THE CIRCUIT COURT
[AN CHUIRT CHUARDA]

DUBLIN CIRCUIT **COUNTY OF CITY OF DUBLIN**

IN THE MATTER OF AN APPEAL UNDER SECTION 26 OF THE DATA PROTECTION ACTS 1988 AND 2003 BROUGHT PURSUANT TO ORDER 60 THE CIRCUIT COURT RULES

THE COURTS SERVICE

Appellant

-and-

THE DATA PROTECTION COMMISSIONER

Respondent

-and-

P.M.

Notice Party

Ruling of Judge Comerford delivered in Dublin on the 3rd day of February, 2020.

This is a court ruing concerning the difficulties that can arise from the dissemination of a court judgement. The point directly at issue is that Respondent has made a decision that the Appellant uploaded a Court judgement on a website in 2014 in a manner that breached the data protection legislation which then applied. This was the pre-GDPR regime. The breach identified involved the disclosure of personal data concerning the Notice Party. The matter at issue in these proceedings relates to the interplay, if any, between the pre-GDPR data protection rules and the publication of a court judgement on a website. The rules under consideration are the data protection Acts 1988 and 2003, which is really the 1988 Act as amended by the 2003 Act but it seems to be commonly referred to as the 1988 and 2003 Acts. It is a feature of this regime that this may involve consideration of the then applicable relevant European directives which had primacy over the Irish legislation.

2. Before considering, the issues relating to the Data Protection Acts, I wish to first set out my understanding of the way that the dissemination of judgements evolved prior to the impact of technology and the data protection rules. These comments are not evidence in this appeal, and are not matters that have to be determined in the appeal, which is focused solely on a legal evaluation of the decision made by the Respondent. All these comments do is provide an indication of the background and context in which the evaluation takes place. Historically, when a pronouncement by a court was made, the operative order of the Court was recorded by court officials. This was the

necessary and essential recording of decision that had to be done for the purposes of the administration of justice and to give effect to that specific ruling . A common law system, based on precedent, requires more than this. For the operation of precedent to work, the reasoning behind the decision must also be available so that the law may be known. For this purpose, going back to the 1600's and 1700s and perhaps before, private individuals attended at courts and recorded the reasoning of the judges as part of recording the overall case and these booklets of law reports became the source material for the development of the law. It may have been that judges or court officials facilitated this process by furnishing copies of judgements on occasion and certainly at some point, a practice evolved in some courts of holding a copy of the judgement on file. As the law evolved, the system of law reporting became more formalised with recognised commercial or institutional bodies preparing recognised law reports often with semi-official status. This were commonly made available for purchase usually by subscription. This was in parallel to those cases where approved copies of the reasoning were kept on file, and that obligation too developed and it is now a recognised requirement of the Irish legal system that a Judge of the Superior Courts make an approved copy of a reasoned judgement available. This was recognised by O'Donnell J in the case of DPP v Nash [2017] IESC 51. The maintenance on file was part of the official functions of the Court Officials. A practice also evolved whereby court officials made copies of such judgements available to bodies that produced written reports such as the Irish Reports.

3. These law reports recorded judgements which were pronounced in public by a judge at a hearing which in save in circumstances prescribed by law, was required by the Constitution to be conducted in public. The general rule then was that was whatever was contained in the pronounced judgement could and should be made available to the public. It was always the case though that there were court hearings which were not fully public or which were subject to reporting restrictions. The most numerous of these now are the vast majority of family law proceedings which are held in camera and subject to a settled rule of law that the parties can not be identified. Restrictions also applied, giving non-exhaustive examples, to some types of company law applications, to testamentary proceedings concerned with the make them making a moral provision for children, and a range of criminal proceedings involving certain types of sexual offences and quite extensively in criminal proceedings involving children. There were also classes of proceedings which needn't by law heard otherwise than in public but this could be directed by Court order. By the terms of section 28 of the Data Protection Acts 1988 and 2003, these present proceedings in which this judgement is given, may be heard otherwise than in public. This did not occur in this case but an order was made directing that the identity of the notice party to these proceedings should not be disclosed. In addition to restrictions on the public hearing of classes of cases, a wide range of discrete statutory powers exist which can result in restrictions on the public hearing or as to the identification of persons involved in the litigation.

4. This reality that not all cases can be reported as fully public hearings is a fact that would have to be known by anyone producing and disseminating judgements within law reports. A person producing copies of judgements to be disclosed to members of the public whether commercially or without charge would have to be aware of these classes of cases which could only be reported in a restricted manner and have in place some procedures to ensure that a breach of the law did not occur in the course of reporting the judgement. This obligation not to disclose matters which by law were required to be kept undisclosed existed long before the introduction of any data protection legislation. The precise method by which this obligation might be enforced may not have a well-defined but it would appear that issues of contempt of court would arise and perhaps there might be liability for breach of privacy as a tort or perhaps relief under the tort of negligence. It did occasionally happen that paper copies of a judgement which did require that the identity of the parties be anonymized were circulated

with the name set out in full, but when this happened it was a breach of law. It was also the case that when the judgement in the case was formally reported in one of the established law reports at that time, the persons publishing reports ensured that the report of the judgement was properly anonymized

5. A significant change occurred with the development of the Internet where copies of judgements were made available on various databases, some available only through payment of a fee and others made widely available free of charge. Many courts systems in the world make their judgements available as an official act of Court administration. With the development of the internet, many of the established paper subscription reports fell away but in the round this extensive publishing on the internet was a positive development; making judgements far more readily available to far more people. In many cases there was a loss of formality in the way the judgements were presented and there was perhaps less consideration when judgement being prepared for inclusion on the database. A screen refuses pixels with less vigour than a paper refuses ink. The preparatory work that was done for the printed law reports, in the form of consideration for the preparation of a headnote and checking with the parties if necessary, with this work being done by a qualified lawyer did not carry over in the preparation of the publication of judgement an internet database.

6. By legislation in 1998, there was a change in the manner in which the administration of the courts was conducted. The Courts Service, the Appellant in these proceedings, was established and all court officials from that point on were employees of the Appellant but the work of the Appellant involved far more than just providing Court officials for Court hearings. The functions of the court service included supporting the judiciary, managing the courts and generally this could be described as facilitating the administration of justice but not administering justice.

