

CCTV Schemes Authorised under

Section 38(3)(a) of the Garda Síochána Act 2005

Commission Decision-Maker(s):

Helen Dixon (Commissioner for Data Protection), sole member of the Commission

Date of Decision: 23 August 2019

INDEX:

1. Background

Two officers of the Data Protection Commission ('DPC') were authorised on 14 June 2018 to conduct a connected series of own-volition inquiries under section 123 of the Data Protection Act 2018 ('the 2018 Act') into a broad range of issues pertaining to surveillance technologies deployed by State authorities, in particular An Garda Síochána ('AGS') and the various local authorities. In initiating the inquiries, the DPC wished:

- to establish whether any data processing that takes place in this context is in compliance with relevant data protection laws (considered in Section 2) and
- in advance of further investment and deployment of newer surveillance technologies, ensure that full accountability measures for the collection and processing of personal data are in place.

Surveillance in public places has the potential to affect most if not all persons in the State. A permanent tension exists between surveillance measures to deliver security versus other civil liberties such as the ability to go about one's daily business free from unnecessary supervision. In this State, the legislature has provided for a system of authorisation by AGS of CCTV schemes that are to operate in public places to help to deter, prevent, detect and prosecute offences. Thirty-eight schemes have been authorised by the Garda Commissioner under section 38(3)(a) of the Garda Síochána Act 2005 ('the 2005 Act').[1]

The inquiry leading to this decision was conducted initially by means of an audit under section 136 of the Data Protection Act 2018. This facilitated the DPC Authorised Officers in compiling facts in relation to the operational deployment of surveillance technologies under the various authorised schemes. The Authorised Officers made follow-up inspections at five selected Garda Stations (corresponding to four discrete approved CCTV schemes) over a four-week period commencing in mid-January 2019. In general, the technologies at issue in this report relate to CCTV live feeds and recording systems and to Automatic Number Plate Recognition Technology ("ANPR") linked to certain of those CCTV systems.

This decision makes findings only in relation to a some of the schemes authorised by the Garda Commissioner under section 38(3)(a) of the 2005 Act. The focus of this decision is on operational issues pertaining to the schemes as operated by AGS. The DPC did not examine either the criteria used to assess and approve the schemes nor whether the approval process administered by the Garda Commissioner was correctly the undertaken. As a consequence, this decision does not address these matters.

The Inquiry Report presents a range of issues by reference to four different approved CCTV schemes, namely those at Tullamore, Co Offaly, Limerick, Dublin South Central and Duleek and Donore, Co Meath. However, my decision is addressed to AGS as the relevant data controller for all four schemes rather than to the Garda "member in charge" at the individual locations of the schemes.

[1] Section 38(3) of the Garda Síochána Act 2005 Act, Security in Public Places, states that (3) Authorisation may be given to any or all of the following: (a) members of the Garda Síochána;

2. Applicable legal regime pertaining to the inquiry and this decision

The personal data processing identified in this inquiry is conducted by AGS for law-enforcement purposes.

2.1 Legal Basis – Applicable Regime

The General Data Protection Regulation ("GDPR") is the direct-effect legal regime covering the processing of personal data in the European Union. 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 …".* [emphasis added]

The Law Enforcement Directive, [Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016] is a *lex specialis* that provides specific rules relating to the protection of natural persons with regard 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, respecting the specific nature of those activities. It sets down specific measures for the protection of personal data including special categories of personal data in this law-enforcement context. It further lays down a range of general and more specific obligations on competent authorities with regard to technical and organisational measures. These include implementation of systems that deliver data protection by design and default and ensuring persons employed by the controller are aware of and comply with all of the relevant technical or organisational measures.

Section 69(1) of the 2018 Act defines "competent authority" as including:

> *"(a) a public authority competent for the prevention, investigation, detection or prosecution of criminal offences".*

It is clear from the functions prescribed to An Garda Síochána by section 7 of the Garda Síochána Act 2005,[2] that An Garda Síochána is a '*competent authority*' as envisaged by the GDPR and section 69(1) of the 2018 Act.

In these circumstances, the relevant legal framework for this decision is to be assessed by reference to the Law Enforcement Directive (EU 2016/680), as transposed into Irish law by Part 5 (sections 69 – 104) of the 2018 Act. As a consequence, the applicable corrective powers that apply in relation to any infringements identified in this decision are those set out at section 127 of the 2018 Act.

[2] Section 7(1) of the of the Garda Síochána Act 2005 Act states that the function of the Garda Síochána is to provide policing and security services for the State with the objective of a) preserving peace and public order, b) protecting life and property, c) vindicating the human rights of each individual d) protecting the security of the State e) preventing crime, f) bringing criminals to justice including by detecting and investigating crime, and g) regulating and controlling road traffic and improving road safety.

3. Materials Considered

The Final Report of Audit and Inquiry (the Inquiry Report) was received by me from the Authorised Officers on 22 July 2019. I was also provided with all of the submissions received in compiling the report including:

- the Draft ANPR Policy,
- the Draft ANPR Procedures Document,
- HQ Directive 55/2012, HQ Directive 82/2009,
- HQ Directive 157/2006,
- Code of Practice for CCTV Systems authorised under section 38(3)(c),
- Garda Síochána Act, 2005,
- CCTV Policy for Duleek & District Text Alert Community CCTV System and Duleek & District Text Alert Community, and
- CCTV System Privacy Impact Assessment

to which I have had regard in reaching my decision below.

I am satisfied, having reviewed the Inquiry Report, that the audit and inquiry were correctly conducted and that fair procedures were followed throughout including, but not limited to, notifications to the data controller and opportunity for the data controller to comment on a draft of the Inquiry Report before it was submitted to me as a decision-maker. In making my decision, I have remained open to the possibility of inviting further submissions from the controller on any areas concerning which I considered it fair to hear further from them. In the event, this was not necessary as the controller's response to the draft of the Inquiry Report indicated that AGS accepted the accurate factual representations contained in it and expressed its full commitment to addressing all of the issues identified. Finally, my findings do not depart significantly from the provisional positions identified by the Authorised Officers in this particular case.

