THE CIRCUIT COURT
AN CHÚIRT CHUARDA

DUBLIN CIRCUIT **COUNTY OF THE CITY OF DUBLIN**

IN THE MATTER OF THE DATA PROTECTION ACT 2018 AND THE GENERAL DATA PROTECTION REGULATION (EU) 2016/679

AND IN THE MATTER OF AN APPEAL UNDER SECTION 150(5) OF THE DATA PROTECTION ACT 2018

Record No. 2022/00465

Between:

SIMON MCVANN

APPELLANT

AND

DATA PROTECTION COMMISSION

RESPONDENT

AND

THE IRISH PRISON SERVICE

NOTICE PARTY

Record No. 2022/00467

Between:

SIMON MCVANN

APPELLANT

AND

DATA PROTECTION COMMISSION

RESPONDENT

AND

HEALTH SERVICE EXECUTIVE

NOTICE PARTY

Judgment of His Honour Judge John O'Connor delivered on the 19th day of April, 2023

Table of Contents

1. Introduction

1.1 This decision relates to two appeals by the Appellant against the Respondent. The first, is an appeal against the Decision of the Respondent dated 17th January 2022 and bears the record number 2022/465. The second, is an appeal against the Decision of the Respondent dated 17th of January 2022 and bears the record number 2022/467.

1.2 In brief, the issues raised concern the following:

- The processing by Mayo University Hospital (the "**Hospital**") of the Appellant's personal data in the form of CCTV footage. CCTV footage of the Appellant was collected by the Hospital and then provided to the Appellant's employer, the Irish Prison Service (the "**IPS**"). The Appellant submitted that such processing was contrary to the requirements of data protection law.
- The use by the Notice Party (the "**IPS**") of the Appellant's personal data in the form of third-party CCTV data for the purpose of an internal prison investigation and disciplinary proceedings. The Appellant submitted that such uses were contrary to the requirements of data protection law.

The issues are more substantially described later in the judgment.

2. Facts

2.1 The Appellant is a prison officer employed by the IPS. On 8 September 2018, the Appellant and another prison officer were on duty at Mayo General Hospital, now known as Mayo University Hospital ("**the Hospital**"), accompanying a prisoner who had been taken to the Hospital for medical treatment the previous night.

2.2 During the medical treatment in the Accident and Emergency Department of the Hospital, the prisoner escaped from custody ("**the incident**").

2.3 Following the incident, the Governor of Castlerea Prison ("**the Prison**") appointed a Chief Officer to carry out an internal prison investigation of the incident. As part of that investigation, by email dated 10 September 2018 at 14:22 to the Hospital, the Chief Officer requested that the Hospital "*facilitate [him] with a viewing of CCTV for that area at that time*".

2.4 Later in the day, on the 10 September 2018, the escaped prisoner was apprehended by An Garda Síochána.

3. The use of the Appellant's personal data for an internal prison investigation

3.1 On 11 September 2018, the Chief Officer of the prison viewed the CCTV footage held by the Hospital. He subsequently referred to the CCTV footage in his report on the incident dated 19 November 2018.

3.2 The IPS also referred to the data obtained from the CCTV footage in disciplinary proceedings against the Appellant. On 11 January 2019, the Governor of the Prison initiated a complaint against the Appellant under the Prison (Disciplinary Code for Officers) Rules 1996. The summary of the evidence on which the allegation was based cross-referenced and included an attachment of a report prepared by the Chief Officer.

3.3 The Appellant objected to the use of the CCTV footage collected by the Hospital on the basis of data protection law, by letter dated 5 June 2019. The IPS declined to adjourn the disciplinary proceedings against the Appellant unless directed to do so by the Commission. The IPS stated that it was *"... satisfied that it followed the correct procedure to view this CCTV footage and to use same as part of an investigation into the escape of and to assist in apprehending the said prisoner, who was still at large*".

4. The Legal Principles: Case Law

4.1 The legal principles governing lawful processing under the GDPR and the 2018 Act are broadly accepted by both parties. Instead, it is the application of these principles to the facts of this case which are substantially in dispute.

4.2 In *Nowak v. Data Protection Commissioner* [2016] 2 IR 585, ("**Nowak**") the Supreme Court (O'Donnell J., as he then was) held that the test to be applied on any appeal pursuant to the Data Protection Acts 1988-2003 (the 'Acts') is that promulgated by Keane CJ in *Orange v. Director of Telecommunications Regulations* [2000] 4 IR 159 at pages 184 to 185 ("**the Orange Test**").

4.3 The effect of this, is that an appeal is not a full re-hearing on the merits and is limited in nature. The following cases were discussed by the parties during the hearing:

- *Orange Communications v. The Director of Telecommunications Regulation and Another No. 2* [2000] 4 IR 159
- *Cormac Doolin v. The Data Protection Commissioner and Our Lady's Hospice and Care Services* [2020] IEHC 90; [2022] IECA 117.
- *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde -v- Rīgas pašvaldības SIA 'Rīgas satiksme*

4.4 Elaborating further, the Respondent submitted that the test that must be satisfied to successfully make out an appeal against error was promulgated by Keane CJ in the decision of *Orange Communications v. The Director of Telecommunications Regulation and Another No. 2* [2000] 4 IR 159 (the Orange Judgment), commonly referred to as the Orange Test. The Appellant must establish, as a matter of probability that the decision reached by the Respondent was vitiated by a serious and significant error or a series of such errors, and in arriving at a conclusion on such an issue, the court must have regard to the degree of expertise and specialised knowledge available to the tribunal/decision-maker.

4.5 At page 184 of the Orange Judgment, Keane CJ states "*in short, the appeal provided for under this legislation was not intended to take the form of re-examination from the beginning of the merits of the decision appealed from culminating, if may be, in the substitution by the High Court of its adjudication for that of the first defendant. It is accepted that, at the other end of the spectrum, the High Court is not solely confined to the issues which might arise if the decision of the first defendant was being challenged by way of judicial review. In a case of this legislation at least, an applicant will succeed in having the decision appealed from set aside where it establishes to the High Court as a matter of probability that, taking the adjudicative process as a whole, the decision reached was vitiated by a serious and significant*

error, or a series of such errors. In arriving at a conclusion on that issue, the High Court will necessarily have regard to the degree of expertise and specialised knowledge available to the first defendant."

4.6 However as will be noted later in this judgment, the Appellant submitted the additional option open to the Circuit Court is to impose the Court's own decision under the 2018 Act.

4.7 As noted at paragraph 4.3, both the High Court and Court of Appeal recently considered the use of CCTV in disciplinary proceedings in the case of *Cormac Doolin v. The Data Protection Commissioner and Our Lady's Hospice and Care Services* ("Doolin"). This case concerned whether CCTV footage viewed by the Appellant's employer was further processed in breach of the Data Protection Act 1988. The net question was whether CCTV footage that was captured for the purposes of security can be processed for another employment issue.

4.8 In *Doolin*, graffiti was discovered in a staffroom of the Hospice which gave rise to security concerns. An investigation was launched by the Hospice to identify the person who placed the graffiti in the staff room. This investigation included a review of the CCTV footage of the incident. Mr. Doolin was an employee of the Hospice. While the CCTV footage did not show any concerns considering Mr. Doolin from a security point of view, it allegedly showed him taking unauthorised breaks during his work.

4.9 The High Court held that the purpose of viewing the CCTV footage was to prevent crime and to promote staff security and public safety. However, the High Court also held that the information derived from same was unlawfully further processed for the purpose of disciplinary action against an employee for the unauthorised breaks, which was a different purpose than that which the CCTV was originally collected.

4.10 The purpose for which the CCTV footage was collected was stated on a sign beside the CCTV camera. The sign stated, "*Images are recorded for the purposes of health and safety*

and crime prevention". The Court held that had CCTV material been intended to be used for disciplinary purposes, it is a requirement that that purpose is identified in signage and/or CCTV policy.

4.11 In this case the High Court held there was no evidence to conclude that the further processing in the context of the disciplinary hearing was for security purposes.

4.12 Hyland J. upheld Mr Doolin's appeal from the Circuit Court in the High Court as she stated there was no evidence that the use of CCTV footage or material derived from it in the disciplinary hearing was for security purposes. Therefore, she concluded the Commissioner made an error of law in holding that no further processing took place.

4.13 The Court of Appeal, in upholding the decision of the High Court, clarified that the mere fact the data was used for a different purpose does not mean that the use was unlawful. It is only where the further processing occurs in a manner incompatible with the stated purpose that an illegality arises.

4.14 Noonan J. in the Court of Appeal, applied the compatibility test as set out by the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, also known as the Article 29 Data Protection Working Party:

A substantive compatibility assessment requires an assessment of all relevant circumstances. In particular, account should be taken of the following key factors:

- the relationship between the purposes for which the personal data have been collected and the purposes of further processing;
- the context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use;

- the nature of the personal data and the impact of the further processing on the data subjects;
- the safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects.

4.15 At paragraph 89 of the judgment, Noonan J. proffered the example that if it was in fact the employee who was responsible for the graffiti, the employee would face a disciplinary process for doing the very thing which gave rise to the security issue in the first place. In that event it could not be argued that the CCTV was being used for an unspecified purpose or one that was incompatible.

4.16 In addition, Advocate General Bobek's Decision in the Rigas Case (Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde -v- Rīgas pašvaldības SIA 'Rīgas satiksme'), as referenced in paragraph 4.3, was opened to the Court. This case concerned a taxi driver who stopped his vehicle at the side of the road. A bus was passing by as the taxi passenger opened the door of the vehicle which caused damage to the bus. The bus company sought the taxi driver's identity number from the police in order to bring civil proceedings to compensate for the damage sustained. The police refused to disclose the identity number. The Latvian Court referred a preliminary reference to the CJEU, namely were the police, as the data controller, obliged under Article 7(f) of Directive 95/46/EC to provide the third party with the data subject's personal data.

4.17 Advocate General Bobek opined that there was no obligation to disclose the personal data but there was facility to do so conditional upon (a) a legitimate interest and (b) a balancing of interests.