7. At some point, the Appellant came to establish a database of judgements of the Irish courts readily accessible free of charge to the world. This was a function far more in the nature of that which been carried out by the law reports rather than the function which had previously been carried out by court officials of simply preserving and holding copies of orders and judgements on file. It is clear from the terms of the database maintained by the Appellant that its function is not to make an official recording of operative orders or judgements but the judgements are rather described in a disclaimer on the court service website as "**the judgements available on this site are provided by the Courts service as a convenience reference... They do not purport to be the authorised version. The authorised version of the judgement is that signed or approved by the judge or court concerned and retained in the court records.**" The terms of this disclaimer is taken from the hearing of this appeal and it is set out in the decision giving rise to the appeal. It is clear from those terms that this database is not established for the purpose of the formal of recording orders and judgements as is done by court officials for the direct purposes of the administration of justice. They do not purport to be authorised. They are only a convenient reference. This is part of a useful function of making sources of law readily available to the public. An issue will arise as to whether this is part of the administration of justice or not. It is contended that the only person who can carry out an act performed in the course of the administration of justice is a Judge, so that the administration of justice is coterminous with the functions of a Judge. I lean more to the view that Court officials may carry out tasks that facilitate the administration of justice indirectly and I am not sure that the term the "administration of justice" is used at all times to mean, an act that only a Judge can perform. As concerns, the publishing of Irish judgements, a similar function may have been carried out by court officers prior to the development of the Internet by making unreported decisions available but the maintenance of a database of indicative judgements that do not purport to be authorised does appear to have been a new development.

8. The other development that occurred was the introduction on a graduated basis of data protection laws. This classified a great many persons who had a function in processing the personal data of others as data controllers and this restricted by the law the manner in which the data controller could deal with this personal material. In order to enforce this regime of law effectively, the role of the Respondent was established by law. These functions included an obligation to consider complaints made by members of the public that their personal data had in processed by a data controller in breach of the data protection regime. It was such a complaint concerning asserted processing by the Appellant who was asserted to be a data controller that gave rise to the decision of the Respondent which is under appeal in this case. The core of the complaint is that the Appellant disseminated a judgement and this disclosed the identity of the notice party when by direct order of a Court the judgement should have been anonymised.

9. I should state here expressly that the Appellant's stance in these proceedings is that the data protection legislation have no application to any function it has in disseminating judgements and that the Appellant is not a data controller. One of the basis for which this is argued is that the acts of publishing a judgement is part of the judicial function and so can't be the responsibility of the Appellant who in publishing does not to carry out its own functions but merely follows the direct instructions of a Judge. It does seem though, without expressing any view at this point, on the special Constitutional and statutory position of the Appellant, that as concerns, a wholly private operator of a judgments data base, it is difficult to conclude but that a database of legal judgements would be considered to contain personal data and that such a private operators who processed this data would be a data controller. The application of the data protection regime does not preclude personal data or sensitive personal data being collected, held and disseminated but if the regime does apply, there has to be statutory authorisation found in the data protection legislation.

10. There is a public interest in the dissemination of judgements but if done by a Data Controller or Data Processor and not done in compliance with the legislation, it would be prohibited. I take it that the Respondent these proceedings is indicating that as a rule, there is no difficulty with disseminating judgements, but that if the dissemination, which constitutes an act of processing under the legislation, is done in a way that is not authorised, then a data breach occurs.

11. The regime that applies is that a breach can occur either because of the absence of appropriate procedures to safeguard against a breach or else because an unauthorised act of processing has taken place despite the existence of appropriate procedures.

12. I won't set out the obligations in their precise statutory terms at this point but by broadbrush stroke based only on those terms most relevant to the issue arising in this case, the regime that applies is a follows. The first obligation that a data controller must meet is to have in place, appropriate security measures, to prevent the unauthorised disclosure of data. By reference to the European Directives security measures comprises technical or organisational measures. It is therefore a precondition, regardless of anything else, that these appropriate measures be in place before anything is done with personal data. Everything the private operator of a judgement database who was a data controller did would be prohibited without appropriate security measures and in the context of disseminating judgements some of which have to be redacted, having appropriate procedures in place to avoid unauthorised disclosure would be an essential. At this point, I'm going to express the view that in this context disclosing the identity of litigant who should be anonymized could constitute unauthorised disclosure.

13. However, even if these appropriate measures are in place, there still may be a breach because no system is perfect, and unauthorised disclosure may still take place. The leading textbook on this

legislation "Privacy and Data Protection Law in Ireland" Dennis Kelleher Second Edition 2015 contains numerous references to case studies from the respondent's yearly reports which identify cases where good procedures were set at nought by errors or misconduct by employees who had been properly trained. This is because even if there is full compliance with all the requirements of section 2 which is the section that includes the obligation to have appropriate security measures, processing of personal data can still only be conducted if the conditions set out in section 2A are met. Paraphrasing the most relevant conditions for this dispute, in the case of a private operator of a judgements database this would be that the dissemination was necessary for the purposes of the legitimate interests of the data controller and of the person to whom the data is disclosed, save where this is prejudicial to the general interests of the data subject. If the Appellant was considered ultimately to be a data controller, the most relevant provisions might be that the provision permitting processing that was necessary for the administration of justice or for the performance of a function conferred by statute or for the performance of a function of a public nature performed in the public interest by the appellant. Provided that such a condition is met and that there is compliance with section 2, personal data may be authorised.

14. There is the further possibility of a breach if the personal data constitutes sensitive personal data. It is a precondition that there is full compliance with the obligations under section 2 and section 2A but in addition there must be compliance with one of the conditions set out in section 2B in these conditions include disclosure necessary for the administration of justice or for the performance of a function conferred on a person by enactment or if otherwise necessary for the purposes of establishing exercising and defending legal rights.

15. The regime that applies then is that no personal data can be processed, including by being disclosed to the public, unless there is compliance with s.2. So if personal data is processed in the absence of s.2 there is automatically a breach of s.2A. If there is compliance with section 2 there can still be a breach of s.2A unless one of its conditions that authorise processing is met. If sensitive personal data is processed in the absence of compliance with either s.2 or s.2A, there is automatically a breach of s.2B of but if there is compliance with those sections there still may be a breach under s. 2B.

16 I will point out at this time that the view of the appellant is that this regime is completely irrelevant to its actions in publishing judgements on its website, including because the Data Protection act doesn't apply to this conduct when done by the Appellant, and even if it did there is an exemption which would catch this conduct and therefore exclude the Application of the Acts. The Appellant is also saying that it isn't a data controller in any event and that there was no breaches of any of these sections, and those latter matters fall to be considered later, but prior to making those points there is the contention that the data protection acts have no application to the actions of the appellant which are deemed to be a breach.