4. Relevant Data Controller

This decision and the corrective measures imposed are addressed to An Garda Síochána as the relevant data controller in relation to the findings made. [3],[4]

Under section 38(3)(a) of the 2005 Act, the Garda Commissioner approves schemes, doing so on the basis of standardised criteria that AGS has devised under section 38(4) of that Act. Each scheme is intended to operate for the purposes provided for in section 38(1), namely "securing public order and safety in public places by facilitating the deterrence, prevention, detection and prosecution of offences". They are further subject to a standardised AGS Code of Practice for CCTV in Public Places. It is therefore AGS – rather than the 'member in charge' of any particular district – that controls the decisions on purposes and means of the personal data collection and processing that takes place through the deployment of surveillance technologies. This decision, as stated earlier, is for that reason properly addressed to AGS.

[3] Section 69. (1) of the Data Protection Act, 2018, Part 5 Processing of Personal Data for Law Enforcement Purposes states that - In this Part "competent authority", subject to subsection (2), means (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 (b) any other body or entity authorised by law to exercise public authority and public powers for the purposes of 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: "controller", subject to subsection (2), means (a) a competent authority that, whether alone or jointly with others, determines the purposes and means of the processing of personal data, or (b) where the purposes and means of the processing of personal data are determined by the law of the European Union or otherwise by the law of the State, a controller nominated (i) by that law, or (ii) in accordance with criteria specified in that law;

[4] Section 118 of the Data Protection Act, 2018, Chapter 3 Enforcement of Directive Interpretation states that "controller" and "processor" have the meanings they have in Part 5.

5. Personal Data

The technologies at issue in this decision relate to CCTV systems located in public places, some of which are connected to Automatic Number Plate Recognition Systems.

Personal data is defined in section 69 of the 2018 Act. [5]

Images of members of the public are therefore routinely collected and processed by these technologies. Given the ability of AGS to identify individuals from their images and even potentially their gait and shape where a person's face is not visible, the data obtained from CCTV footage constitutes personal data. The ANPR system photographs vehicle registrations and captures images of drivers and passengers, which means this system also entails the processing of personal data.

[5] Section 69 of the Data Protection Act, 2018, Part 5 Processing of Personal Data for Law Enforcement Purposes states that "personal data" means information relating to (a) an identified living individual, or (b) a living individual who can be identified from the data, directly or indirectly, in particular by reference to (i) an identifier such as a name, an identification number, location data or an online identifier, or (ii) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual

6. Analysis and Findings

The Authorised Officers identified a total of twenty-six issues in the course of their inquiry and inspections of the four schemes outlined above. I have considered each in turn and I also considered the commonality of issues identified across the schemes.

Accordingly, and given that AGS is the controller in each and all cases of the issues identified, I will group my analysis and findings in respect of the issues based on the nine unique matters identified in the Inquiry Report and now set out below.

6.1 Governance and Oversight

6.1.1: No restriction on bringing smart phones into CCTV monitoring rooms and excessive access to monitoring rooms.

Inquiry Report Issues: 1, 5, 11, 16 and 24.

A fundamental requirement of data protection legislation is that personal data is collected and processed in a manner than ensures appropriate security of the data and prevents unauthorised disclosure to third parties. This is explicitly provided for in section 71(1)(f) of the 2018 Act, which requires competent authorities to implement appropriate technical or organisations measures to protect against unauthorised processing and accidental loss, destruction or damage. The Authorised Officers identified, in relation to the schemes they physically inspected, that any staff (or contractors) who had access to the CCTV monitoring rooms could enter with their own personal smart phones or recording devices. The DPC is aware of at least one case of a complaint it investigated in recent years where a member of AGS took a recording of CCTV footage of a member of the public and may have circulated it to a WhatsApp group. This indicates that, where personal recording devices can be used in proximity to CCTV monitors, a risk that the personal data processed through the CCTV system may be unlawfully recorded and disclosed to unauthorised persons. However, the ubiquitous nature of personal smart devices that include recording equipment means that there are virtually no circumstances in which this risk does not now arise. Section 77(a) of the 2018 Act specifically requires competent authorities to "evaluate the risks to the rights and freedoms of individuals arising from the processing concerned". Paragraph (b) requires them to implement a range of protective measures. Subparagraphs (i) and (ii) of the latter envisage measures that would deny access to the processing equipment and that prevent the reading or copying of the data.

Proportionality

Section 75 of the Data Protection Act 2018[6]imposes "General obligations of controller with regard to technical and organisational measures". These include a clear accountability requirement under section 75(1)(b), obliging controllers to implement technological and organisational measures to demonstrate their compliance with these obligations. Controllers must ensure that measures they implement are kept under review "at regular intervals and, where required, updated". This can be particularly important in the context of fast-moving developments and social norms around personal devices. While section 75 relates to the General Obligations, sections 72 and 77 prescribe in further detail the actions that a controller must take to ensure security of processing. In the context of this decision, I have considered the proportionality of requiring a policy that would restrict the bringing of smart devices into an area where CCTV is being monitored by AGS. In the CJEU judgment in *Volker and Schecke*[7], the Court found that the principle of proportionality requires that the proposed measures is appropriate for attaining the objective pursued and does not go beyond what is necessary to achieve it.

[6] Section 75 of the Data Protection Act, 2018, General obligations of controller with regard to technical and organisational measures states that (1) A controller shall implement appropriate technical and organisational measures for the purposes of (a) ensuring that the processing of personal data for which it is responsible is performed in compliance with this Part, and (b) demonstrating such compliance. (2) A controller shall ensure that measures implemented in accordance with *subsection (1)* are reviewed at regular intervals and, where required, updated. (3) The measures referred to in *subsection (1)* shall include the implementation of an appropriate data protection policy by the controller, where such implementation is proportionate in relation to the processing activities carried out by the controller.

[7] Combined Cases Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen

Prohibiting use of personal devices

Clearly, the aim here is to ensure there is no unauthorised access to and dissemination of CCTV images under AGS control. I have considered, in the context of the means proposed by the Authorised Officers, that it would be impractical and extremely problematic to enforce a system of prohibiting those entering a monitoring room to have mobile telephones on their person. On the contrary, I consider the risk that arises can best be addressed by other means – for example, by a policy that explicitly prohibits use of (rather than the bringing of) personal audio or video recording devices into the area of the monitoring screens. Such a policy could be highlighted through signage at the entrance to the monitoring area. This type of policy operates in certain security areas of airports and rather than restricting the bringing of personal smart devices through the airports, it requires they remain unused in certain settings.