5. The Legal Principles: GDPR and the Data Protection Act 2018

5.1 The following legislative provisions were discussed by the parties during the course of the hearing:

5.2 Article 5: Principles relating to Processing of Personal Data

1. Personal data shall be:

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

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

5.3 Article 6: Lawfulness of Processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
   (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
   (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
   (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
   (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
   (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;
   (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.
3. 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 the 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.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
   (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
   (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
   (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
   (d) the possible consequences of the intended further processing for data subjects;
   (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

5.4 Section 150 of the Data Protection Act 2018 – Right to an Effective Judicial Remedy

(1) A controller or processor on which an information notice or enforcement notice or a notice under section 135 (1) is served may, within 28 days from the date on which the notice is served, appeal against a requirement specified in the notice.

(2) The court, on hearing an appeal under subsection (1), shall—

(a) annul the requirement concerned,

(b) substitute a different requirement for the requirement concerned, or

(c) dismiss the appeal.

(3) This subsection applies to an appeal brought under subsection (1)—

(a) against a requirement specified in an information notice to which section 132 (3) applies, or an enforcement notice to which section 133 (6) applies, and

(b) that is brought within the period specified in the notice concerned.

(4) Notwithstanding any provision of this Act, the court, on hearing an appeal to which subsection (3) applies, may on application to it in that behalf, determine that non-compliance by the controller or processor concerned with a requirement specified in the notice, during the period ending with the determination or withdrawal of the appeal or during such other period as the court may determine, shall not constitute an offence.

(5) A data subject or other person affected by a legally binding decision of the Commission under Chapter 2 or 3 may, within 28 days from the date on which notice of the decision is received by him or her, appeal against the decision.

(6) The court, on hearing an appeal under subsection (5), shall—

(a) annul the decision concerned,

(b) substitute its own determination for the decision, or

(c) dismiss the appeal.

(7) Where the Commission, being the competent supervisory authority in respect of a complaint within the meaning of Chapter 2 or 3, does not comply with section 108 (2) or, as the case may be, section 121 (2), the complainant concerned may apply to the court for an order under subsection (8)(a).

(8) The court, on hearing an application under subsection (7), shall—

(a) order the Commission to comply with the provision concerned, or

(b) dismiss the application.

(9) The Circuit Court shall, concurrently with the High Court, have jurisdiction to hear and determine proceedings under this section.

(10) The jurisdiction conferred on the Circuit Court by this section shall be exercised by the judge for the time being assigned to the circuit where—

(a) in the case of an appeal under subsection (1), the controller or processor is established,

(b) in the case of an appeal under subsection (5), the data subject or other person resides or is established, or

(c) in the case of an application under subsection (7), the data subject resides,

or, at the option of the controller, processor, data subject or person concerned, by a judge of the Circuit Court for the time being assigned to the Dublin circuit.

(11) A decision of the Circuit Court or High Court, as the case may be, under this section shall be final save that an appeal shall lie to the High Court or Court of Appeal, as the case may be, on a point of law.

(12) For the purposes of this section, a "legally binding decision" means a decision—

(a) under paragraph (a) or (b) of section 109 (5) or paragraph (a) or (b) of section 122 (4),

(b) under section 111 (1)(a), 112 (1), 113 (2)(b), 114, 124 (1)(a) or 125 (1), or

(c) to exercise a corrective power under Chapter 2 or 3.

5.5 The Prison (Disciplinary Code for Officers) Rules 1996 was in existence if the Governor decided to initiate an investigation into a breach of prison discipline. While not relevant to these proceedings the Code was revoked in 2022 and replaced by the Civil Service Disciplinary Code.

6. The Appellant's complaint to the DPC against IPS

6.1 On or about 19 June 2019, the Appellant's solicitors submitted a complaint to the Commission in relation to the Data Protection issues raised by the IPS' use of the CCTV footage alleging that the use of same was:

> **(a)** In breach of the requirement under Article 5(1)(a) of the GDPR to process personal data lawfully, fairly and in a transparent manner. The Appellant also alleges it was never informed of the purpose for which his personal data was processed and was never given notice by the IPS that CCTV footage obtained from a third party could be used in disciplinary proceedings against him.
>
> **(b)** In breach of the requirement under Article 5(1)(b) of the GDPR not to further process personal data for a purpose which is incompatible with the purpose for which it was collected. The IPS stated in its letter dated 5 June 2019 that it obtained the personal data from the CCTV footage for the purposes of its "*investigation into the escape of and to assist in apprehending [the] prisoner*" (the first purpose). However, the Appellant alleges that the personal data was then used for a fundamentally different and unrelated purpose: the taking of disciplinary proceedings against the Appellant; and
>
> **(c)** In breach of the requirement under Article 6 of the GDPR to process personal data only on foot of a lawful basis. The IPS, in a letter dated 9 June 2019, stated that the use of the CCTV footage took place as part of its investigation into *"the escape of and to assist in apprehending [the] prisoner*". However, the Appellant alleges this is incorrect as, by the time the footage was viewed on 11 September 2018, the prisoner had already

been apprehended. Therefore, the Appellant alleges that the IPS did not have a legal basis for the use of the personal data in disciplinary proceedings.

7. The Appellant's complaint to the DPC against the Hospital

7.1 The Appellant lodged a separate complaint against the Hospital in relation to Article 6 of the GDPR. In the Appellant's view the IPS did not have a lawful basis under Article 6(1)(d) of the GDPR to view and process the CCTV footage furnished to it by the Hospital as the prisoner had been apprehended late evening prior to the disclosure of the CCTV footage by the Hospital to the IPS. Therefore, the Appellant alleged the purported legal basis did not exist at the time of the said disclosure by the Hospital to the IPS as there was no evidence that the disclosure of the CCTV footage by the Hospital to the IPS was objectively necessary to protect vital interests of the general public.

7.2 The Appellant also submitted that there was no evidence that the Hospital had provided the Appellant with the identity of the data controller or the purpose for which the data was to be processed in compliance with Article 5(1)(a) and Article 13 of the GDPR. In addition, the Appellant submitted no notice was given by the Hospital in advance of the original processing of his personal data on 8 September 2018, that the Appellant's personal data could be disclosed to a third party and processed for the purposes of an internal prison investigation and subsequently in disciplinary proceedings against him. The Appellant further submitted that no evidence was shown that the Hospital had a data protection policy in place that provided for the disclosure of data subject's personal data to a third party without their consent and the further processing of that personal data for purposes of an internal prison investigation and in disciplinary proceedings against the data subject.

8. The Health Service Executive

8.1 The Health Service Executive (the "**HSE**") was added as a Notice Party by Court Order dated 13 October 2022 and this will be discussed further at subheading 21.

9. Summary of Decision of the DPC dated 17 January 2022 in respect of the Appellant's complaint against the IPS in accordance with section 109(6) of the Data Protection Act 2018 (the "2018 Act")

9.1 In its Decision the DPC rejected all the grounds of the Appellant's complaint and found as follows:

(a) That the IPS had a lawful basis under Article 6(1)(e) of the GPDR for processing the personal data of the Appellant contained in the CCTV footage for the purpose of the performance of the function of the Governor under the Prison Rules 2007;

(b) That the processing of the CCTV footage by the IPS from the Hospital for use in connection with its investigation was not incompatible with the purposes for which the footage was originally collected; and

(c) That the IPS had a lawful basis under Articles 6(1)(b)(c) and (f) of the GPDR for processing the personal data of the Appellant contained in the CCTV footage for the purposes of grounding disciplinary proceedings.

9.2 The Appellant's complaint was therefore dismissed, such dismissal being an action identified at section 109(5)(b) of the 2009 Act.

10. The Nature of this Appeal

10.1 This is an appeal against the Decisions of the DPC dated 17 January 2022 under Section 150(5) of the 2018 Act (the "2018 Act").

10.2 The Appellant submitted that the test to be applied has not significantly been considered by the courts in respect of Section 150(5) of the 2018 Act. He acknowledges that the test under Section 26 of the Data Protection Act 1998 was to apply "**the Orange Test**" as described at paragraph 4.4 of this judgment. However he submitted that under the 2018 Act, the Oireachtas has afforded the Circuit Court the power to substitute its own determination for the decision of the Commission. In summary counsel for the Appellant submitted that:

"You're [the Court] tasked with looking at errors of law and errors of fact. There is deference to be afforded but in the 2018 Act this court has been provided with the power to substitute the decision for its own determination". The net effect results in "taking some of the deference away from the DPC."

10.3 The Respondent counsel submitted that the test to be applied is "the Orange test" and whether there was a series or significant error. In this regard counsel for the Respondent submitted that deference is given to the expertise of the decision-maker. Counsel pointed out that Keane CJ outlined in Orange that an appeal was not intended to take the form of a re-examination of the entire case, but that in this case they submitted that the Appellant is asking the court to re-examine the merits of the case and not just the law. Counsel for the Respondent submitted that "*every finding of the DPC decision is raised as an issue. Across the board – almost entirely*. [It is] *not the role of the court. If the court were to take on such a role it would be overloaded by appeals of this kind*."

10.4 However, it is important to bear in mind that the Circuit Court has an additional power, as outlined at paragraph 5.4 of this judgment. Under Section 150(5) and (6) of the 2018 Act, the Circuit Court can:

(a) annul the decision concerned,

(b) substitute its own determination for the decision, or

(c) dismiss the appeal.

This new power to substitute its own determination for the decision of the Commission is an important new power given to the Circuit Court by the Legislature.

10.5 Counsel for the HSE agree with the Respondent that the Orange Test is the applicable test and adds "*the notice of appeal is quite detailed so much as to say every issue determined*

is under review. That is not the function of an appeal under s.150(5). And that the post-GDPR case law has not suggested that the Orange Test is watered down in this context."

11. <u>Decision of the DPC dated 17 January 2022 in respect of the Appellant's complaint against the Hospital in accordance with section 109(6) of the 2018 Act</u>

11.1 The DPC rejected all the grounds of the Appellant's complaint and found as follows:

(a) that the hospital had a legitimate basis to fulfil the IPS' request to process the relevant CCTV footage, at that time, especially considering the gravity of the situation and the potential for future incidents, and the IPS carrying out its tasks to investigate these matters.