17. I'm going to deal with the contentions of non-applicability and exemption at this point as these do have the potential to be determinative of this appeal. I should point out that these contentions were raised at a very late point, only at the first day of hearing of these proceedings. The contention was not raised in communications with the respondent during the course of its investigation, there are matters of law but they were not prefigured in any way in the affidavits filed in this appeal and they were not referred to in the legal submissions received by the circuit Court office on 14 February 2019, just under two months before the hearing, four and a half years after the Appellant was first notified of the complaint. Neither the respondent or notice party make any procedural objection to this issue being raised before me.

18. The contention for non-applicability is based on s.1(4)b which provides:-

(4) This act does not apply to –

...

(b) personal data consisting of information that the person keeping the data is required by law to make available to the public,

19. I'm rejecting the contention of non-applicability on the basis that the appellant has not satisfied me that the keeping of a judgement database of judgements not purporting to be authorised and for the purpose of convenience reference is the performance of a function that the appellant is required to carry out by law. I'm perfectly satisfied that it is a useful function to carry out in the support of the proper administration of justice in Ireland and that is one to be welcomed and I am of the view that the obligation is to make the judgement available but the method is discretionary. To make too colloquial an analogy, the court service used to provide or facilitate restaurant facilities in the Four Courts for the benefits of members of the public attending at litigants and witnesses. This was nothing like as important a service as the maintenance of database but it was within the capacity of the court service to provide this facility and it was permissible. However, there was no legal obligation to do this and the Court Service was not breaching a law when it ceased to arrange for the restaurant facility. As I say, the database so is a far more important service, and it more readily falls into the category of administration of justice and it is also one that dovetails with the obligation to keep records of authorised judgements but the maintenance of a data basis of judgements that do not purport to be authorised is not something expressly required by law. I am making a distinction here between the formal holding of authorised records on a court file, however constituted and the holding of convenient reference documents that do not purport to be authorised. I am also rejecting the argument made on behalf of the Appellant, if not at hearing, certainly in the e-mail to the Respondent of the 16th of November, 2017 that the Appellant is required to provide this service as part of its statutory duty under s.5 of the Court Services Act, 1998 as part of the function of offering support to the judiciary. The website is undoubtedly a most valuable support to the Judiciary but it is a website made available to the world and goes far outside any obligatory scope of a duty under s.5. This issue is discussed later in the judgement. There is further issue, which will arise again in this judgement, that I can't see that the appellant was required by law to disclose the identity of someone in breach of a High Court order which is the unauthorised disclosure that the Respondent decided occurred in this case.

20. The contention for an exemption from the application of the act is based on Section 8(e) which provides:

S.8 Any restrictions in this Act on the processing of personal date do not apply if the processing is-

...

(e.) required by or under any enactment or by a rule of law or order of a court,

21. Exactly the same reasoning applies from as to the consideration of s.1(4)b, the uploading of judgements to a convenient reference database is not been shown to be required by any enactment or rule of law. Even if the agreed instructions a Judge to upload on the existing website was deemed

to be a court order, and it doesn't seem that it could be, this instruction would have been countermanded by the more formal court order made in Court in this case that the identity of the notice party should not be disclosed. The Appellant was certainly not required by enactment or rule of law to contravene a High Court order.

22. If it transpired that I was incorrect about either of these contentions, I will indicate that I was persuaded by the argument made on behalf of the Respondent that both of the statutory provisions should be dis-applied as they effect a derogation from the operation of the European directives, particularly Directive 95/46 and this derogation is not authorised by those directives. It isn't in the normal run for the function of a circuit Court judge to dis-apply a statutory provision but the European jurisprudence does appear to be the effect that in the maintenance of the European regime of law places a field marshal's baton in in his knapsack of almost any public official. There is an obligation on public officials implementing European law to take such steps are necessary to give effect to the European law, which can include acting to dis-apply provisions of domestic law which are not consistent with directly applicable European law. I don't have to do make that decision in light of my view that neither of the provisions apply on the facts of this case, but I am of the view that it would be appropriate to dis-apply the provisions if that was necessary.

23. This bring me to the factual circumstances that gave rise to the decision by the Respondent that the Appellant was in breach of data protection legislation. The notice party in this case, was also the notice party in another case. This was also a data protection case and the proceedings were in the High Court. I don't need to go into the details of these but the nature of the case was that it concerned matters relating an investigation of complaints of sexual abuse and the proceeding would in the absence of Court order be fully public proceedings. The High Court judge made an order on the 30th of January, 2014, that nothing that would identify the notice party should be published.

24. On 9 May, 2014, the same High Court judge delivered judgement in that High Court Data Protection case and the judgement as delivered contained the name of the notice party and the notice party's name was mentioned at various points in the judgement.

25. On 12 May 2014 the Appellant disseminated on its website the judgement with the name of the notice party contained in the title and within the judgement. This judgement was also disseminated to various libraries which maintain databases of judgements.

26. On 13 May 2014, a solicitor involved in the High Court proceedings notified the Appellant that this dissemination on the website was in breach of the High Court order granting anonymity and the appellant immediately caused the judgement to be removed from the register on the 14th of May, 2014 and on the 15th of May, 2014 requested the various libraries delete the judgement. These steps did not prevent an account of the decision including the name of the notice party appearing in at least one instance in the print media.

27. The notice party was aggrieved by this and make complaints to the Appellant, to the ombudsman and to the Respondent. The complaint to the Respondent was made on 4 July, 2014 and was communicated to the Appellant. The initial view expressed by the respondent did not indicate that there was a breach of data protection law and the Respondent notified the notice party of this in 2014. The notice party however revitalised his complaint in a communication of 25 June 2016 and the Respondent re-opened the investigation and various exchanges of communications followed. Complaint is made by the Appellant as concerns these communications and I will revert to this matter later.

28. On 13 June, 2018, the Respondent delivered a written decision which concluded that the appellant was a data controller for the purposes of the data protection Acts and that the Appellant breached section 2(1)(d), Section 2A and section 2B(1) of of the Data Protection Acts 1988 and 2003. I am attaching this decision in full at the end of this judgement.