Access to screens

[redacted]

Again, the obligation under section 77[8] for competent authorities to undertake a risk evaluation exercise specifically requires a data controller, prior to carrying out automated processing to,

[8] Section 77 of the Data Protection Act, 2018, Security of automated processing states that a controller or processor, prior to carrying out automated processing, shall (a) evaluate the risks to the rights and freedoms of individuals arising from the processing concerned, and (b) implement measures designed to (i) deny access to the processing equipment used for the processing to any person other than the persons authorised in that regard by the controller or processor, as the case may be, (ii) prevent the reading, copying, modification or removal of the data media concerned, other than in so far as is authorised by the controller or processor, as the case may be, (iii) prevent the input of personal data other than in so far as is authorised by the controller or processor, as the case may be, (iv) prevent the inspection, modification or deletion of the data other than in so far as is authorised by the controller or processor, as the case may be, (v) prevent the use of the automated processing system by persons using data communication equipment who are not authorised to do so by the controller or processor, as the case may be, (vi) ensure that where a person is authorised to use the automated processing system concerned, he or she has access to personal data on the system only in so far as he or she is so authorised by the controller or processor, as the case may be, (vii) ensure that it is possible to verify or establish the persons to whom personal data have been or may be transmitted or made available using data communication equipment, (viii) ensure that it is possible to verify or establish which personal data have been input into an automated processing system, and in relation to such data, to verify and establish the person who input the data and when the data were input, (ix) prevent the reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media, other than in so far as is authorised by the controller or processor, as the case may be, (x) ensure that an installed automated system may be restored in the event of an interruption in the service of the system, (xi) ensure that the automated processing system properly performs its function and the appearance of a fault in

among other things, evaluate the risks to the rights and freedoms of individuals arising from the processing concerned. Such an evaluation will allow the controller to consider what measures are appropriate to implement under section 77(b) and may include, per section 77(b)(i), the denying of access to the processing equipment.

6.1.1 – Findings:

I find that the issue as identified by the Authorised Officers (failure to prevent the bringing of personal recording devices into monitoring areas) does not constitute an infringement of section 71(1)(f) of the 2018 Act. However, I find that, pursuant to its obligation under section 77(a) of the 2018 Act, AGS should give further consideration to the matter, evaluate the risk arising in light of previous incidents of which it is aware and implement a suitable policy and measures on this specific issue as appropriate in accordance with section 77(b).

[redacted]

From the evidence supplied by the Authorised Officers, I see nothing that demonstrates that AGS has taken account of section 77(a) of the 2018 Act in terms of the requirement to conduct an evaluation of the risks. AGS therefore cannot have implemented section 77(b), leading to a failure to take measures for the purpose of demonstrating its compliance with Part 5, as required by section 75(1)(b). I therefore find there is non-compliance with section 77 and section 75(1)(b).

the automated processing system is reported to the controller or processor, as the case may be, and (xii) ensure that personal data that are stored on the automated processing system cannot be corrupted by means of a malfunctioning of the system.

6.1.2: Governance issues in relation to access logs, auditing of access logs, record-keeping regarding downloads, excessive retention of footage, privacy by design and default and training of Garda members on the use of the Garda authorised CCTV systems:

Inquiry Report Issues: 1, 2, 5, 6, 10, 11, 12, 15, 16, 17, 19, 20, 21, 24, 25 & 26.

6.1.2 (a) Systems Access

The Authorised Officers identified a range of issues across the schemes where some CCTV systems appeared to have no capability to record access instances [redacted]. In other cases [redacted], the Authorised Officers identified that there was an electronic audit trail capability that can identify who has accessed the system and at what time by reference to individual Gardaí was in place, but there was no evidence of proactive auditing of the access logs such that improper use could be detected. It is clear from section 77 and in particular subsections (b)(vi) and (vii) that controllers must implement measures such that they know who is accessing their automated systems and can satisfy themselves that those persons have access only to the data that is strictly necessary. Further, section 75(2) requires regular review of the measures implemented, implying in this context that an auditing function is necessary.

In a further case, only one generic login to the access system existed with the log-on credentials posted on a whiteboard making it near impossible to identify who had accessed the system. In this particular scheme, there was in any case as set out at the top of this paragraph no capability to log individual access instances [redacted].

6.1.2 (b) Maintaining records of downloads

Further issues identified by the Authorised Officers related to a failure to maintain records of CCTV footage downloaded and reviewed by Garda members [redacted]. This is again a requirement under section 77 of the 2018 Act and in particular of subsection (b)(ix). Section 75 requires the controller to implement technical and organisational measures. Overall, there appears to be an inconsistency across the Garda stations inspected regarding the comprehensiveness of manual records kept.

6.1.2 (c) Training of staff

The absence of adequate records of downloads may be unsurprising given a further issue identified by the Authorised Officers. This concerned the absence of a training programme for members attached to the latter two schemes on use of the Garda authorised CCTV systems including reviewing and downloading of images and footage. Section 72(2) of the 2018 Act sets down a clear imperative for competent authorities to ensure that "persons employed by the controller are aware of and comply with the relevant technical or organisational measures". Such a level of awareness cannot typically be delivered without some form of training being implemented.

6.1.2 (d) Privacy by Design and Default

[redacted], specific issues around the design of the CCTV implementation were in evidence. Members operating the 'pan, tilt and zoom' cameras in this scheme appeared to routinely fail to manually return the cameras to their original focus; in some cases these were left directed at private homes in [redacted]. It is not clear if a technological solution to this issue was sought by AGS.

[redacted]

Section 76 of the 2018 Act clearly and specifically requires a controller to determine the means of and carrying out of processing, to implement appropriate technical and organisational measures that are designed to integrate necessary safeguards. Subsection (3) of section 76 makes this obligation clear and requires consideration of the amount and extent of personal data processed.