12. <u>The Grounds of the Appeal in respect of the DPC decision on the use of the data by the IPS</u>

12.1 The grounds of appeal were set out in the Notice of Appeal which states that the DPC erred in fact and/or in law:

(1) In deciding that the IPS had a lawful basis under Article 6(1)(e) of the GDPR and Section 38 of the Data Protection Act 2018 for processing the Appellant's personal data contained in the CCTV footage for the purpose of an internal investigation and pursuant to Rule 83(1) of the Prison Rules 2007 in circumstances where they state there was no evidence in the Decision that the IPS had informed the Minister in writing of the incident. Furthermore, the IPS was not entitled to rely on Article 6(1)(e) of the GDPR in circumstances where they state the IPS had failed to comply with the provisions of Article 5 in relation to the processing.

(2) In deciding that the IPS had a lawful basis under Article 6(1)(f) of the GDPR for processing the Appellant's personal data contained in the CCTV footage for the purposes of disciplinary proceedings in circumstances where:

(i) as a division of the Department of Justice, the IPS was acting as a public authority in the performance of its tasks and was not entitled to rely on Article 6(1)(f) as a legal basis for processing the Appellant's personal data in disciplinary proceedings;

(ii) the IPS never sought to rely on Article 6(1)(f) as a legal basis for the processing of the Appellant's personal data and/or the Commission never advised the Appellant that the IPS was seeking to rely on same as a legal basis for the said processing;

(iii) in the alternative, there was no evidence in the Decision that the IPS had evaluated whether it had a legitimate interest before processing the Appellant's personal data;

(iv) The IPS was not entitled to rely on Article 6(1)(f) of the GDPR in circumstances where the IPS had failed to comply with the provisions of Article 5 of the GDPR in relation to the processing;

(3) Deciding that the viewing by the IPS of the CCTV footage for use in connection with its investigation and subsequent use in connection with its investigation and the subsequent use of the CCTV footage in disciplinary proceedings against the Appellant was not incompatible with the purposes for which the footage was originally collected and thus not in contravention of Article 5(1)(b) in circumstances where:

` **(i)** in its view that the DPC failed to lawfully and properly interpret, apply, and address the requirements of Article 5(1)(b) and Article 14 of the GDPR;

(ii) They state there was no evidence in the Decision from the Hospital as to the purposes for which the CCTV footage was originally collected;

(iii) At paragraph 17 of the Decision, the Appellant submitted that the DPC erred in law in deciding that there was "*a clear and entirely legitimate purpose resulting from the normal operation of the law for the IPS to have viewed the CCTV footage, even though the prisoner was apprehended at the time of the viewing, and the interpretation of data protection law should be guided by a common sense approach especially considering the gravity of the situation and the potential for future incidents if learnings are not taken from such security breaches*";

(iv) The DPC failed to properly apply the four factors set out by the Article 29 Working Party in its Opinion 3/2013 on purpose limitation.

(v) The DPC failed to apply the law as laid down by the High Court judgment in Doolin v. Data Protection Commission [2019] IEHC 90 and on appeal by the Court of Appeal in [2022] IECA 117, which dealt with the issue of "purpose limitation".

(4) In deciding that the processing of the Appellant's personal data contained in the CCTV footage in connection with the disciplinary proceedings was not incompatible with the purpose for which the IPS collected the personal data (internal investigation) and thus not in breach of Article 5(1)(b) in circumstances where it submitted that that:

(i) that the DPC failed to lawfully and properly interpret, apply, and address the requirements of Article 5(1)(b) and Article 14(4) of the GDPR.

(ii) The DPC erred in law in deciding that the relevant purpose for which the personal data was collected were those of the IPS (i.e., internal investigation) and not those of the original operators of the CCTV system.

(iii) The DPC erred in concluding that the purpose for which the CCTV footage was ultimately used was not incompatible with the purpose for which the original controller processed the personal data.

(5) The DPC erred in deciding that the IPS was entitled to rely upon Article 5(1)(a) in the circumstances of the case and insofar as the disciplinary proceedings were concerned for the reasons given at paragraph 23 of the Decision of the DPC. Furthermore, the DPC erred in law in concluding that information provided to the Appellant on 13 September 2018 (five days after the processing of the data by the Hospital and three days after the Chief Officer viewed the CCTV footage) satisfied the requirements of transparency under Article 5(1)(a) of the GDPR.

(6) The DPC erred by failing to consider whether the IPS had complied with the requirements of Article 14(1), (2) and (4) of the GDPR in circumstances where the personal data had not been obtained from the Appellant.

13. <u>The Grounds of the Appeal in respect of the DPC decision on the use of the data by the Hospital</u>

13.1 The grounds of appeal states that the DPC erred in fact and/or in law:

(1) In deciding that the Hospital had a lawful basis to process the Appellant's personal data by disclosing it to the IPS in circumstances where

(a) the DPC failed to lawfully and properly interpret and apply Article 6 of the GDPR.

(b) the Hospital was not entitled to rely on Article 6(1)(d) of the GDPR in circumstances where the prisoner had been apprehended one day prior to the disclosure of the CCTV footage by the Hospital to the IPS and the purported legal basis did not exist at the time of the said disclosure.

(c) there was no evidence in the Decision of the DPC that the disclosure of the CCTV footage by the Hospital to the IPS was objectively necessary to protect vital interests of the general public;

(d) the DPC erred in law in concluding at paragraph 7 of the Decision that the IPS had a lawful basis under Article 6 of the GDPR to view and process the CCTV footage.

(e) that the DPC erred in law in concluding that, as a consequence, the Hospital had a lawful basis to disclosure the CCTV footage to the IPS.

(2) The Appellant further submitted that the DPC erred in fact and/or in law in deciding that the Hospital had complied with the requirement of Article 5(1) and Article 5(2) of the GDPR in circumstances where:

(a) the DPC failed to lawfully and properly interpret, apply and address the requirements of Article 5 and Article 13 of the GDPR;

(b) there was no evidence in the Decision that the Hospital had provided the Appellant with the identity of the data controller or the purpose for which the data was to be processed in compliance with Article 5(1)(a) and Article 13 of the GDPR;

(c) there was no evidence in the Decision that the Appellant was given notice in advance of the original processing of his personal data on 8 September 2018 by the Hospital, that the Appellant's personal data could be disclosed to a third party and processed for the purposes of an internal prison investigation and subsequently in disciplinary proceedings against him;

(d) there was no evidence in the Decision that the Hospital had a data protection policy in place that provided for the disclosure of data subject's personal

data to a third party without their consent and the further processing of that personal data for purposes of an internal prison investigation and in disciplinary proceedings against the data subject.

14. <u>Oral submissions by the Parties</u>

14.1 In addition to detailed written submissions, counsel for the various parties made extensive oral submissions. Although there is considerable overlap with the written submissions, for completeness' sake the oral submissions are summarised below.

15. <u>Oral Submissions by the Appellant</u>

15.1 The following is a summary of the oral submissions made on behalf of the Appellant:

15.2 In circumstances where there was no evidence that the IPS informed the Minister in writing of the incident and where they failed to comply with the provisions of Article 5 of the GDPR, the Appellant submitted that the IPS is not entitled to rely on Article 6(1)(e) of the GDPR. They submitted that pursuant to Article 6(1)(e) of the GDPR, processing must 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.

15.3 The Appellant submitted that the DPC erred in finding that the IPS could justify its processing on Article 6(1)(e). Rule 83(1) of the Prison Rules states "*shall inform the Minister in writing*". Rather than considering necessity and proportionality of the processing, the Appellant submitted that the Respondent assumed any and all of the processing was necessary based on the obligation in Rule 83. In circumstances where there was no evidence that the IPS actually reported the incident to the Minister, the IPS sought access to the footage in the

investigation of the complaint. However, the Appellant submitted that the processing became unnecessary when the prisoner was apprehended prior to viewing the CCTV footage.

15.4 Specifically the Appellant submitted the disciplinary purpose was separate to the internal investigation. The basis relied on in Article 6(1)(e) is not a legal basis that could be relied on in the disciplinary proceedings.

15.5 Furthermore, the Appellant submitted the DPC erred in law in deciding that the IPS had a lawful basis under Article 6(1)(f) of the GDPR for the purpose of disciplinary proceedings. The Appellant submitted, as a division of the Department of Justice, the IPS was acting as a public authority and was not entitled to rely on Article 6(1)(f). In addition, the IPS never sought to rely on this Article as a legal basis, it was the DPC that came to this conclusion without this basis being proffered by the IPS. Therefore, there was no evidence in the decision by the Respondent that the IPS evaluated that it had a legitimate interest before processing.

15.6 The Appellant further submitted that the DPC go further and state that it was clear that the processing was undertaken as part of the employment relationship between the Appellant and IPS. In other words, the Respondent states that the IPS were not performing tasks as a public authority but acting as an employer and in this context they are entitled to rely on Article 6(1)(f). However, the Appellant submitted that this is fundamentally flawed and inconsistent with the position previously adopted by the IPS. Furthermore, the IPS state that in correspondence they were carrying out their duties as Governor and not as employer and reference paragraph 14 of the DPC's decision. The IPS did not state it was relying on Article 6(1)(f). There was no evidence the IPS conducted the relevant evaluation, in other words they did not consider "relevancy and proportionality".

15.7 The Appellant also submitted that there was no evidence from Mayo Hospital as for the purposes for the which the footage was originally collected. In this regard they state that the

Respondent erred in holding that there was a legitimate purpose as the prisoner was apprehended at the time. Specifically, they point out that the DPC failed to apply the rationale in *Doolin v. The Data Protection Commissioner* [2020] IEHC 90 which is the only case in Irish law addressing "purpose limitation". In other words, the Appellant submitted that the Respondent failed to look at the purpose the data was used for. They state that this failure in the decision to address the purpose limitation amounts to a significant breach of the law. The DPC decision records the data was collected for one purpose outlined at paragraph 17 of the decision, namely the security of the building, then it was obtained by the IPS for the purpose of its internal investigation, and then further processed for the purpose of use in the disciplinary proceedings. In respect of Article 5(1)(b), the data must be collected for a specified, legitimate, and explicit purpose. In this respect they submitted that the controller must be able to demonstrate compliance with this principle.