29. The investigation conducted by the respondent established that despite the existence of an order of 30 January, 2014 directing that should be no publication of the notice party's name that the High Court judge, who made that order, after pronouncing judgement on 9 May 2014, sent an unredacted copy of the judgement to the Appellant for the purpose of being published electronically. The judgement as published was the judgement as sent to the appellant by the High Court judge. On 13 May, the Appellant became aware of this publication which contained the name of the notice party when it should not have and on 14 May removed the judgement and on 15 May sent a letter to the various libraries asking that the judgement sent to them be deleted. The High Court judge then furnished a second iteration of the judgement and this removed the name of the notice party from the title but not from throughout the judgement. I'm satisfied from the facts that were property the subject matter on the Respondent could make a decision that this second iteration must be treated as never been published on the website. This is despite the fact that the notice party does not agree that this is so. The problem with the second iteration was noted by the officers of the Appellant and was not published but was sent back, this led to a third iteration of the judgement and this was fully redacted but it contained formatting errors as concerns the paragraph numbers. The correction of these errors was complicated by the retirement of High Court judge and ultimately, these errors were only corrected under the aegis of the then President of the High Court and the judgement wasn't published on the website in a fully redacted form without these formatting errors until November 2014.. These paragraph numbering errors were retained on the official copy of the judgement retained on the court file.

30. This investigation led to the decision of the respondent dated the 13th of June 2018. This was a nine page decision which set out, the background to the complaint and the timescale of the investigation of the complaint with details of issues that arose and which included discrete assertions of fact as found by the respondent and then involved analysis and findings in relation to the complaint. The first finding in this regard was a finding that the appellant was a data controller. The appellant had contested this and the notice party had argued for this conclusion. The respondent was heavily influenced by the Wirtshaftsakademie Schleswig Holstein Case C-210/16 decision of the court of justice which was delivered in June 2018. The reasoning in this case and an excerpt were included in the decision. The respondent went on to consider the provisions of Section 2, Section 2A and Section 2B and concluded that there was a breach of s.2(1)(d) in failing to have in place appropriate security measures to prevent unauthorised disclosure and breaches of section 2A the disclosures of personal data and section 2B the disclosure of sensitive personal data. The conclusion of the judgement indicated that the opportunity for an amicable resolution did not arise because of the fundamental issue of whether or not the appellant was a data controller. The decision concluded by notifying of the right of the right of appeal to the circuit court and notifying of potential liability under section 7 of the act.

31. The most relevant sections of the data protection Acts 1988 and 2003, at the relevant time stated, inter alia as follows:

Section 2:

[1] a data controller, as respects personal data kept by him or her, comply with the following provisions:

(a) the data or, as the case may be, the information constituting the data shall have been obtained, and the data shall be processed, fairly,

(b) the data shall be accurate and complete and where necessary kept up to date,

(c) the data-

(i) shall have been obtained only for one or more specified, explicit and legitimate purposes,

(ii) shall not be further processed in a manner incompatible with that purpose or those purposes

(iii) shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they were collected or are further processed, and

(iv) shall not be kept for longer than is necessary for the purpose or those purposes.

(d) appropriate security measures shall be taken against unauthorised access to, or an act unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

[2] – [8]

Section 2A

[1] personal data shall not be processed by a data controller unless section 2 of this act (as amended by the act of 2003) is complied with by the data controller and at least one of the following conditions is met:

(a) the data subject has given his or her consent to the processing or, if the data subject, by reason of his or her physical or mental incapacity or age, is or is likely to be unable to appreciate the nature and effect of such consent, it is given by a parent or guardian or a grandparent, uncle, and, brother or sister of the data subject and the giving of such consent is not prohibited by law,

(b) the processing is necessary-

(i) for the performance of a contract to which the data subject is a party,

(ii) in order to take steps at the request of the data subject prior to entering into a contract,

(iii) for compliance with the legal obligation to which the data controller is subject other than an obligation imposed by contract, or

(iv) to prevent –

(i) injury or other damage to the health of the data subject, or,
(ii) serious loss of or damage to property of the data subject,

or otherwise to protect his or her vital interests where the seeking of the consent of the data subject or another person referred to in paragraph (a) of this subsection is likely to result in those interests being damaged,

(c) the processing is necessary-

(i) for the administration of justice,

(ii) for the performance of the function conferred on a person by or under an enactment,

(iii) for the performance of the function of the government or a minister of the government, or
(iv) for the performance of any other function of a public nature performed in the public interest by a person.

(d) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.

[2] the Minister may, after consultation with the commissioner, by regulations specify particular circumstances in which section (1)(d) of this section is, or is not to be taken are satisfied.

Section 2B:

[1] sensitive personal data shall not be processed by that controller unless:

(a) sections 2 and 2A (as amended and inserted, respectively, by the act of 2003) are complied with, and

(b) in addition, at least one of the following conditions is met: ...

32. Conditions (i) to (xiii) are then listed. Condition vi (I) is if the processing is for the administration of justice, condition (vii) deals with processing necessary for the purpose of obtaining legal advice or otherwise necessary for the purposes of establishing exercising and defending legal rights. The authorising condition of "for the performance of any other function of a public nature performed in the public interest by a person" as exists in s.2A does not contained in s.2B. Perhaps raising an issue as to how a data base of judgements containing sensitive personal data could be processed by any person unless it is encompassed in the administration of justice, which might raise a problem for private subscription data bases unless this has been resolved by regulation. This doesn't arise for consideration in this case.

33. The stance of the appellant is that these provisions are not relevant to the appellant in the context where it's obligations are being considered as arising from the fact it is a data controller, because it is at all times been the contention of the appellant that it is not a data controller. This was the most heavily contested issue in the course of the investigation and in this Appeal.

34. At paragraph 19 in the decision of 13 June 2018, the respondent stated: –

> *"As acknowledged by the court service, the content of the official record of legal findings of a Court judgment are created by the judge alone and these may be recorded as a written judgment with the assistance of the Court Officer. However, the judgments that appear on the Court Service website are unofficial copies where the Court Service has published a disclaimer noting that the authorised version is retained in the court records. In the instant case, it was admitted that the draft judgement was dictated by the judge and typed up by a secretary who is an employee of the Courts Service. In addition to the legal analysis of the facts, precedent and findings of law, a published judgment contains content which is created solely by the Courts Service, such as the neutral citation. Accordingly I have determined that in relation to the un-redacted judgment which was published, both [the judge] and the Courts Service were data controllers within the meaning of the Acts."*

35. The core contention as I understand it of the Appellant is that it has no control over the contents of a court judgement and no control once a direction is given by a judge to publish a judgement, as to whether it should be published or not. One of the reasons for this being that the act of publishing a judgement is part of the administration of justice and therefore a judicial act and that this is so even if the judgement does not purport to be authorised. In this context the Appellant relies upon s.65 of

Courts Act 1926 act and those provisions in its own establishing act in particular s.9 which precludes it from trespassing upon any of the functions of a judge. The appellant relies heavily upon the particular constitutional status of members of the superior courts whose role is specifically recognised within the constitution. The appellant concedes that it may make requests of the judiciary to exercise judicial power in a particular way but indicates that as far as the content of judgements on the website operated by the appellant, it has no actual control of those and must follow a direction to publish the document on the website. This is on the basis that subsection 2 of section 65 of the 1926 Act provides:-

"Where an officer attached to any court is engaged on duties relating to the business of that court which is the time being required by law to be transacted by before under or pursuant to an order of a judge or judges of that court he shall observe and obey all directions given to him by such judge or judges."