6.1.2 (e) Retention

The Authorised Officers also identified inconsistency in application of the AGS Code of Practice for CCTV in Public Places as regards retention of footage in the course of their inspections. [redacted] operates a 56-day retention policy rather than the 31 days set out in the Code. No justification was provided for this extended period (such as, for example, that the particular footage was required for a live investigation or prosecution). On the day of the Authorised Officers' inspection , CCTV footage that was 79 days old was identified. Section 76(3)(c) of the 2018 Act is clear that controllers must implement measures that take account of the necessity of personal data processing in the context of the period for which it is proposed to be stored. Section 71(1)(e) further explicitly provides that personal data shall be kept "no longer than is necessary for the purposes for which the data are processed". Failure to adhere to its own Code of Practice indicates that AGS is not complying with these provisions.

6.1.2 (f) Data-logging

Section 82 of the 2018 Act obliges data controllers to create and maintain a 'data log' in their automated processing systems such that, amongst other things, it can be ascertained when and if personal data was consulted by any person or whether personal data was disclosed or transferred to any other person. Subsection 4 requires the controller to make a data log available to the Data Protection Commission for inspection and examination if requested to do so.

Section 82(5) deals with automated systems that predate 6 May 2016 which appears to be the case for the CCTV schemes inspected by the Authorised Officers. In such circumstances, compliance with section 82 is not required in the first instance prior to 6 May 2023 but only where the controller can demonstrate it would involve disproportionate effort to implement the section.

In relation to the obligation for data logging under section 82 of the 2018 Act,[9], the following question was put to AGS in the initial Questionnaire and the response copied received.

> Q 41. Data logging for automated processing systems (in respect of an automated processing system established after 6 May, 2016) (Section 82):
>
> In relation to its law enforcement functions where personal data is processed through the use of CCTV systems, ANPR technology, Body Worn Camera technology or any other forms of technology that capture or record the images of individuals, please describe the data log that An Garda Síochána has created and maintained in order to comply with section 82 of the Data Protection Act, 2018.
>
> Reply: *It is a requirement under the Garda CCTV Code of Practice to have a manual audit trail in place for all CCTV downloads. No record is retained by the system where CCTV footage is reviewed Forms entitled 'Log of Review Request & CCTV Picture Prints & Copies of Recorded Footage', and 'Application for Copies of Recorded CCTV Footage Captured on Community Based CCTV Schemes' are employed for this purpose and both require that the PULSE ID number (if known) be recorded on the form.*

The DPC's overall reading of section 82 and Article 25 of the Directive[10] (from which section 82 derives) is that the logging required is electronic and automated in nature. This can be inferred from the first line of Article 25, which refers to logs in automated processing systems. I therefore find that the response from AGS, which details manual audit trails, does not meet nor even address the obligation under section 82.

Further, given the obligations set down in subsections 82(5)(a) and (b), the onus is on AGS to demonstrate either that disproportionate effort would be involved in complying with section 82 in advance of 6 May 2023 or that "serious difficulties for the operation of the automated

[9] Section 82 of the Data Protection Act, 2018 Data logging for automated processing system states that (1) Subject to *subsection (5)*, 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 (in this section referred to as a "data 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 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; (d) the erasure of the personal data, or some of the date.
Section 82 (5) of the 2018 Act states that his section shall not apply, in respect of an automated processing system established on or before 6 May 2016 (a) prior to 6 May 2023, where compliance by a controller or processor, as the case may be, with this section prior to that date would involve disproportionate effort, or (b) prior to 6 May 2026, where compliance by a controller or a processor, as the case may be, with this section prior to that date would cause serious difficulties for the operation of the automated processing system to which the data log relates.

[10] Article 25 of the Directive (EU) 2016/680 of the European Parliament and of the Council - Logging, states that (1) Member States shall provide for logs to be kept for at least the following processing operations in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination and erasure. The logs of consultation and disclosure shall make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data. (2) The logs shall be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings. (3) The controller and the processor shall make the logs available to the supervisory authority on request.

processing system" would arise if implemented earlier than 6 May 2026. In other words, the section intends that controllers will implement data logging in advance of the two dates set down above and that where they do not intend to implement before those dates, they must justify why in accordance with section 82(5). No such analysis nor justification has been presented by AGS.

6.1.2 General

In overall terms, the inquiry conducted by the Authorised Officers yields no evidence of AGS having considered and implemented the provisions of the LED as transposed by the 2018 Act in respect of the section 38(3)(a) CCTV schemes. Specifically, the AGS Code of Practice for CCTV in Public Places has remained unchanged since 2006 and does not appear to have been reviewed. Regarding systems identified in the Inquiry Report as lacking digital tracing of individual access, no plans to upgrade were conveyed to the Authorised Officers. Indeed, the Inquiry Report discloses no actions undertaken to account for the new legal framework for personal data with the exception of the appointment of a Data Protection Officer in 2018 and a Record of Processing Activities (ROPA) across AGS that was implemented the same year. The AGS circulars accompanying responses to the Authorised Officers' questionnaire seeking responses on foot of the audit all date back many years; nothing current and updated to take account of the 2018 Act was attached. Section 77(a) of the 2018 Act specifically requires competent authorities to "evaluate the risks to the rights and freedoms of individuals arising from the processing concerned", while paragraph (b) requires them to implement a range of protective measures.

6.1.2 Findings

I find that AGS is infringing a range of provisions under the Data Protection Act 2018, specifically:

6.1.2.(a): Section 75 of the 2018 Act - General obligations on controller with regard to technical and organisational measures and section 77 of the 2018 Act - Security of automated processing

The Inquiry Report highlights a number of issues in relation to security measures, such as the absence of a digital audit trail on the CCTV recording systems to record individual accesses [redacted], the use of one generic log-on for all Garda members with the password displayed on an adjacent wall [redacted] and the overall lack of auditing of audit trails, such that the AGS cannot know whether or demonstrate that all access to its CCTV systems are authorised and justified. AGS has not demonstrated that it has undertaken any of the evaluation steps required under section 77(a) nor implemented the measures to address the issues identified under section 77(b). Further, section 75 requires the controller to implement technical and organisational measures to ensure compliance with Part 5 and to demonstrate that compliance.