15.8 Article 6(4) of the GDPR states that when assessing the compatibility of another purpose, the following should be taken into account:

a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

d) the possible consequences of the intended further processing for data subjects;

e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

15.9 The Appellant relied on paragraph 51 of the High Court judgment of Hyland J in *Doolin v. The Data Protection Commissioner*, in which the learned Judge stated:

> "*Had CCTV material been intended to be used for disciplinary purposes as well as the other purpose identified, that would require to be identified (as indeed was subsequently done in the policy amendment). If, at the time of collection, the policy was as it is now, none of the above difficulties would have arisen. This is not intended in any way as a criticism of OLHCS but rather to demonstrate that the draconian consequences of upholding the Appellant's claim as urged upon me by counsel for the DPC are unlikely. It was asserted that such a finding would seriously hamper investigations of the kind carried out here. I do not accept that. Where a processor wishes to use CCTV data for identified purposes, if those purposes are clearly identified before the material is collected (assuming of course that they are otherwise permissible purposes having regard to the Act) then the use of such material is likely to be uncontroversial.*"

15.10 The Appellant also referenced the Court of Appeal decision (Noonan J.) *in Doolin v. The Data Protection Commissioner*. However, the Appellant acknowledged that while the High Court decision was delivered in *Doolin* before the DPC's decision, the Court of Appeal decision was not issued until after the DPC's decision in this case.

15.11 The Appellant accepted that is reasonable to expect that CCTV footage from a public access area could be used. However, it was submitted that it was collected for security purposes and not for the purpose of disciplinary proceedings. The Appellant submitted that it was not reasonable to expect CCTV footage from a public access area could be used in disciplinary proceedings and the Appellant suggests this was not addressed in the Respondent's Decision.

15.12 The Appellant submitted that this situation could have been avoided. Furthermore, it was submitted that if the court allowed the appeal it would not lead to the draconian consequences that were alluded to in the Respondent's decision. These were highly unusual circumstances. Counsel for the Appellant stated that there is a need to comply with notice requirements and ensure that there is a valid legal basis for processing the data.

16. <u>Oral Submission by the Respondent</u>

16.1 The Respondent submitted that the fundamental question for this Court on this appeal is whether, taken the adjudicative process as a whole, the Appellant has established, as a matter of probability, a "*serious and significant error or a series of such errors*" in the Respondent's Decision.

16.2 It stated that the Appellant's appeal is wide-ranging and alleges serious and significant errors on the part of the Respondent in practically every aspect of the Decision. In that regard, the Respondent submitted that, the Appellant in effect invites this Court to engage in a re-examination from the beginning of the merits of the decision. The Respondent submitted that this is precisely the manner rejected by the Supreme Court in *Orange Ltd. v. Director of Telecoms (No. 2)* [2000] 4 IR 159 ('*Orange*').

16.3 The Respondent submitted that it is settled law that, where a data controller processes personal data falling within the scope of the GDPR, the data controller must have a legal basis for processing. This requirement stems from the general principle of lawful, fair and transparent processing enshrined in Article 5(1)(a) of the GDPR, which is given further effect in the terms of Article 6 GDPR.

16.4 The Respondent submitted that Article 6 of the GDPR provides an exhaustive list of legal bases which may be relied upon by a data controller for the purposes of processing personal data. Under Article 6(1)(e), processing shall be lawful where "*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". In accordance with Article 6(3), the basis for processing relied on under Article 6(1)(e) must be laid down in Union or Member State law.

16.5 The Respondent points out that Article 6(1)(e) GDPR is given further effect in Irish law through Section 38 of the 2018 Act which provides, in its first section, that the processing of personal data shall be lawful to the extent that such processing is "*necessary and proportionate for*" inter alia "*the performance of a function of a controller conferred by or under an enactment or by the Constitution*".

16.6 The Respondent submitted that whilst the standard of necessity has been strictly interpreted in the caselaw of the Court of Justice of the European Union, the Court of Justice has made it clear that, in applying that standard, it is necessary to consider whether there are other means, less restrictive of the data subject's rights, by which the objective of general interest being pursued "*can reasonably be achieved just as effectively*" as stated in the decision of *Latvijas Republikas Saeima (Points de pénalité)*, Case C-439/19, EU:C:2021:504.

16.7 In respect of Rule 83(1) of the Prison Rules, the Respondent submitted that it is clear from the terms of the Decision that the Respondent determined that, in the circumstances of the case and on the basis of the evidence available to it, the unlawful escape of a prisoner, such as occurred in this case, clearly satisfied the requirement that processing is necessary and proportionate for the performance of the functions under the Prison Rules 2007, including under Rule 83(1). They further submitted that the Appellant has not identified any alternative to the use of the CCTV footage in these circumstances and appears to take the view that, because the prisoner was subsequently apprehended, the processing for the purpose of the investigation was "*unnecessary*". In so submitting, the Appellant appears to suggest according to the Respondent that that the subsequent apprehension of the prisoner would obviate the need

for an investigation into a very serious security incident of this kind. However, the Respondent submitted that, as a matter of practicality and common sense, obtaining the CCTV footage in relation to the prisoner's escape was clearly necessary and appropriate in order to identify how a serious security incident of this kind occurred and to ensure that such an incident would not recur. Having regard to the gravity of the incident, and the lack of any equally effective alternative to the use of the CCTV footage in these circumstances, it was submitted by the Respondent that it was fully justified in reaching its conclusion that the IPS had a lawful basis for processing the Appellant's personal data for the purposes of its internal investigation under Article 6(1)(e) GDPR and section 38 of the 2018 Act.

16.8 With respect to the Appellant's argument that there was no evidence that the IPS "*had actually informed the Minister in writing of the incident*", the Respondent states that its decision is not premised on the IPS having actually informed the Minister in writing of the incident or such a communication being an essential prerequisite of reliance on Article 6(1)(e) of the GDPR and Section 38 of the 2018 Act. Rather, the Respondent stated it expressed the view that in order to comply with the legal obligation to keep the Minister informed under Rule 83(1) of the Prison Rules, the IPS must be able to take the steps necessary to investigate incidents of particular importance which the Governor of the Prison ("the Governor") "*might consider should be brought to the Minister's attention*". What is important for the purposes of the Decision according to the Respondent is that, in carrying out the investigation, the IPS was engaged in processing necessary for the performance of a task carried out in the public interest conferred on it under an enactment. The Respondent acknowledges in its submissions that it is for the Governor in any given case to decide as to whether or not a matter should ultimately be brought to the attention of the Minister. However, it also submitted that if the IPS were not in a position to carry out such investigations, the Governor would not be in a position to

determine whether or not this is the case and thus to comply with the obligations under the Prison Rules, including under Rule 83(1).

16.9 The Respondent submitted that it is not the case that, in reaching its conclusion under this heading it conflated two separate processing purposes: that of the internal investigation into the prisoner escape, on the one hand, and that of the disciplinary proceedings, on the other. The Respondent submitted that it is apparent from the Decision that the Respondent considered these issues separately, with the processing for the purposes of the internal investigation considered first and the further processing for the purposes of the disciplinary proceedings considered subsequently. The Respondent submitted that the reference in the Decision to Rule 75(4)(i) – regarding officers' fitness for duty and good conduct – does not undermine that position. Rather it submitted that it is clear from the relevant part of the Decision that this was considered in the context of the IPS "*conducting internal investigations for the purpose of ensuring that "the Officer escorting had followed the strict security protocols when escorting a prisoner*". Having regard to the underlying facts, and the overlap between the matters the subject of the internal investigation and the disciplinary proceedings, the Respondent submitted that it made no error in this regard and did not conflate the separate processing operations at issue.

16.10 Generally, the Respondent submitted that that the Appellant has not identified any serious and significant error or series of such errors in its conclusion that the IPS had a lawful basis under Article 6(1)(f) GDPR for processing the Appellant's personal data for the purpose of the disciplinary proceedings.

16.11 Specifically, the Respondent submitted that the IPS is a public authority and for the reasons outlined that it is not precluded from relying on Article 6(1)(f) GDPR as a lawful basis for processing of the Appellant's personal data for the purposes of the disciplinary proceedings.

While the Respondent acknowledged that Article 6(1) on its face precludes a public authority from relying on Article 6(1)(f) GDPR, it pointed out that in the Respondent's submission, this is not an absolute bar on a public authority relying on the legitimate interest's legal basis. Rather it states that a public authority is precluded from relying on this legal basis *"in the performance of their tasks,*" which is properly understood as referring to the performance of its tasks carried out in the public interest, in line with Article 6(1)(e) GDPR. This, it submitted is consistent with Recital 47 GDPR which states that, given that it is for the legislature to provide by law for the legal basis for public authorities to process personal data, that legal basis "*should not apply to the processing of public authorities in the performance of their tasks*".

16.12 In this case, the Respondent submitted that the processing is for the purposes of the disciplinary proceedings and the data was processed as part of the employment relationship between the Appellant and the IPS. In other words, the IPS was exercising its powers qua employer, rather than engaged in the performance of its tasks qua public authority. The Respondent submitted that whilst the IPS's position as a public authority forms a relevant part of the context for the purpose of assessing the legitimate interests at play, it is in its capacity as an employer that the IPS is entitled to initiate disciplinary proceedings.

16.13 The Appellant submitted that neither the IPS nor the Respondent advised the Appellant of the IPS's reliance on Article 6(1)(f) GDPR. However, the Respondent submitted that it is not a condition of reliance on Article 6(1)(f) GDPR that the data subject must be informed in advance of reliance thereon. In this case, while it acknowledges that the IPS may not have specifically referred to Article 6(1)(f) of the GDPR in terms, as noted in the Decision, the substance of the IPS's submission was that the processing in question was necessary in order for the IPS to pursue its legitimate interests.

16.14 Finally the Appellant submitted that there is no evidence that the IPS had conducted the necessary evaluation under Article 6(1)(f). However, the Respondent submitted that this does not preclude reliance on Article 6(1)(f) where the Respondent is satisfied that the conditions of Article 6(1)(f) are satisfied. In this case, the Respondent states that having referred to the facts before it and the submissions of the IPS, the Respondent submitted that it set out clearly the basis on which it considered that the requirements of Article 6(1)(f) GDPR were satisfied and, in particular, that the legitimate interests of the IPS were not overridden by the rights and interests of the Appellant. The Respondent further submitted that that while there was no evidence in the Decision that the IPS had carried out the necessary evaluation, it states that in its view the Appellant does not appear to challenge the substantive basis for the Respondent's conclusion that the conditions for reliance on Article 6(1)(f) were fulfilled.