I will point out that applies to an officer attached to a Court and dealing with business being transacted before the Court and the argument would be at its strongest if the registrar who perfected the order was the person who uploaded the judgement onto the website. I have no particular evidence of this one way or the other.

36. In challenging, the indicia relied upon by the respondent in holding that it was a data controller, the appellant relies upon the conceded error in the decision which indicated that reformatting of the relevant judgement prior to its second and final uploading was done by the data protection officer of the appellant. The respondent concedes that this was an error and it is accepted that this reformatting which had to be done after retirement of the judge was done under the aegis of the then President of the High Court. The appellant contends that the fact that the judgement was typed by an employee of the appellant having been dictated by the judge is not a relevant factor when this employee in no way participated or had any influence over the contents of the judgement which were solely the responsibility of the judge. Equally it is submitted that the act of putting a neutral citation onto a judgement or some non-substantive formatting does not indicate any control over the contents of the judgement. The appellant accordingly says that decision is flawed by reason of reliance on these immaterial indicia. The appellant further makes the case that the decision is flawed because the finding is that the appellant is a joint data controller with the judge when it was not the intent of statute that the 1988 and 2003 Acts, that is, the data protection regime would apply to judges. One of the grounds for asserting this, was that it would not be appropriate for Circuit Court judge in a data appeal to make a determination as to the legal validity of actions taken by a High Court Judge in his capacity as a High Court judge.

37. In making this argument, the underlying contention is that the Appellant was not exercising one of its own functions but was taking steps with regard to a function directly connected with the administration of justice which could only be a matter for the judiciary. The Appellant relied relied upon the commentary in the decisions of Baker J. in Stubbs Gazette and O'Donnell J in DPP v Nash:-

38. At paragraph 59 of BPSG Limited v. Courts Service and ors [2017] 2 IR 343, (the Stubbs Gazette case), Baker J stated:-

> *"It is, in my view beyond doubt that the pronouncement of a judgement by a judge in every court in the state, whether that be a judgement delivered orally or in a written judgement, is to be considered to be part of the administration of justice and must be done in a way that is officially open and sufficiently public that the identity of litigants and the result of litigation is known, and capable of being known, by all members of the public."*

39. In DPP v Nash, O'Donnell J stated:-

> *"Often judgements are delivered marked "unapproved" and in the process of the approval of a judgement for promulgation on the website of the courts service, and perhaps reporting in official or unofficial reports, such areas including typographical and grammatical errors, can be addressed. It is not desirable to announce a decision judgement without circulating the judgement on that day making it available. The delivery of judgement is part of the administration of justice in public normally comprehends making the text of a judgement publicly available."*

40. The Appellant contends that these obligations mean that publishing of a judgement is an act required to be preformed by a Judge as part of the administration of justice, so that the Appellant must publish the judgement on its website in whatever form it is delivered to the Appellant by the Judge.

41. The Appellant has also argued that the reason the respondent fell into error was that the respondent initially was of the view that public hearings of the courts would not be subject to data protection, and then moving from this view adopted a new view that if there was a breach of a High Court order restricting disclosure that this caused a triggering of the application of the 1988 and 2003 Acts. I can see how this argument is open to the appellant because of the initial letter of the Respondent to the complainant prior to the revitalisation of the complaint and prior to the issues receiving more considered attention from the respondent but nonetheless I think the argument is fundamentally wrong. I believe the correct analysis of the operation of the application of the data protection Acts to public hearings of the courts, is that if a person, without any special constitutional legal status, disseminates information from court proceedings, that will clearly contain personal and often sensitive personal data, that the public nature of the hearing will suffice to meet the conditions of section 2A or section 2B as would allow for processing of this personal or sensitive personal data but that the 1988 and 2003 acts still apply. They apply regardless, of a breach, that is, it isn't the fact of the breach that makes them apply. I never took the stance of the Respondents in this case to be that the Data Protection Acts don't apply to Court pronouncements that don't require redaction but do apply to Court pronouncements that do require redaction. I think this was a straw man set up by the Appellant, with the benefit of a small amount straw growing out of that initial response by the Respondent to the Notice Party, but it was still a straw man. It is patently not the case that the acts only apply when there is a breach. I don't believe that in its general approach that the the respondent did conflate the breach of the court order with a breach of the data protection act, although there is specific issue on which this point does have traction and so does throw up some more straw, and I will deal with that later. However, the basic underlying contention of the Appellant as to this asserted flaw is not well founded. The fact that the dissemination of the name was in breach of a Court order was, of course significant within the Data Protection regime but it was significant not in making the Data Protection Acts apply, it was rather that the fact the disclosure was not in compliance with law had the effect of making it impossible for a person who was processing personal or personal sensitive data to rely on some of the qualifying conditions in Section 2A and Section 2B that would provide the basis in law for processing the personal data in the judgement.

42. The Respondent and the notice party both contend that the processing in question is not the inclusion of the appellant's name in the judgement, it is the dissemination of the judgement on the website and to libraries and contend that this is the website operated by the appellant and a servant or agent removed the judgement from the website on the 14th day of May, 2014 without reference to

the judge who had by the description of the agreed protocols directed that the judgement be uploaded. It was averred to on behalf of the appellant that this was an interim measure taken because of the unavailability of the judge, but if there was a binding direction pursuant to section 65 of 1926 act, the readiness of the servant or agents of the Appellant to remove it without judicial approval does call for explanation. Equally, the Respondent and notice party say despite the assertion of the binding nature of the instruction to upload the judgement to the website, when as servants or agents of the appellant were not satisfied with the second or third reiterations presented by the judge, they did not upload the judgement to the website until the Appellant was satisfied that it was appropriate to do so. It also appears, that servants or agents of the appellant were prepared to indicate to members of the Superior Court judiciary that judgements would only be uploaded if the appellant's requirement that the judgement be marked either that redaction not necessary or the necessary redaction was already done. The notice party argued that if the Appellant was not a data controller the notice party as a person who has his personal data wrongly disseminated would be left without remedy. I will note this presupposes that there was no remedy against the judge as data controller and that this might not necessarily be the case. It is true though that no claim has been made against the judge, as data controller or otherwise, but one view of the stance of the Appellant is that the notice party and Respondent were targeted on the wrong entity. If this case was made, it was done so without any contention that a judge was a data controller and in fact making an assertion to the contrary