6.1.2.(b): Section 75 of the 2018 Act - General obligations on controller with regard to technical and organisational measures and section 77 of the 2018 Act - Security of automated processing

There is no evidence that AGS, in advance of May 2018, implemented a review and update of its technical and organisational measures surrounding its use of surveillance technologies in public places. Section 75 requires the controller to implement technical and organisational measures to ensure compliance with Part 5 and to demonstrate that compliance. Extraordinarily, the AGS Code of Practice for CCTV in Public Places has not been updated since 2006. Consequently, there is no reference to cooperation agreements with local authorities concerning certain schemes to share live feeds, nor to the new technologies now deployed in Duleek and Donore, namely Automatic Number Plate Recognition (ANPR). Furthermore, the Authorised Officers identified that records of footage downloaded and reviewed are not being kept in all instances. AGS has not demonstrated that it has undertaken any of the evaluation steps required under section 77(a) nor implemented the measures to address the issues identified under section 77(b).

6.1.2(c): Section 72 of the 2018 Act - Security measures for personal data

The members of AGS operating a number of the schemes inspected had received no training on the operation of the CCTV systems and the correct handling and protection of the personal data involved. In one instance [redacted], the Garda members operating the scheme were unaware of the full range of technical features of their own CCTV system.

6.1.2 (d): Section 76(1) of the 2018 Act – Data Protection by Design and Default

AGS failed to install CCTV cameras in such a way that they do not unnecessarily infringe the privacy rights of private individuals, and further failed to install technology that defaults back to its original settings without relying on a note attached to the recording units to remind staff to manually restore the position (pan, tilt and zoom).

6.1.2(e): Section 71(1)(e) of the 2018 – Storage limitation

No justification by reference to the functions of AGS was provided for retaining personal data in a form that identifies a data subject for longer than is necessary. [redacted].

6.1.2(f): Sections 82 of the 2018 Act – Data logging

AGS has not identified what actions it intends to take in relation to data logging, and by when, in light of section 82(5). It should evaluate this matter urgently in light of the considerable time required for development of new systems.

6.1.2 General: Section 77 of the 2018 Act - Security of automated processing

AGS has not demonstrated that it has undertaken any of the evaluation steps required under section 77(a), nor has it implemented measures to address the issues identified under section 77(b).

6.2 Privacy and Accountability

6.2.1 Appropriate Signage and General Transparency

Inquiry Report Issues: 3, 7, 13 & 18

The first principle of data protection is set down in section 71 of the 2018 Act.[11] It requires that personal data shall be processed lawfully and fairly. A cornerstone of fairness is that individuals are aware that personal data concerning them are collected, used, consulted or otherwise processed and to what extent.

The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used to explain them.

[11] Section 71 of the Data Protection Act, 2018 Processing of Personal Data states that (1) 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; (b) the data shall be collected for one or more specified, explicit and legitimate purposes and shall not be processed in a manner that is incompatible with such purposes; (c) the data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed; (d) the data shall be accurate, and, where necessary, kept up to date, and every reasonable step shall be taken to ensure that data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; (e) the data shall be kept in a form that permits the identification of a data subject for no longer than is necessary for the purposes for which the data are processed; (f) 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. (2) The processing of personal data shall be lawful where, and to the extent that (a) the processing is necessary for the performance of a function of a controller for a purpose specified in section 70(1)(a) and the function has a legal basis in the law of the European Union or the law of the State, or (b) the data subject has, subject to subsection (3), given his or her consent to the processing. (3) Where the processing of personal data is to be carried out on the basis of the consent of the data subject referred to in subsection (2)(b), the processing shall be lawful only where, and to the extent that (a) having been informed of the intended purpose of the processing and the identity of the controller, the data subject gives his or her consent freely and explicitly,(b) the request for consent is expressed in clear and plain language, and where such consent is given in the context of a written statement that also concerns other matters, the request for consent is presented to the data subject in a manner that is clearly distinguishable from those other matters, and (c) the data subject may withdraw his or her consent at any time, and he or she shall be informed of this possibility prior to giving consent. (4) Where a data subject withdraws his or her consent to the processing of personal data pursuant to subsection (3)(c), the withdrawal of consent shall not affect the lawfulness of processing based on that consent prior to the consent being withdrawn. (5) Where a controller collects personal data for a purpose specified in section 70(1)(a), the controller or another controller may process the data for a purpose so specified other than the purpose for which the data were collected, in so far as (a) the controller is authorised to process such personal data for such a purpose in accordance with the law of the European Union or the law of the State, and (b) the processing is necessary and proportionate to the purpose for which the data are being processed. (6) A controller may process personal data, whether the data were collected by the controller or another controller, for (a) archiving purposes in the public interest, (b) scientific or historical research purposes, or (c) statistical purposes, provided that the said processing (i) is for a purpose specified in section 70(1)(a), and (ii) is subject to appropriate safeguards for the rights and freedoms of data subjects. (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. (9) A processor, or any person acting under the authority of the controller or of the processor who has access to personal data, shall not process the data unless the processor or person is (a) authorised to do so by the controller, or (b) required to do so by the law of the European Union or the law of the State, and then only to the extent so authorised or required, as the case may be. (10) A controller shall ensure that it is in a position to demonstrate that the processing of personal data for which it is responsible is in compliance with subsections (1) to (8) of this section.

Section 90(2) of the 2018 Act[12] lists information that data controllers must make available to data subjects within a reasonable period after the date on which the controller obtains the personal data concerned. This information includes the identity of the data controller and the purposes of the processing. Other information required to ensure fair and transparent processing may be communicated to data subjects in further "layers" of information.

Inadequate signage is an issue identified repeatedly across the schemes inspected. In relation to the Donore and Duleek scheme, the Authorised Officers identified only one CCTV sign in the village of Duleek naming AGS. Signage naming a private contractor [redacted] and with no reference to or contact details for AGS appeared in multiple locations in both Duleek and Donore villages. [redacted] signage observed was located at such a height on the poles to which it was attached that is doubtful anyone driving by could read it. No CCTV signage of any description was observed on the approach roads travelled by the Authorised Officers to Duleek and Donore .

At Pearse Street Garda Station, Dublin and Henry Street Garda Station, Limerick, the inspection team observed CCTV signage erected adjacent to the respective Garda Stations. No purposes for the CCTV nor contact details for AGS appeared on the signs, although the AGS logo was included. Members of the public approaching the Pearse Street Dublin area from the south side of the city encounter no advance signage to alert that they are coming into a CCTV monitored area. In Limerick, the approach roads to the city and in particular the Dublin Road route into Limerick city travelled by the Authorised Officers, had no signage giving advance-warning that travellers are approaching a CCTV-monitored area.