17. <u>The Purpose Limitation Principle</u>

17.1 The Appellant alleged that the Respondent erred in finding that there was no breach of the purpose limitation principle under Article 5(1)(b) of the GDPR insofar as the Appellant's personal data deriving from the CCTV footage, originally collected by the Hospital and viewed by the IPS, was used in the context of the disciplinary proceedings concerning the Appellant. In the Decision the Respondent concluded that, while the CCTV footage was originally collected and viewed for security purposes, it states that it was reasonable to expect that the investigation into the security incident could result in findings which may require further action on the part of the IPS, including disciplinary action, and that processing for this purpose was not incompatible with the original purpose.

17.2 According to the Appellant, the Respondent erred in its assessment of the purpose limitation principle by failing to address, first, the original purpose for which the personal data was collected and, second, the different purposes for which the IPS processed the personal data. The legal principles governing purpose limitation under Article 5(1)(b) GDPR are not

materially in dispute. Instead, the Respondent submitted that it is their application to this case which is in dispute between the parties.

17.3 The Respondent acknowledges that, in its judgment in *Doolin v. Data Protection Commissioner* [2022] IECA 117, the Court of Appeal concluded that the use of CCTV footage, originally processed by an employer for security purposes, and subsequently for the purposes of disciplinary proceedings, constituted processing for an incompatible purpose contrary to the purpose limitation principle. However, it states that there is a fundamental distinction between the facts of *Doolin* and the facts of this case.

17.4 In *Doolin*, the Respondent submitted that the Court of Appeal took the view that there were two investigations or, at minimum, an investigation into two different matters: on the one hand, a security incident relating to graffiti on the premises and, on the other hand, the taking of unauthorised breaks by an employee. In these circumstances, they suggest that the Court considered that the fact that the viewing of the CCTV was for the purpose of attempting to detect the perpetrator of the offensive graffiti and damage to Hospice property was "*entirely irrelevant to the incidental observation of Mr Doolin taking unauthorised breaks*" and there was no evidence that "*the taking of such breaks represented a security issue in itself*".

17.5 By contrast, the Respondent submitted that the Court of Appeal also held in *Doolin* that, if an employee faced disciplinary proceedings for doing the very thing that gave rise to the security issue in the first place, "*it could not be argued that the CCTV was being used for an unspecified purpose or one that was incompatible*". In the Respondent's submission, this is precisely the situation in which the Appellant finds himself in this Appeal. The disciplinary proceedings derive from, and are specifically linked to, the security incident.

17.6 The Appellant submitted that the Respondent failed to appreciate the significance of the source of the CCTV footage and the purpose for which it was collected by the Hospital and

that, rather than grounding its assessment in the express purpose for which the data was collected by the original data controller, the assessment in the Decision was grounded on a consideration of the purpose pursued by the IPS at the time of viewing the CCTV. In the Respondent's submission, there is no basis for this complaint. At the outset, the Respondent reminds this Court that the Appellant's complaint, which was the subject of the Decision and now the Appeal in this case, was against the Irish Prison Service. While the Appellant made a separate complaint against the Hospital, the Decision was not directly concerned with the lawfulness of the processing undertaken by the Hospital.

17.7 The Respondent submitted that Appellant acknowledges that the Respondent does specifically identify the purpose for which the CCTV footage was collected i.e. for the purposes of security, namely the security of the building and the people who work in, and attend, the hospital. However, the Respondent submitted that it also clearly recognises that the processing of the CCTV footage by the IPS was for security purposes i.e. to "*ascertain the circumstances surrounding the escape to ensure no future possible system failure and to ensure that the Officer escorting had followed the strict security protocols when escorting a prisoner*".

17.8 In these circumstances, the Respondent submitted that it cannot seriously be contended that the initial processing by the IPS of the CCTV footage for security purposes was for a different or incompatible purpose to that for which the CCTV footage was originally collected by the Hospital. Contrary to the Appellant's submissions, it states that there is a necessary and obvious linkage between the collection of the data for security purposes and its subsequent use and processing for that same purpose.

17.9 Having regard to the nature and gravity of the incident, the Respondent submitted there is no basis for contending that the potential negative impact on the Appellant weighed against the compatibility of the two purposes. If it were so, they submitted that any data subject could

prevent the proper investigation into serious security incidents that might require the processing of personal data, such as that occurring in this case. Having regard to the fact that the data was processed by the IPS for security purposes entirely in line with the purposes for which the CCTV footage was collected by the Hospital, and that there was in the Respondent's view appropriate signage in place to make data subjects aware of the purpose of processing, and therefore there was no failure to have appropriate safeguards in place.

17.10 The Appellant submitted that the Decision erred in concluding that the use of the information gathered from the CCTV footage in disciplinary proceedings did not constitute a different purpose as it arose in the same context of handling the security incident where these were clearly separate and distinct purposes. However, the Respondent submitted that in concluding that the use in the disciplinary proceedings did not constitute a different purpose to the use in the investigation of the security incident, the Respondent did so on the basis that, in a case of this kind, "*security issues and disciplinary issues may overlap*".

17.11 In this respect the Respondent submitted that while there may be different approaches to characterising the use and purpose of processing in a particular context, it was submitted that it is clear from the judgment of the Court of Appeal in *Doolin* that, if and insofar as there is further processing of personal data, the critical question is whether such processing is incompatible with the purposes for which the personal data was originally processed.

17.12 Therefore, in the Respondent's submission even if in this case the security and disciplinary purposes may be regarded as separate and distinct purposes, the critical question is whether the use of the CCTV for disciplinary purposes in this instance is incompatible with the security purposes for which the data was originally collected and accessed by the IPS.

17.13 Contrary to the Appellant's submissions, it was submitted by the Respondent that the use of the personal data from the CCTV footage in the disciplinary proceedings was not

incompatible with the security purposes for which the data was originally collected and accessed. The Respondent submitted that as the Court of Appeal held in Doolin, in the event that an employee faced disciplinary proceedings for doing the very thing that gave rise to the security issue in the first place, "*it could not be argued that the CCTV was being used for an unspecified purpose or one that was incompatible*".

17.14 The Respondent submitted that in contrast to the position in *Doolin*, there was a clear and inescapable linkage between the use of the CCTV footage for the investigation of the security incident and its use in the context of the disciplinary proceedings directly arising from that security incident. In circumstances where the data was collected for security purposes and not used in a manner incompatible with those purposes, the processing cannot be regarded as running contrary to the reasonable expectations of a data subject as to further use. For similar reasons as outlined above, having regard to the nature and gravity of the incident, this suggests that there is no basis for contending that the potential negative impact on the Appellant weighed against the compatibility of the two purposes. If it were so, they stated that any data subject could prevent the proper investigation into serious security incidents that might require the processing of personal data, such as that occurring in this case.

17.15 Having regard to the fact that the data was never processed in a manner incompatible with the purposes for which the CCTV footage was originally collected, that there was in the Respondent's view appropriate signage in place to make data subjects aware of the purpose of processing, and that the Appellant was duly informed by the IPS of the position, they submitted that there was also no failure to have appropriate safeguards in place.

17.16 The Respondent also submitted that there is an acknowledgement by both parties that, in accordance with Article 5(1)(a) GDPR, any processing of personal data must not only be lawful (in the sense of having a legal basis) but also must be fair and transparent. They also

state that there is also agreement that Article 14 of the GDPR lays down certain requirements regarding the information to be provided where personal data have not been obtained from the data subject. However, the Respondent submitted that it is important to underline that those requirements are not absolute and, in accordance with Article 14(5), they do not apply in certain circumstances such as where the data subject already has the information, or the provision of such information proves impossible or would involve a disproportionate effort. In considering these issues, the Respondent further submitted that it is necessary to take account of the specific circumstances and context in which the processing of personal data takes place, which has a significant effect on whether and how information may be provided to data subjects. In this regard it was further submitted by the Respondent that the Appellant has not identified any serious and significant error or series of such errors in the Respondent's findings in respect of the principles of fairness and transparency.

17.17 The Respondent stated that with respect to the fairness of processing, the Appellant's complaint on appeal overlaps significantly with its complaint that there was a breach of the purpose limitation principle. For similar reasons to those set out above in the context of purpose limitation, it was submitted by the Respondent that there is no basis for impugning the conclusion that the processing undertaken in this case was fair and cannot properly be regarded as contrary to the reasonable expectations of a data subject in this specific context.

17.18 With respect to the transparency of processing, as stated above, the Respondent states that it was necessary to assess compliance with this principle by reference to the specific circumstances and context in which the processing of personal data takes place. In this case, the Respondent stated that it was entitled to conclude that, by informing the Appellant at an early stage of the position in respect of the investigation, the IPS had complied with the requirements of transparency. Having regard to the nature and gravity of the security incident

in question, and all the circumstances of this case, it further submitted that it would not be reasonable for the Respondent to impose a more onerous standard on the data controller.

17.19 With respect to Article 14 of the GDPR, the Respondent submitted that as noted in the Replying Affidavit sworn on behalf of the Respondent, in the complaint lodged with the Commission on 19 June 2019, no specific complaint was made in respect of alleged contraventions of Article 14 of the GDPR. While it acknowledges that the issue was raised in the course of subsequent submissions, it submitted that the fact that the Respondent did not specifically address this further issue in express terms in the Decision does not constitute a serious and significant error on the part of the Respondent, particularly having regard to the number and breadth of the Appellant's grounds of complaint.

18. <u>Lawful Basis for Processing: Hospital</u>

18.1 First, according to the Respondent the Appellant alleges that the Respondent erred in concluding that the Hospital had a lawful basis under Article 6(1)(d) of the GDPR for disclosing the CCTV footage, which contained personal data relating to the Appellant, to the IPS. The Respondent therefore submitted that in its Decision, having noted the Hospital's reliance on Article 6(1)(d) GDPR, the DPC concluded that the Hospital had a lawful basis to disclose, and the IPS had a lawful basis to obtain, the CCTV footage in order to assist the IPS in investigating the security breach in line with the legal obligations placed on the IPS in those circumstances.