43. My task in this appeal is to decide if I can see an error or errors in the decision of the respondent in holding that the appellant was a data controller and whether this error is sufficiently significant to vitiate the finding. I am of the view that the core finding is that the appellant was a data controller and if there are errors, such as the errors, the true issue is whether these mean that the finding that the appellant was a data controller is incorrect. This is in accord with paragraph 29 of the Judgement of O'Donnell J. in Peter Nowak v. The data protection Commissioner [2016] 2 I.R. 585 at paragraph 30: –

> *"In my view, in addition to considering the terms of the statute, it is useful to ask why the Oireachtas might have created a right of appeal to the court rather than a further expert appellate body, as occurs, for example when planning appeals are brought to An Bord Planala, or indeed as occurred in the telecommunications field when, briefly, an expert appeal panel was established. First, it may, no doubt be that the Oireachtas wished by designating the court as the appropriate body to provide a guarantee of independence. It is, of course, possible to establish a body which is, by statute independent, but providing for appeal to the court, the legislation invokes, and to some extent, benefits from the constitutional guarantee of independence in decision-making. Thus, provision for appeal to a court can be seen as an assurance that extraneous considerations, whether national or local, or industry requirements or expectations or perhaps, public controversy, will not affect the decision. In so much as any appeal raises a point of law, then it is natural to expect that a court would determine such issues. Furthermore however courts while perhaps having no expertise in the underlying area, to have considerable experience both in decision-making and in review of decision-making and reasoning processes. On the other hand, even the greatest admirer of courts might think it unlikely that individual courts could, in the course of a single case, develop the type of technical expertise acquired by, and available to, specialist bodies in a complex area, and in any event, might reasonably doubt that adversarial litigation is the most effective cost efficient way of educating a judge on technical issues to the point where he, or she could with confidence, substitute his or her decision in a technical issue for that of the original decision-maker. This function analysis perhaps supports the test identified in Orange Ltd. v. Director of telecoms (No.2) [2000] 4 I.R. 159: a court can be expected to detect errors in law, and they identify*

serious errors in reasoning or approach. It can be said that if an error is sufficiently clear and serious to be detectable by a non-expert court after scrutiny, and that is the justification for overturning the decision, even though the court may lack more specific expertise. In my view, the standard in Orange Ltd. v. Director of telecoms (No.2) is the appropriate standard to apply here...."

44. The test set by Keane J in the Orange Ltd has been described as being that the appellant bears the onus of establishing as a matter of probability, that taking the process as a whole, the decision reached was preceded by a serious and significant error or series of such errors, but did contain the caution that there should be curial deference to the degree of expertise and specialist knowledge of the original expert decision-maker. The point did arise at hearing that in the statement of this rule by O'Donnell J in Nowak at paragraph 29 it was summarised as *"a decision will be set aside on appeal if it is wrong in law or if it is vitiated by a serious error or series of errors."* That is the word *such* in the phrase *"series of such errors"* was dropped which makes the test read more logically. In the process of process of following precedent, it is an established that judicial findings are to followed on the basis of the principles they establish, not on the basis of construing the precise words of the Judge as if they were a statutory provision (as an example DPP v. Shane Canavan, [High Court, 1st August, 2007, Birmingham J. *However, judgments are not to be parsed and analysed as if they were sections in a Finance Act.*). Insofar as it arises, I am satisfied that he proper test to apply is that if there are a series of errors, it is cumulative effect of them that must be serious and significant.

45. On this point, there are two admitted errors in the decision of 13 June 2018. On the second page of the ruling it is stated that the court order which directed that there should be no publication of the name was made on the 9 May 2014. In fact the order for nondisclosure was made on 30 January 2014 and was restated at the end of May. I don't think any party is contending that this is an error of any significance. There is also a second admitted error in that at paragraph 17 there is a statement that the data protection officer of the court service was the person who corrected a paragraph numbering error, after the retirement of the Judge, did so effectively on her authority, whereas in fact when this was done by a different servant of the appellant and was done under the aegis of the then president of the High Court. The appellant relies on this as it might have been relied upon as an indicia relevant to the decision as to whether the Appellant was a data controller, even though it was not specifically mentioned in paragraph 19 which the Appellant described as a curial portion of the decision.

46. The consideration then for the Court is whether the finding that the Appellant is a data controller is wrong in law or vitiated by an error or errors that are significant and serious.

47. The statutory definition for a data controller in the acts is ***"a person who, either alone or with others, controls the contents and use of personal data"***.

48. The definition from directive 95/46 defines data controller as meaning: –

"The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes means of the processing of personal data; where the purposes and means of processing are determined by national or community law or regulations, the controller or by the specific criteria for his nomination may be designated a national or community law."

49. In the second edition of privacy and data protection law in Ireland, Kelleher states *"the key issue in deciding who is or is not a controller is whether a person has the power to determine whether and how data is processed."* As referred to by the Respondent in the 13th of July, 2018 decision, Keane J.

identified in the case of Mount Carmel Medical Group (South Dublin) Limited (in liquidation), [2015] 1 I.R. 671 held that the issue was a question of fact conditioned by the legal definition.

50. In making the decision, as to whether the appellant was a data controller the respondent was influenced by the Court of Justice Wirtshaftsakademie Schleswig Holstein decision (case C – 210/16) which had been delivered the previous month. The Respondent correctly noted that complete control over all aspect of the process was not necessary. The passage quoted by the Respondent included the sentences "*ever more frequently, data processing is complex comprising several distinct processes, which involve numerous parties which themselves have differing degrees of control. Consequently, any interpretation which focuses on the existence of complete control over all aspects of data processing, is likely to result in serious lacunae in the protection of personal data.*" I am satisfied by the argument the case and by my consideration of the decisions referred to an argument of the Court of Justice which followed Wirtshaftsakademie Schleswig Holstein, these were Jehovan todistajat (C-25/17) and Fashion ID (C-40/17) that Wirtshaftsakademie Schleswig Holstein correctly stated the law and that the one effect of these decisions is that personal rights should be protected by affording wide scope to the definition of data controller and that data controller need not as a necessary condition of being a data controller have control over the content of the personal data whereby it has the capacity or the authority to alter the contents. Not only is it is not a requirement that a data controller have sole control, it is the case that a very limited degree of control, perhaps even just the capacity to cease involvement in the facilitation of the processing, can suffice, provided the data controller is acting for its own purposes and not solely as an agent of another.