Some, but not all, of the approach roads to Tullamore did have signage alerting the public that they are about to enter a CCTV monitored area. However, the signage was deficient in the same manner as that deployed adjacent to the Dublin and Limerick Garda Stations identified above.

The Authorised Officers further noted that the various Garda Stations operating the schemes failed to provide to callers at the public counter information leaflets on AGS CCTV operation in the relevant area. As decision maker, I have also conducted a search of the *garda.ie* website. While it provides extensive information in relation to mobile traffic cameras and their locations, there is no information specific to the individual CCTV schemes authorised under section 38 of the 2005 Act.

[12] Section 90 of the Data Protection Act, 2018, Right to information states that (1) Subject to subsection (4) and section 94, a controller shall ensure that the data subject is provided with, or, as appropriate, has made available to him or her, the information specified in subsection (2) in relation to personal data relating to him or her within a reasonable period after the date on which the controller obtains the personal data concerned, having regard to the circumstances in which the data are or are to be processed. (2) The information to which subsection (1) applies is: (a) the identity and the contact details of the controller; (b) the contact details of the data protection officer of the controller, where applicable; (c) the purpose for which the personal data are intended to be processed or are being processed; (d) information detailing the right of the data subject to request from the controller access to, and the rectification or erasure of, the personal data; (e) information detailing the right of the data subject to lodge a complaint with the Commission and the contact details of the Commission; (f) in individual cases where further information is necessary to enable the data subject to exercise his or her rights under this Part, having regard to the circumstances in which the personal data are or are to be processed, including the manner in which the data are or have been collected, any such information including: (i) the legal basis for the processing of the data concerned, including the legal basis for any transfers of data; (ii) the period for which the data concerned will be retained, or where it is not possible to determine the said period at the time of the giving of the information, the criteria used to determine the said period; (iii) where applicable, each category of recipients of the data. (3) The information referred to in paragraphs (a) to (e) of subsection (2) may be made available to the data subject by means of publication on the website of the controller.

In relation to the schemes inspected, it is clear that members of the public are not adequately on notice in relation to the processing that is taking place via CCTV operated by AGS. In many instances inspected, the first layer of signage is not present or, where it is present, it is not adequate in light, as no contact details for the controller are supplied nor purposes for processing stated. Nor is there a second layer of information available to the public, either on the garda.ie website or on leaflets in Garda stations. Were they aware, individuals may opt to use a different route or may continue and enter a CCTV-monitored area but secure in the knowledge that they can contact the relevant data controller if they wish to make inquiries or exercise any of their data protection rights.

Further, in relation to the Duleek and Donore scheme specifically where ANPR cameras are deployed, none of the signs inspected by the Authorised Officers mentions that ANPR is in use. In addition, the CCTV policy for Duleek and District (in respect of which, in any case, I make a finding at 6.2.4(a) below as the policy is not one designed and implemented by AGS as controller), fails to address in any meaningful way the purposes for which ANPR has been installed. Furthermore, the CCTV policy in overall terms fails to set out details of the capability of the ANPR cameras and there is little in the policy to explain to the general public what ANPR is, how it processes personal data and why that is necessary. This deficiency is particularly noteworthy given the significance of the use of ANPR cameras from a data protection perspective and its potential impact on the rights and fundamental freedoms of data subjects.

6.2.1 Findings:

I find that AGS infringes section 71(1)(a) and section 90(2) of the 2018 Act in that information on the personal data it collects and processes via its public CCTV systems (at least as concerns the individual schemes inspected) is not adequately communicated to the public by primary signage setting out the high-level purposes of the processing and secondary information via its website or leaflets. Nor is the identity of the data controller of the CCTV schemes clear in many instances. The effect of this infringement is to render the data unfairly collected and processed.

It is noteworthy that, notwithstanding that AGS is the data controller in relation to each scheme and the purposes are identical in terms of the personal data obtained through each scheme, that there is little consistency observed in the signage inspected for the purposes of this inquiry. AGS needs to identify and procure a consistent form of signage that meets the requirements of the 2018 Act and that will be easily recognisable by members of the public no matter where they travel in Ireland.

6.2.2 Absence of written contracts between AGS and third party data processors

Inquiry Report Issues: 4, 8, 14 & 23

The Authorised Officers identified the absence of a contract for processing between AGS as a controller and maintenance contractors on the CCTV schemes deployed. A processor is defined in section 69 of the 2018 Act.[13]

On the basis of the definition of 'processing' of personal data in section 69(1) of the 2018 Act (which includes *"the retrieval, consultation or use of the data"* and *"the disclosure of the data by their transmission, dissemination or otherwise making the data available"*) the maintenance contractor for the Garda CCTV schemes is a data processor. The AGS responses to the Authorised Officers' request for comment on the Inquiry Report did not disagree with the identification of the maintenance contractors as processors for the purposes of the 2018 Act.

The Law Enforcement Directive sets down an explicit requirement that, where a processor's work involves handling personal data on behalf of a controller, the controller may engage a processor only if there is a written contract and the processor guarantees that it will implement appropriate organisational and technical measures to protect the rights of individuals whose data is processed. It is therefore unlawful for a processor to process data of a controller in the absence of such an agreement. Section 80 of the 2018 Act[14] sets down a clear prescription for the detail that must be included in the written contracts. A key component of such an arrangement is that the processor may act only on the instructions of the controller as concerns the processing of the personal data. The purpose of the written contracts is to ensure that responsibilities are clear and apportioned and that data subject rights will at all times be respected in the handling of the personal data.

The Inquiry Report identifies that [redacted] are operating without written contracts in place with third party

[13] Section 69 of the Data Protection Act, 2018, Part 5 Processing of Personal Data for Law Enforcement Purposes states that a "processor" means 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;

[14] Section 80 of the Data Protection Act, 2018, Processors, states that (1) A controller shall engage a processor to carry out processing on its behalf only where (a) the processing is carried out, subject to subsection (3), in pursuance of a contract in writing between the controller and the processor that provides for the matters specified in subsection (2), and (b) the processor provides sufficient guarantees to implement appropriate technical and organisational measures to ensure that (i) the processing shall comply with the provisions of this Part, and (ii) the rights and freedoms of the data subjects are protected. (2) 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, and (d) provide 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.

contractors that maintain and service their CCTV systems, which service includes those contractors handling AGS-controlled personal data.