18.2 The Appellant submitted the Decision of the DPC in this respect is flawed for a number of reasons:

a) First, because the prisoner had been apprehended by the time the CCTV footage was viewed by the Chief Officer on 11 September 2018, it was not necessary to process the personal data in the CCTV stage.

b) Second, as a matter of law, "vital interests" for the purposes of Article 6(1)(d) has a very narrow meaning and there was no evidential basis for finding that the life of any

person was in danger as a result of the prisoner's escape, all the more so after the prisoner was apprehended.

c) Third, the vital interests legal basis can only be relied upon to justify processing which cannot be manifestly based on another legal basis.

18.3 The Appellant submitted that it is well established that, where a data controller processes personal data falling within the scope of the GDPR, the data controller must have a legal basis for processing. This requirement stems from the general principle of lawful, fair and transparent processing enshrined in Article 5(1)(a) GDPR, which is given further effect in the terms of Article 6 of the GDPR.

18.4 Article 6 of the GDPR provides an exhaustive list of legal bases which may be relied upon by a data controller for the purposes of processing personal data. Under Article 6(1)(d), processing shall be lawful where "*processing is necessary in order to protect the vital interests of the data subject or of another natural person*".

18.5 Recital 46 provides that processing should be regarded as lawful "*where it is necessary to protect an interest which is essential for the life of the data subject or that of another person*" and that processing on the basis of the vital interests of another natural person "*should in principle take place only where the processing cannot be manifestly based on another legal basis*". They suggest that examples of situations where processing of this kind may be justified include monitoring epidemics and humanitarian emergencies (including situations of natural and man-made disasters).

18.6 In respect of the complaint that the vital interest's legal basis could not apply because the prisoner had been apprehended prior to the viewing of the CCTV footage, it was submitted that, in its letter of 16 December 2020 cited in the Decision, at the time of the viewing, the Hospital was not aware that the prisoner was no longer at large. The Hospital's position - that

"*in reply to the emergency situation, it was considered that the viewing was in the vital interests of the general public in order to safeguard the general public*" - provided a valid basis for reliance on Article 6(1)(d) GDPR. The Respondent stated that the Hospital has at all times emphasized the threat to public security presented by the escape of the prisoner. They also state that in any event, in light of the nature and gravity of the security incident entailed by the escape of a prisoner in this particular setting, the risk presented for staff and service users in the Hospital and other persons, and the importance of a proper investigation into this incident, it was submitted that, notwithstanding the fact that the prisoner had been apprehended shortly before the viewing of the CCTV footage in this case, reliance on this legal basis on the part of the Hospital remained valid at the time the viewing occurred.

18.7 The Respondent stated that while acknowledging that the concept of "*vital interests*" for the purposes of Article 6(1)(d) is narrowly interpreted, the very nature and gravity of the security incident at issue in this case, the escape of a prisoner in a hospital setting, was such as to give rise to a real risk to the vital interests, in particular the life and safety, of members of the public. In these circumstances, the Respondent stated that it is not necessary for the Hospital to provide specific evidence of a risk to the life of a particular individual or individuals in order to rely on this legal basis; the threat to public security, including to the life and safety of members of the public, was manifest. They also submitted that the Appellant's approach would represent an overly restrictive application of Article 6(1)(d) which is not consistent with its purpose.

18.8 While it was acknowledged that Recital 46 of the GDPR signals that the vital interest's legal basis should be used only where another legal basis is not available, the Respondent stated, that it is not a formal condition for reliance on Article 6(1)(d) GDPR that no other legal basis is available. They submitted that it is settled law that, while recitals in EU legislation are an aid to an interpretation, they have no binding legal force. Nevertheless, in this case, the

Respondent submitted that it does not appear that the Hospital considered that another legal basis was available to it. This being so, even if the principle laid down in Recital 46 of the GDPR was binding, the Respondent states it is not apparent that the processing by the Hospital could have been "*manifestly based on another legal basis*".

19. <u>Lawful Basis for Processing: the Irish Prison Service</u>

19.1 The Respondent submitted that the DPC decision concluded that the prison service did have a legal basis under Article 6(1)(e) i.e. in the public interest or exercise of official authority which is founded on EU law or domestic law. Thus, they submitted that the criteria outlined in Section 38 of 2018 Act, for processing a task in the public interest or in the exercise of official authority, was met and was necessary and proportionate. In respect of the Prison Rules and specifically Rule 83(1), they submitted these individual provisions work together to form a legal basis for the processing involved.

19.2 In respect of the Appellant's submission that there was no evidence that the IPS informed the Minister in writing of the report, the Respondent replies as follows: the DPC's decision is not premised on the Governor of the Prison writing to the prisoner. Rather the issue is whether the Governor considered it might be an issue that should be brought to the attention of the Minister for Justice. Therefore, in regard to Rule 83(1) such processing is necessary and proportionate to perform this function. In short, the IPS must use all information available.

19.3 The Respondent submitted that it flies in the face of common sense if the IPS was not entitled to access CCTV in these circumstances to investigate the incident. They stated that there was a clear legal basis identified in the decision and the Appellant according to the Respondent has not identified any error, not less a significant error.

19.4 The Appellant submitted that the parties are not entitled to rely on this legal basis where there has not been compliance with Article 5 i.e. there must be transparency and the IPS ought to have notified the Appellant.

19.5 The Respondent submitted in reply that this proposition should have been tested against reality. The question they suggest should be "Is it practical that he should be so informed prior to the downloading of the CCTV?" The Respondent submitted that this gives rise to a real air of unreality. In other words, they state that that there is conflation of the requirements of transparency and legal basis. While acknowledging that it is good practice to note the legal basis beforehand where possible, they submitted that there will be circumstances where it is not practical or possible to inform a data subject in advance and that is why there are data protection policies.

19.6 The Respondent notes that the DPC concluded the prison service had a legal basis under Article 6(1)(f) to process the data in its disciplinary investigation. In this regard the Appellant states the prison service is a public authority and cannot rely on Article 6(1)(f). The Respondent acknowledges that this is a correct interpretation in that they cannot rely on Article 6(1)(f) in the performance of its public duties. However, they refer to the purpose of Recital 47. Therefore, the Respondent submitted that the limitation relates to situations where the public authorities are carrying out tasks in the public interest and that this is apparent from various user Information Documents and specifically referenced Guidance Documents from DPC on various legal issues. In this regard they state that page 21 leaves open for public authorities to use this basis if not performing public tasks. The Respondent states that it is clear from reading paragraph 14 and 15 of DPC's decision that the DPC is concerned with the IPS's role not as public authority but as an employer.

19.7 The Respondent also submitted that the "legitimate interests" were identified by IPS in the early stages. It is acknowledged that they initially relied on Article 61 and the DPC agrees with the Appellant that this was not possible. However, they suggest that the DPC are not precluded from identifying another legal basis. In the Respondent's submission there is therefore a clear legitimate interest.

19.8 In regard to the change of use of the data i.e. the use of data for public security and then use of it for the purposes of an employment issue, the Respondent submitted it is possible to rely on more than one basis and referenced Advocate General Bobek's Decision in the Rigas Case (*Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde -v- Rīgas pašvaldības SIA 'Rīgas satiksme'*)

19.9 The Respondent also submitted that even if the Court was not prepared to accept this submission, the Respondent suggest it could query if there was any other legal basis available such as the legal obligation carrying out tasks in the public interest. They submitted that it is relevant because of the new remedial flexibility under the 2018 Act in reviewing the DPC decision. However, they stress this is very much a fall back submission, and they state that they are firmly of the view that the DPC was correct in relying on Article 6(1)(f).

20. <u>Transparency</u>

20.1 It was alleged by the Appellant that the Respondent erred in its conclusion on the question of transparency of the processing. In its Decision, having set out the measures taken by the Hospital to bring the operation of the CCTV to the attention of data subjects, the Respondent concluded that, for the purposes of the requirements of transparency under Article 5(1)(a) GDPR, there was "*adequate signage ...in place at the time of the incident*".

20.2 However the Appellant submitted that the Decision in this respect is flawed for a number of reasons:

a) it was submitted that there was no evidence in the Decision that the Hospital had provided the Appellant with the identity of the data controller or the purpose of processing in compliance with Articles 5 and 13 GDPR.

b) it was submitted that there was no evidence in the Decision that the Appellant was given notice in advance of the original processing, the possibility of disclosure of the personal data to a third party and the purposes for which it could be processed.

c) it was submitted that there was no evidence in the Decision that the Hospital had a data protection policy relating to the disclosure of personal data to third parties.

20.3 The Respondent acknowledges that there is no dispute that, in accordance with Article 5(1)(a) GDPR, any processing of personal data must not only be lawful (in the sense of having a legal basis) but also must be fair and transparent. It pointed out that for its part, Article 13 of the GDPR lays down certain requirements regarding the information to be provided where personal data have been obtained from the data subject. In accordance with Article 13(4), these requirements do not apply where the data subject already has the information.

20.4 However in considering these issues, the Respondent stated it is necessary to take account of the specific circumstances and context in which the processing of personal data takes place, which has a significant effect on whether and how information may be provided to data subjects. Thus, for example, they submitted that in the case of CCTV footage, it will not be possible for a data controller to provide information to every data subject on an individualised basis and the requirements of transparency must generally be met through adequate signage providing the data subject with a first layer of information and on the basis of which the data subject can seek such further information in respect of the processing as the data subject considers appropriate or necessary in a given case.

20.5 The Respondent submitted that the Appellant has not identified a serious and significant error in the Decision in this respect which would justify allowing this appeal. They state that the three grounds of appeal under this heading all raise a similar issue: the alleged lack of evidence in the Decision that the Appellant was provided with certain information (such as the identity of the controller or the purposes of processing), that the Appellant was made aware in advance of the processing, and that the Hospital had a data protection policy in place.