51. The circumstance of the Wirtshaftsakademie case are of significance. It is not that the facts are all on all fours with the present case for the facts are to the reverse. The process being considered was, not the dissemination out of personal data, but rather the collection in personal data, so that in some ways it was a mirror-image of the present case. Wirtshaftakademie administered a Facebook fan page, and used this fan page to advertise its activities and were encouraging users to click on to and use the fan page. When a user did this, this allowed Facebook to extract personal data, not only from the person who joined the Fanpage but from other parties, but in any event, personal data was gathered by Facebook who then did give anonymized statistical information about users back to Wirtshaftsakademie, who didn't have control or knowledge of any individual's personal details yet the Court of Justice, held the fact of administering the fan page made Wirtsshaftsakademie a data controller and not notifying users of the use of their personal data was a breach. The finding might be regarded as borderline, the domestic courts in Germany at the appellate level did not hold Wirtshaftakademie to be a data controller, but this was the finding of the court of justice and that approach has been approved subsequently. This case would argue strongly to me, that if one set up and operated a website for one's own purposes, with the intent that the personal data of others would place on the website by a third party, that this could be the act of a data controller.

52. To quote some of the discussion concerning a data controller in Wirtshaftsakademie Schleswig Holstein, Jehovan and ID Fashion decision of the Court of Justice.

53. From Wirtshaftsakademie Schleswig Holstein:-

> 36: in this context, according to the submissions made to the court, the creation of the fan page on Facebook involves the definition of parameters by the administrator, depending inter alia on the target audience and the objectives of managing and promoting its activities, which had an influence on the processing of personal data for the purpose of producing statistics based on the visits to the fan page. The administrator may, with the help of filters made available by Facebook, defined the criteria in accordance with which the statistics are to be drawn up and even designate the categories of persons whose personal data is made use of

by Facebook. Consequently, the administrator of the fan page hosted on Facebook contributes to the processing of the personal data of visitors to its page.

37: in particular, the administrator of a fan page can ask for – and thereby request processing of – demographic data relating to the target audience, including trends in terms of age, sex, relationship occupation, information on the lifestyles and centres of interest are the target audience and information on the purchases and online purchasing habits of visitors to its page, the calories categories of goods and services that appeal the most, and a geographical data which tell the fan page administrator were to make special offers were to organise events, and more generally enable it to target best information it offers.

38. While the audience statistics compiled by Facebook are indeed transmitted to the fan page administrator only in anonymized form, it remains the case of the production of the statistics is based on the prior collection, by means of cookies installed by Facebook, on the computers or other devices of visitors to that page, the processing of the personal data of those visitors for statistical purposes. In any event, directive 95/46 does not, were several operators are jointly responsible for the same processing, require each of them to have access to personal data concerned.

39. In these circumstances, the administrator of a fan page hosted on Facebook, such as Wirtshaftsakademie Schleswig Holstein must, must be regarded as taking part, by the definition of parameters depending in particular on its target audience and the objectives of managing and promoting its activities, in the determination of the purposes and means of processing personal data of the visitors to its fan base. The administrator must therefore be characterised in the present case, as a controller responsible for the processing within the European Union, jointly with Facebook Ireland, within the meaning of article 2(d) of directive 95/46

40. The fact that administrator of the fan page uses the platform provided by Facebook in order to benefit from the associated services not exempted from compliance with its obligations concerning the protection of personal data.

41. It must be emphasised, moreover, the fan pages hosted on Facebook can also be visited by persons who are not Facebook users and so do not have a user account on a social network. In that case the fan page administrative responsibility for the processing of the personal data of those persons appears to be even greater, as mere consultation of the homepage by visitors automatically starts the processing of their personal data.

42. In those circumstances, the recognition of joint responsibility of the operator of the social network and the administrative fan page hosted on that network in relation to the processing of the personal data of visitors to that page contributes to ensuring more complete protection of the rights of persons visiting a fan page, in accordance with the requirements of directive 95/46.

54. This case was as containing the general indication that the intent of the Directives in affording protection should be given effect and also indicating that control over the contents is not necessary, does indicate that control of the website for one's own purposes which deals with the personal data of members of the public can be sufficient to render an entity, a data controller.

55. In Jehovan, which concern the collection of information by Jehovah Witnesses arising from door to door collection, which was extremely limited, being only in indication of houses where calls were not welcome resulted in a breach of data protection laws.

65. As expressly provided for in article 2(d) of directive 95/46, the concept of "controller" refers to the natural or legal person who "alone or jointly with others determines the purposes and means of the processing of personal data". Therefore the concept is not necessarily referred to a single natural or legal person and may concerned several actors taking part in a processing, with each of them then been subject to the applicable data protection provisions

(see to that effect, judgement of 5 June 2018, Wirtshaftsakademie Schleswig Holstein, C-210/16, EU:C:2018:388, paragraph 29).

66. The object of that provision being to ensure, through a broad definition of the concept of "controller", effective and complete protection of the persons concerned, the existence of joint responsibility does not necessarily imply equal responsibility of the various operators engaged the processing of personal data. On the contrary, those operators may be involved at different stages that processing personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the case..."

67. In that connection, knew the wording of Article 2(d) of directive 95/46 nor any other provisions of that directive supports a finding that the determination of the purpose and means a processing must be carried out by the use of guidelines or instructions from the controller.

68. However, natural or legal person who exert influence over the processing of personal data for his own purposes and who participates, as a result, in the determination of the purposes and means that processing, may be regarded as controller within the meaning of article 2(d) of directive 95/46. [my bolding facing].

56. Fashion ID GmbH & Co. KG C-40/17 concerned the use of like buttons and I won't go into the facts any more than that, on principle the case stated:

73: when looking at the applicable test to identify a "joint controller" with a critical eye, it seems to me that the crucial criterion after Wirtshaftsakademie Schleswig Holstein and Jehovan todistajat is that the person in question "made it possible" for personal data to be collected and transferred, potentially coupled with some import that such a joint controller has as to the parameters (or at least the wearer's silent endorsement of them) if that is indeed the case, and in spite of the clearly stated intention to this effect to exclude it in Wirtshaftsakademie Schleswig Holstein it is difficult to see how normal users of an online (based) application, be it a social network or any other collaborative platform, but also other programs, would also become joint controllers. Usual typically set up as account, providing parameters to administrators to house account is to be structured, what information he wishes to receive, on what subjects and from whom. He will also invite his friends, colleagues and others to share information in the form of (often quite sensitive) personal data, via the application, the following providing data concerning these persons, both providing those persons become involved themselves in this way. Contributing to the obtaining and processing of personal data of those persons.