In the absence of such a contract, there is no evidence as to how the processor provides the sufficient guarantees required by section 80(1)(b) of the 2018 Act.

6.2.2 Finding:

I find that AGS infringes section 80 of the 2018 Act by failing to put in place a written contract between itself and all third-party contractors servicing its CCTV systems under the authorised schemes, and by failing to ensure the processors in each case provide sufficient guarantees to implement appropriate organisational and technical measures.

6.2.3 AGS accessing live feeds from local authority CCTV Scheme

Inquiry Report Issue 9

[redacted]

[redacted]

- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

6.2.3 Finding:

Pending the outcome of the above-mentioned inquiry [redacted], I make no finding at this time with regard to the issue of AGS accessing live feeds from the local authority. I will revisit this issue when I have the inquiry report of the DPC's Authorised Officers in relation to that local authority. Once I have the complete picture I will decide what finding(s), if any, I may need to make in respect of AGS with regard to this specific issue.

6.2.4 Use of ANPR cameras

Inquiry Report Issue 22

The inspection team identified that, of the fourteen cameras deployed in the Duleek and Donore AGS approved scheme, seven are Automatic Number Plate Recognition cameras. Reports can be exported from the recording system to show a complete log of activity by vehicle. By inputting details of either a full or partial vehicle registration number plate, the system can perform a search and return a still image of the vehicle, including the vehicle registration plate, if it was captured by an ANPR camera. 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 for 31 days in accordance with the AGS Code of Practice for CCTV in Public Places. In addition, searches from the ANPR feeds produce a clear image of the vehicle's driver and front-seat passenger, if any. While this CCTV scheme was ultimately authorised by the Garda Commissioner, it was in fact presented as a *fait accompli* scheme by the 'text alert'communities of Duleek and Donore to the AGS. It was the 'text alert' community which drove and sourced the funding for its installation

Although AGS acknowledges it is the data controller, the documents underpinning the processing operations (a CCTV policy and a Privacy Impact Assessment) were drawn up by the "Duleek and District Text Alert Community" group. I have reviewed the Privacy Impact Assessment which was submitted to this Inquiry by AGS in April 2019. Aside from a reference to the purpose of the ANPR cameras being to "search for a specific number plate after a crime has taken place" and confirming that "The CCTV scheme will only be used by trained members of An Garda Síochána to investigate a crime that has taken place", there is no explanation or justification as to why the two villages of Duleek and Donore would require this form of surveillance technology in permanent logging mode. While this Inquiry has been informed that AGS had no input into this document, it is not clear from the contents of the Privacy Impact Assessment who precisely conducted this Assessment. It is noted that a review of the assessment took place on 9 Nov 2017. In this regard it is noted that the outcome of the review states that*"CCTV has been greatly successful in assisting the An Garda Síochána in crimes that have taken place in the area"*. However, no statistics have been provided in the review to support this statement. Overall therefore it is noteworthy that the Privacy Impact Assessment focused on the CCTV scheme as a whole and did not treat the matter of the deployment of ANPR cameras with any adequate degree of consideration.

I also reviewed the information provided in the 'CCTV Policy for Duleek & District Text Alert Community CCTV System' dated November 2017. I note that on page 4 there is reference to crime statistics in the area and a table highlighting crime statistics by the nature of the crime from 2011 to 2016. According to the statistics provided, crime levels in the area decreased between 2011 and 2016 – i.e. prior to the installation of the CCTV scheme. The CCTV policy also states that*"While crime rates have fallen recently, Duleek Garda station will no longer be manned 24hrs per day. This has caused great concern to the local communities of Duleek and Donore"*.

As the data controller of the CCTV scheme, the obligation lies on AGS to implement an appropriate data protection policy in accordance with section 75(3) of the 2018 Act. I agree with the Authorised Officers' view that the CCTV Policy in overall terms fails to set out details of the capability of the ANPR cameras and the range of data processing that is generated by the deployment of such cameras, and that the policy document does not recognise or draw attention to the fact that the processing of personal data that occurs with the use of ANPR cameras is significantly more intrusive from a data protection perspective than the operation of standard CCTV cameras. In any event, the CCTV Policy document is not owned by the data controller, AGS. Nor did AGS have any input into the drafting of it.

Section 76(2) of the 2018 Act requires data controllers to implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

Furthermore, where data processing activities are likely to result in a high risk to the rights and freedoms of natural persons, section 84 of the 2018 Act requires the data controller to conduct a data protection impact assessment (DPIA) to determine and assess the impact of the processing on the protection of personal data. The Data Protection Commission has determined that a DPIA will be mandatory for, among other things, systematically monitoring, tracking or observing individuals' locations or behaviour where a documented screening or preliminary risk assessment indicates that the processing operation is likely to result in a high risk to the rights and freedoms of individuals. The DPC has published a list of types of data processing operations that require a DPIA in accordance with the requirements of Article 35(4) of the GDPR.

As no evidence was presented of any consideration being given to the issues of design in terms of what the ANPR cameras capture and how data can subsequently be aggregated, searched, consulted and reported, AGS has failed to consider the privacy impact of such surveillance using ANPR cameras. It therefore appears not to meet the requirements of data protection by design and default.

6.2.4 Findings:

I find that AGS is infringing a range of provisions under the Data Protection Act, 2018 and specifically:

6.2.4(a): Section 75(3) of the 2018 Act

I find AGS has infringed section 75(3) of the 2018 Act as it has failed as controller to implement an appropriate data protection policy in respect of the ANPR cameras and associated activities.

6.2.4(b): Section 76 of the 2018 Act

I further find that AGS has infringed section 76, as it has acted passively as the controller in taking over a pre-designed system and cannot have assessed the requirement for or implemented the appropriate data protection by design and default safeguards.