20.6 However, the Respondent submitted that it is important to have regard to the particular context and circumstances of the processing at issue in this case. In the case of CCTV footage, they reiterate that it is not possible or practicable for such information to be provided to data subjects on an individualised basis, as they say the Appellant alleges. Instead, the Respondent submitted that the requirements of transparency are instead met through the placing of appropriate signage at the location(s) in which CCTV operates, which provides a first layer of information. This, the Respondent states makes data subjects aware of the processing and allows them to make further inquiries with the data controller insofar as they may consider appropriate or necessary. In these circumstances, the fact that there was no specific evidence of the matters identified by the Appellant does not, in the Respondent's submission breach the requirements of transparency or call into question the Respondent's conclusion on this issue.

20.7 In this case, it does not appear that the Appellant sought any further information from the Hospital until a dispute arose between the Appellant and his employers and his solicitors were retained. In other words, the first time on which the Appellant raised the alleged issues of transparency was a number of months after the processing took place.

21. <u>Submissions on behalf of the Health Service Executive, a Notice Party</u>

21.1 The Health Service Executive (the "HSE") was added as a Notice Party by Order of the Court dated 13 October 2022. It was submitted that the issues should be adjudicated in the absence of any further affidavit evidence from the HSE and without necessarily embarking on

a substantive examination of whether the Hospital were in compliance with its obligations to the Appellant pursuant to the GDPR. Essentially they have argued the issues subject of the Appeal are as between the Appellant and the Respondent with respect to the DPC's decision and whether same is erroneous in a serious and significant way and that the information that was available to the DPC at the time its decision was rendered. Many of the points raise by the HSE have been made by the Respondent above but for the sake of completeness are also outlined below.

21.2 Article 5 of the GDPR provides, inter alia, that data "*shall be processed lawfully, fairly and in a transparent manner*". Article 6 of the GDPR provides that processing shall be lawful only if and to the extent that one of the lawful bases therein set out applies. Article 6(1)(d) of the GDPR provides that processing will be lawful where the "*processing is necessary in order to protect the vital interests of the data subject or of another natural person*". Recital 46 provides that processing should be regarded as lawful "*where it is necessary to protect an interest which is essential for the life of the data subject or that of another person*". Further, processing of personal data on the basis of the vital interests of another natural person "*should in principle take place only where the processing cannot be manifestly based on another legal basis*".

21.3 Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters. The HSE submitted that it is not apparent what other legal basis the Appellant may assert should have applied or been relied on instead of Article 6(d) of the GDPR.

21.4 The Appellant has submitted that the Respondent ought not to have determined that the Hospital had a lawful basis for processing the Appellant's personal data by disclosing it to the Irish Prison Service (the "IPS"). In this regard, they state it that it should be noted that the nature of the processing was limited to permitting the Chief Officer to view the CCTV footage on 11 September 2018. The limited nature of the processing was referred to in a letter dated 1 December 2020 from the Solicitors for the HSE who confirmed to the Solicitors for the Appellant that a copy of CCTV footage was not provided to the Chief Officer or any other member of the IPS.

21.5 The HSE stated that the Appellant submitted that the Hospital was not entitled to rely on Article 6(1)(d) of the GDPR in circumstances where the prisoner had been apprehended one day prior to the disclosure of the CCTV footage by the Hospital to the IPS and the purported legal basis did not exist at the time of the said disclosure. However, the HSE submitted that the Hospital had a lawful basis to disclose the CCTV footage to the IPS in that it understood at the time that access was required in order to assist the IPS in investigating the security breach in line with the legal obligations placed on the IPS in those circumstances. In this regard, in the letter dated 26 March 2019 the Solicitors for the Hospital confirmed to the Solicitors for the Appellant that:

> "*a prisoner of Castlerea Prison escaped from the emergency department of Mayo University Hospital and that during the search for the prisoner, the Irish Prison Service…requested access to the relevant CCTV footage in order to protect and safeguard the public and to apprehend the prisoner*"

21.6 The HSE point out that the DPC found that this constituted a lawful basis to disclose the CCTV footage to the Chief Officer "in light of the security incident" and quoted them as follows :

"*Accordingly, the IPS had a lawful basis to obtain, and the Hospital had a lawful basis to disclose, the CCTV footage to the IPS to aid them in their full investigation of a security breach in fulfilment of legal obligations placed on the IPS in such circumstances*"[4].

21.7 The HSE submitted that insofar as the Appellant may assert the lawfulness of the Hospital's decision to allow the CCTV footage to be viewed was vitiated by the prisoner being apprehended on the night of 10 September 2018, or that there was no longer a necessity to process the data at that stage, they replied that the Hospital was not aware at the time of the viewing that the prisoner had been apprehended. They also point out that it was accepted that if it had been so aware then the basis for allowing access to the CCTV footage would have had to have been reviewed and it may be that the agreement to provide access may have had to have been rescinded.

21.8 The HSE also submitted that there is no authority for the proposition that a lawful basis for processing data is vitiated merely when circumstances relating to the said lawful basis, about which the data controller was unaware, have changed without the knowledge of the controller. As the reasoning in support of granting access to view the CCTV footage remained in place at the time it was being viewed so too according the HSE did the lawful basis remain.

21.9 The Appellant submitted that there was no evidential basis for finding that the life of any person was in danger because of the prisoner's escape. However, the HSE submitted that the Hospital were at all times concerned about matters of public safety and the safety and security of its own staff. In the letter dated 16 December 2020 the Hospital stated that it was not aware that the prisoner had been apprehended and that "*in reply to the emergency situation, it was considered that the viewing was in the vital interests of the general public in order to*

safeguard the general public". The HSE therefore submitted that this formed a sound, logical and lawful basis for the Hospital granting access to view the CCTV footage.

21.10 The HSE further submitted that the information received from the IPS constituted evidence that the safety and security of the public and staff were at risk. Moreover, given the nature of the information that it received from the IPS the HSE state that the Hospital reasonably apprehended a risk to the safety and security of the public and staff and were therefore justified in relying on Article 6(1)(d) of the GDPR in order to allow the CCTV footage to be viewed.

21.11 In addition, the HSE submitted that quite apart from the apparent danger which an absconding prisoner could have exposed the public generally to, the Hospital was justified and obliged to act in a manner to ensure they provided their staff then present with a safe and secure place of work. It was therefore submitted that Article 6(1)(d) of the GDPR provided the Hospital with a lawful basis to process the Appellant's data, in that the Hospital understood and believed that the absconding prisoner presented a real risk to the "*vital interests*" of the public and staff, and in particular their safety and security.

21.12 Like the Respondent the HSE accepted that the concept of "*vital interests*" for the purposes of Article 6(1)(d) of the GDPR should be narrowly interpreted but the situation that arose was one involving the apprehension of immediate and significant risk to the safety of the public and staff. Therefore, the HSE submitted that it would be unreasonable to have expected the Hospital to have demanded of the IPS some form of tangible evidence of such risks as opposed to relying on a statement made by and on behalf of the IPS such that a prisoner had absconded from the Hospital and according to them "was on the loose". The HSE pointed out that the purpose of Article 6(1)(d) of the GDPR is to provide expressly for circumstances where there is a risk to life or health, and in their view, it would undermine such purpose to require

data controllers to delay the process to investigate matters when an urgent risk arose for consideration.

21.13 The HSE stated the Appellant has submitted that the Hospital failed to lawfully and properly interpret, apply and address the requirements of Article 5 and Article 13 of the GDPR. The Appellant further alleged that the Respondent erred in its conclusion on the question of transparency of the processing and that that there was no evidence in the Decision that the Hospital had a data protection policy relating to the disclosure of personal data to third parties.

21.14 The HSE stated that in its Decision, the DPC noted the response to their enquiries to the Hospital as to the issue of signage. In the email dated 16 December 2020 the Hospital responded as follows:

> "*I wish to advise that there was signage in place advising that CCTV is in operation at the Hospital site.*
>
> *The notification/wording on main sign(s) is as follows: 24-hour CCTV footage in Operation camera image. These signs were provided by a professional company under mounted on permanent structures. The signs are 16" X 16" in dimension and are placed at 6 locations around the grounds of the Hospital. The locations include, along the roadway into the Hospital, at car parks and some entry doors. Another sign dimensions 8" X 8" is at the main entrance door of the Hospital*."

21.15 The HSE submitted that the DPC considered that in those circumstances there was "*adequate signage ...in place at the time of the incident*". Therefore, the HSE submitted that the presence of these signs does constitute a clear and transparent notification to the Appellant as to the collection of his personal data.

21.16 The HSE accepted that there is no dispute that, in accordance with Article 5(1)(a) of the GDPR, any processing of personal data must not only be lawful (in the sense of having a legal basis) but also must be fair and transparent.

21.17 The HSE also submitted that it is accepted that Article 13 of the GDPR sets out the requirements with respect to the information that a controller must provide to a data subject with respect to the processing of his/her data but they further submitted that it is not required to ensure that each and every possible occasion on which data may be processed is set out or that each potential data subject is individually notified of the basis on which the data controller relies and the circumstances in which the data may be processed or indeed the entire gamut of potential reasons why personal data may be processed. Therefore, the HSE submitted that the provision of the signage in this case complies with Article 13 of the GDPR.

21.18 The HSE acknowledged that it was submitted that the Hospital would have had, and has, an obligation to provide clarification to any queries raised in order to ensure compliance with the requirement that the processing is "*lawful, fair and transparent*". However, they pointed out that there is no evidence that the Appellant ever requested, prior to the processing taking place, clarification from the Hospital with respect to the nature of the processing of his personal data. In addition, they stated that the HSE's Data Protection Policy is a publicly available document available online.

22. <u>Submissions on behalf of the Irish Prison Service, a Notice Party</u>

22.1 At the hearing of the appeal, the IPS took no issue with the factual background, and they supported the DPC's decision and DPC's legal submissions. However, they emphasised several points. First, in relation to the significance placed by the Appellant on the prisoner being already apprehended when the CCTV footage was accessed, they stated that the footage would have to be viewed in respect of an investigation of the incident, regardless of the apprehension of the prisoner.

22.2 In addition the escape of a prisoner would have been deemed a safety and security issue and it would be necessary to review the CCTV footage to ensure standard operating procedures were followed correctly and to ensure this does not happen again.

22.3 The IPS reiterated the submission made by the DPC that the viewing of the footage for security purposes and also the disciplinary purpose is compatible, and this complies with the compatibility test laid down by the Court of Appeal in the *Doolin* case. The disciplinary proceedings arise from the security issue.

22.4 In respect of Recital 39 of GDPR, they submitted it must be abundantly clear to a prison officer who knows that there is CCTV footage and who also knows a prisoner has escaped, that CCTV will be used to investigate the incident and disciplinary processes will flow.

23. <u>Court's Decision</u>

23.1 This case raises the following question. Was the processing by the Hospital of the Appellant's personal data in the form of CCTV footage which was collected for security reasons by the Hospital and then provided to the Appellant's employer, the IPS, contrary to the requirements of Data Protection law when used in disciplinary proceedings against the Appellant?

23.2 The Appellant firstly makes the case that when the CCTV was viewed by the IPS the immediate threat to security had passed as the escaped prisoner had been apprehended and it was not a security issue when the IPS viewed the CCTV. Secondly the Appellant further argues that even if the court held it was still for permissible use i.e., to prevent crime and promote staff security and public safety, that information derived from same was unlawfully further processed for the purpose of disciplinary action against him as an employee of IPS which was a different purpose than that for which it was collected.

23.3 In summary the appeal concerns an allegation of misuse of data collected on a security camera for the purposes of disciplinary proceedings against the Appellant as an

employee which he claims, this was done without his permission.

23.4 Although the legal principles governing lawful processing under the GDPR and the 2018 Act are broadly accepted by both parties, there is a considerable divergence of view on the application of these principles by the Circuit Court. In the Court's view, the 2018 Act has not substantially changed the principles as laid down by O'Donnell J [as he then was] in the Supreme Court in *Nowak v. Data Protection Commissioner* [2016] 2 IR 585 ("*Nowak*"), following that promulgated by Keane CJ in Orange v. Director of Telecommunications Regulations [2000] 4 IR 159 at pages 184 to 185 ("*The Orange Test*"). The 2018 Act has given the Court the option to impose its own decision instead of either just accepting or rejecting the decision of the Respondent. That does not broaden the test in the sense of re-examining every factual issue de novo. What it does is allow for the Court based on the facts already established to modify, correct, or even change the Respondent's decision if the principles of justice or equity require it.

23.5 The second issue is the application of the principle of purpose limitation in circumstances where the Appellant's data was processed more than once. The principle of purpose limitation was considered by the High Court (Hyland J.) in *Doolin v Data Protection Commissioner and Another* [2020] IEHC 90 and later on appeal by the Court of Appeal in a judgment by Noonan J. ([2022] IECA 117). In that case the DPC appears to have considered that there was one investigation only into security and therefore the outcome of that investigation must be regarded as security related and thus satisfied the purpose specification. However, both the High Court and the Court of Appeal held that there were plainly two investigations or at a minimum, one investigation into different matters. In that case it was clear to both the High Court and Court of Appeal that where there are two investigations, it cannot be said the investigation singular was for the purpose of security and that the processing of Mr

Doolin's data was not for a security purpose as the DPC contended. It was for a different purpose.

23.6 In her judgment in the High Court, Hyland J referred extensively to the concept of purpose limitation as explained by the Working Party 29 group ("WP29"), a group of experts from the Member States (now re-named under the GDPR as the European Data Protection Board) that from time to time issue opinions on aspects of Directive 95/46, and now on the GDPR.

23.7 Referring to Opinion 3/2013 on purpose limitation 00569/13/EN WP 203 (the "Opinion") at paragraph 22 of her judgment, Hyland J stated:

> "The Opinion goes on to identify four key factors to be considered during the compatibility assessment:
>
> - The relationship between the purposes for which the data has been collected and the purposes of further processing. The Opinion explains that the greater the distance between the purposes of collection and the purposes of further processing, the more problematic this would be for the compatibility assessment.
> - The context in which the data have been collected and the reasonable expectations of the data subjects as to their further use. Here the Opinion explains that the issue here is what a reasonable person in the data subject's situation would expect his or her data to be used for based on the context of the collection. Generally, the more unexpected or surprising the further use is, the more likely it is that it would be considered incompatible. Further the balance of power between the data subject and data controller should be considered and in particular, an investigation should be made as to whether the data subjects were obliged to provide the data under law. The more specific and

restrictive the context of collection, the more limitations there are likely to be on further use.

- The nature of the data and the impact of further processing on the data subjects. Relevant impact may involve the way in which data are further processed. The more negative or uncertain the impact of further processing, the unlikely it is to be considered as compatible use. The availability of alternative methods to achieve the objectives pursued by the controller, with less negative impact for the data subject, would be a relevant consideration.
- The safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects. Appropriate additional measures could serve as compensation for the change of purpose, including additional steps taken for the benefit of the data subjects, such as increased transparency with the possibility to object or provide specific consent."

23.8 And then at paragraph 23 Hyland J stated, "in summary, further processing for a different purpose is not automatically incompatible but must be assessed on a case-by-case basis."

23.9 However, the Court of Appeal went further, and Noonan J stated at paragraph 84 of his judgment:

> "It will be recalled that the High Court held that the evidence indicated that the use of the information from the CCTV footage was used for an entirely different purpose to that for which it was collected. The DPC is correct in arguing that the mere fact that the data were used for a different purpose does not mean that the use was unlawful. It is only where the further processing occurs in a manner incompatible with the stated purpose that an illegality arises."

23.10 In other words, it is necessary for the DPC, or in this case this court, to carry out a compatibility analysis and noting one was not carried out by the DPC. In doing so it is instructive to look at paragraph 89 of the judgment of Noonan J. in *Doolin* where he stated:

> "Counsel for the DPC suggested that on the logic of Mr. Doolin's argument, if he had been detected on the CCTV carving the graffiti into the table, while he might be amenable to criminal sanction, he could not be disciplined for the same thing. While there may be a superficial attraction to that argument, I think, on analysis, it is misconceived. In such a scenario, the employee would face the disciplinary process for doing the very thing which gave rise to the security issue in the first place. In that event it could not be argued that the CCTV was being used for an unspecified purpose or one that was incompatible."

And at paragraph 90 where Noonan J stated:

> "That appears to me however to be a world away from this case. The fact that the viewing of the CCTV here was for the purpose of attempting to detect the perpetrator of the offensive graffiti and damage to Hospice property is entirely irrelevant to the incidental observation of Mr. Doolin taking unauthorised breaks. As I have already said, and as the High Court found, there was absolutely no evidence that the taking of such breaks represented a security issue in itself."

24. <u>Applying the law to the facts in this case</u>

24.1 In this case there is no dispute but that the specified purpose for collecting the data was that of security. This is clear from the notices [though I accept they could be more expansive in their purpose]. I have no doubt from the evidence furnished to the court the Appellant was aware that CCTV was used and that it was for security purposes. I accept that when the IPS first requested the CCTV from the Hospital, the Hospital was led to believe the prisoner was

still at large, but at the time of release of the CCTV the prisoner was apprehended. I believe it flies in the face of common sense to suggest that once the prisoner was captured there was no need to give the CCTV to the IPS. The Hospital have a clear duty of care to patients, staff and the public. While it would far be preferable that the Hospital was aware of the up to date situation, nonetheless it seems to me the IPS and the HSE would have been negligent not to investigate this serious incident to ensure this situation was not repeated. In reality the release of the CCTV by the Hospital was for the purpose, which was known, namely security. I am also conscious that the timeframe between the escape of the prisoner and the viewing of the footage of a day was reasonable.

24.2 However the real question in this case is the further use of the CCTV by the IPS in disciplinary proceedings against the Appellant for a different purpose. The legal basis must be clear. In addition, it does not appear the Respondent carried out a compatibility test as envisaged by *Doolin*. While the Decision in this case was after the High Court decision in Doolin and before the Court of Appeal decision, it is not clear to the court why the Respondent failed to do so. This was a matter the Respondent was aware of and also noting that it was the DPC who submitted to the Court of Appeal in Doolin the importance of carrying out the compatibility test in that particular case.

24.3 There is also the issue of transparency which means that individuals have the right to be informed of the processing of their data. The Appellant submitted that he was not asked for his consent before the disciplinary proceedings. The IPS placed reliance on Rule 83(1) of the Prison Rules in that the Governor was obliged to carry out an investigation to notify the Minister of the incident.

24.4 A common legal basis on which employers place reliance is the ground of legitimate interests (Article 6(1)(f) of the GPDR). In this regard and noting we are now dealing with an

employment issue as opposed to the public interests of safety, a legitimate interest assessment should be carried out by the IPS to demonstrate that it is genuinely in their interests to utilise the CCTV and that it will not have a disproportionate impact on the data subject. In addition, the use of the CCTV must be necessary for the given purpose and proportionate.

24.5 In considering legitimate interests, the Court should also consider Recital 47 EU GDPR which states:

> "the legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationships with the controller.
>
> Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller.
>
> At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.
>
> The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.
>
> Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks.

The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned.

The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest."

24.6 Taking all of these issues into account, I am satisfied that that the Appellant was aware that CCTV was used for security purposes in the Hospital and that the nature of his employment and knowledge meant that there was a reasonable expectation that the CCTV could also be used in any investigation of a breach of that security. However, it is also necessary to carry out a compatibility analysis. In this regard I am satisfied provided that the CCTV is used solely to deal with the security issue that arose in the Hospital during the period the prisoner escaped, it is compatible with the specified original purpose of collecting the CCTV and therefore it is not unlawful. Nonetheless, it would not be compatible to use the CCTV for any other propose than a security breach. Therefore, I agree with the Respondent's decision and accordingly it is not in the Court's view necessary to annul or modify the Decision under Section 150(6) of the 2018 Act. In this respect, I therefore dismiss the appeal.

24.7 However, as the Respondent failed to carry out the compatibility test in reaching its decision, I also accept clarification of the Decision was required from the Circuit Court. I invite the parties to suggest the appropriate wording for the Court Order to reflect this appeal decision. In addition, I will also hear submissions from the parties as to the appropriate costs order to be made.