6.2.4(c): Section 84 of the 2018 Act

I also find AGS is in breach of section 84 by reason of its failure to carry out a data protection impact assessment on the ANPR surveillance system for which it is the data controller, to test the necessity of ANPR cameras and to demonstrate that the use of ANPR cameras is justified and proportionate *vis a vis* the crime levels in the area it is trying to address. In accordance with section 84(1), this assessment should have been completed before the processing operations commenced.

7. Corrective Measures

Having carefully considered the infringements identified in this decision, in respect of the 2018 Act, in accordance with section 124(2)(b) I have decided that it is appropriate to exercise one or more corrective powers. Accordingly, pursuant to section 127(1) of the Data Protection Act 2018, I now exercise the following corrective powers:

1. Pursuant to section 127(1)(d), I hereby **order AGS to bring its processing into compliance** with the relevant provision of the 2018 Act identified in the table below, by taking the relevant action specified in the table below; and

2. Pursuant to section 127(1)(f), I hereby **impose a temporary ban on processing by AGS** as set out at number 11 in the table below, insofar as such processing involves the operation of ANPR cameras, with such temporary ban to cease to have effect only upon compliance with the measures set out in bold at number 5 in the table below; and

3. Pursuant to section 127(1)(b), I hereby **issue a reprimand to AGS** in circumstances where data processing by AGS has infringed a number of provisions of the 2018 Act as referred to above. I have made this decision having regard to the number and extent of the infringements identified in this decision which have occurred across a range of processing operations and a range of AGS locations. In particular I consider that these infringements tend to demonstrate a generalised failure by AGS as data controller to implement appropriate technical and organisational measures in order to ensure that the personal data processed by it is processed in accordance with the provisions of the 2018 Act (insofar as they give effect to the LED), and to demonstrate such compliance, this obligation under section 75 being at the core of a controller's responsibilities and obligations.

No.	Finding Number	Action	Time Scale
1	6.1.1	Section 77 and section 75(1)(b) of the 2018 Act: Assess the risks and implement appropriate organisational and technical measures in accordance with section 75 and 77 of the 2018 Act in relation to the use of personal recording devices in CCTV monitoring rooms and in relation to access to CCTV monitoring rooms by all Garda members of a station.	Complete task by **31st December 2019**
2	6.1.2(a)	Section 75 and section 77 of the 2018 Act: All security deficiencies identified in the findings of this decision with regard to user log ons to the CCTV systems should be remedied.	Complete task by **31st December 2019**
3	6.1.2(b)	Section 75 and section 77 of the 2018 Act: Implement a review and update of AGS's technical and organisational measures surrounding its use of section 38(3)(a) CCTV schemes in line with sections 75(1), 75(2) and 77 of the 2018 Act.	By **31st December, 2019** submit a short report to DPC detailing the actions taken.
4	6.1.2(c)	Section 72 of the 2018 Act: The lack of overall training in relation to the operation of the CCTV systems and the correct handling and protection of the personal data involved must be addressed by means of a comprehensive training programme with significant data protection elements.	By **31st December, 2019** submit a short report to DPC detailing the actions taken.
5	6.1.2(d)	Section 76(1) of the 2018 Act: Implement effective data protection by design and default measures on the section 38(3)(a) schemes to ensure that CCTV cameras do not unnecessarily infringe the privacy rights of private individuals.	By **31st December, 2019** submit a short report to DPC detailing the actions taken.

6	6.1.2 (e)	Section 71(1)(e) of the 2018 Act: Personal data in the form of CCTV footage captured by the section 38(3)(a) schemes should not be retained in a form that identifies a data subject for longer than any objective justification.	Complete task by **31st October 2019.**
7	6.1.2(f) & 6.1.2(a)	Sections 82 of the 2018 Act: Implement the requirements of section 82(5). Where the manual audit trail logs are not comprehensive enough to meet the requirements of sections 82(1) and 82(2), and in order to avail of any time exemption outlined in section 82(5), AGS will need to either (a) demonstrate disproportionate effort or (b) demonstrate how it would cause serious difficulties for its operation of the automated processing system to which the data log relates. AGS should evaluate this matter urgently in light of the life-cycle for new systems development.	By **31st December, 2019** submit a short report to DPC detailing the actions AGS intends to take.
8	6.1.2 General	Section 77 of the 2018 Act: Implement the evaluation steps required under section 77(a) and the measures to address the issues identified under section 77(b). This should also include a revision of the CCTV in Public Places Code of Practice in consultation with the DPC.	By **31st December, 2019** submit a short report to DPC detailing the actions taken and submit a draft revised code to the DPC by this date.
9	6.2.1	Section 71(1)(a) and section 90(2) of the 2018 Act: Design a standardised primary signage for AGS approved public CCTV schemes that meets the requirements of sections 71(1)(a) and 90 of the 2018 Act and commence its roll-out as soon as possible thereafter.	Design to be completed and procurement for new signage to be

			initiated by **31st December 2019.**
10	6.2.2	Section 80 of the 2018 Act: Implement appropriate section 80 of the 2018 Act contracts between AGS and third party contractors.	Complete task by **31st December 2019**
11 & 12	6.2.4(a) and (b)	Section 75(3), 76 and 84 of the 2018 Act: Under section 75(3) of the 2018 Act, AGS is required to implement an appropriate data protection policy in respect of the ANPR cameras and associated activities under the Duleek and Donore scheme. In order to demonstrate the necessity and justification for the use of ANPR cameras in the Duleek and Donore scheme, AGS is required to carry out a comprehensive data privacy impact assessment, which includes a detailed public consultation with all residents in the villages of Duleek and Donore. This DPIA should also address the implementation of appropriate data protection by design and default safeguards. **Pending the completion of both of these actions the seven ANPR cameras should be switched off within seven days of receipt of this decision. These ANPR cameras should only be reactivated following approval of the DPC which will seek to evaluate both the new DPIA and the new CCTV Data Protection Policy referred to above.** [redacted]	Complete task by **31st December 2019**

8. Right of Appeal

This decision is a decision in accordance with section 124 of the 2018 Act. Accordingly, under section 150(5) of the 2018 Act, AGS has the right to appeal against this decision within 28 days from the date on which notice of the decision was received by it. .

Helen Dixon

Commissioner for Data Protection