74. Furthermore, what about the other parties in a "personal data change"? When pushed to the extreme, if the only relevant criterion for joint control is to me that data processing possible, thus in effect contributing to the processing any stage with the Internet service provider, which makes the data processing possible because it provides access Internet, or even electricity provider, they not also be the joint controllers potentially jointly liable for the processing of personal data?

75: The intuitive answer is of course "no". The problem is the delineation of responsibility so far does not follow from the broad definition of the controller. The danger that definition becoming too broad is that it results in a number of persons being oh co-responsible for the processing of personal data

57. Having posed this question, which indicated caution as to applying the Wirtshaftsakademie Schleswig Holstein approach too extensively, later referring to Wirtshaftsakademie Schleswig Holstein, the judgement continued:-

97. I think however that the key statement of the court is the second one, namely that "operators may be involved at different stages of that processing of personal data and different degrees" the suggestion finds support in the definitions contained in directive 95/46, in particular with regard to the definition of (i) the notion of processing in article 2(b) and (ii) the notion of controller in article 2(d).

98. First, the notion of personal data processing contains "any operation set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment combination, blocking, erasure or destruction"

99. Even if the notion of processing is, similar to the notion of controller, rather broad, it clearly underlines and aims at a stage in the processing: it refers to an operation or a set of operations, with an illustrative list of what such individual operations might be. But then logically, the issue of control should should rather be assessed with regard to the discrete operation question, not with regard to the undetermined bundle of everything and anything called processing."

100. Second, the notion of joint control is not specifically defined by 95/46. But logically, that notion builds on the notion of controller in article 2(d): the situation of joint control appears when two or more persons determine the means and the purposes of processing of personal data together. In other words, for two (or more) persons to qualify as joint controllers, there must be an identity of the purposes and means the personal data processing between them.

101: is the combination of these two definitions that ought, from my point of view, to determine the obligations and potential liability of joint controllers. A (joint) controller is responsible for that operation or sets of operations for which it shares or co-determines the purposes and means as far as a given processing operation is concerned. By contrast, that person cannot be held liable for under the preceding stages or subsequent stages of the overall chain of processing, for which it was not in a position to determine either the purpose or means of that stage of processing.

58. This commentary is focused on the idea of joint controller, and its application may be less clear if the Judge in this case was held in law not be a joint controller, but even in those circumstances, the concept that a person can be a controller at some stage in a process but not at a preceding stage is of assistance in analysing the facts of the present case. It is seems to be compatible with the law for the Appellant not to be a controller as concerns the creation and delivery in Court of the judgement but to be controller when the processing in question becomes the dissemination of the judgement, or a version of it that does not purport to the authorised to the public. In light of this commentary and in particular in light of the approval of the approach in the Wirtshaftsakademie Schleswig Holstein case, I'm of the view that the reliance by the respondent on this authority was appropriate and not an error in law.

59. This case also supports the view that in interpreting the Irish statutory definition of data controller that where there is more than one person who has control, it is not necessary that each of these persons have control of both contents and use, but one person could have control of content and another control of use, and indeed the levels of the control can encompass what might be described as influence or to the negative control that comes from declining to participate.

60. However, more decisive than any considerations arising from the implications of Wirtshaftsakademie Schleswig Holstein, I find it very difficult to come to any view but that the appellant was obviously a data controller. The appellant set up a website and at some point made a decision to establish a database of convenient reference judgements which wasn't being set up for the purpose of having an official record of judgements and therefore arguably for the sole or direct purposes of the administration of justice, but rather was being set up as a convenient reference for

the public which would be less directly for the purpose of the administration of justice than arises in the case of maintenance of formal records. It also seems to an act that could comply with its own statutory functions.

61. Section 5 of the Courts Service Act, 1988 states:-

The functions of the Service shall be to:-

(a) Manage the Courts
(b) Provide support services for the judges
(c) Provide information on the courts system to the public,
(d) Provide, manage and maintain court buildings, and
(e) Provide facilities for users of the courts.

62. I am firmly of the view that establishing this data base accessible to the world on its website that the Appellant was acting at least in part pursuant to its functions under heading (a) and (e) and perhaps under heading (c) and not solely under heading (b) as asserted on behalf of the Appellant. As a matter of fact, the data base actually is a significant support to the judges. If was set up as part of the Judge's Library and was accessable only to Judges and support staff, its sole statutory authorisation could be found in heading (b) but the data reference data base serves a wider purpose. As concerns whether this is part of the administration of justice or not, the true question is whether it is part of a judicial function or not. There is a general public entitlement to hear a judgement being delivered and there should be a public entitlement to view an official written judgement held on a court file. I may have some doubts that in practice that the Appellant always facilitates this but that isn't the issue before me. On the basis of the commentary of Baker J in Stubbs and O'Donnell J in Nash, I must accept that publication on the website falls into the category of the administration of justice but I don't believe that the commentary in those cases goes so far as to say that it is part of a Judge's function to oversee and direct the manner in which the decision is made available to the public by the Appellant. That dissemination is the Appellant's function. As indicated before, the provision of this website is a permitted and laudable activity but I see no basis for holding that this database was set up by reason of direction given to the Appellant by a judge, as opposed to being the decision of either an official of the Appellant or of the Board of the Appellant. The Board of the Appellant does of course have judges as members but it is not an entity empowered to give judicial directions and constitutionally could not be. I am prepared to accept, that a judge in furnishing a judgement to the appellant does this as a judicial act related to the case in which the judgement was pronounced and I'm prepared to accept that it is understood both by the judge and by the appellant that the furnishing of this judgement is a direction to the appellant to put the matter upon the website. I have some doubts whether it's actually an judicial act to make a judgement that only purport to be available as a convenient reference, but if, as an extrapolation from the words of O'Donnell J in Nash, this is the position, so that the direction to put the judgement on the website is a judicial direction, I can see no basis for saying the website itself is operated on foot of a judicial command from a specific judge as would cause section 65 of 1926 act to apply. In operating that website, the applicant is exercising control over the use of the personal data which is designed to receive and to disseminate and clearly in acting this way. The appellant is not just a processor or a servant but is operating the website to achieve its own goals including facilitating Courts users by disseminating personal data. I am satisfied that on the information before the Respondent that the Respondent would be entitled to hold that the Appellant was operating the data base on the website for at least in part, its own statutory functions, that it exercised control over this data base, including the power to delay and remove as an interim measure or otherwise and had to discretion to cease the operation of the data base and meet any obligations to make judgements publicly available in some other manner.

63. I can see no basis for saying that the Respondent was in error in identifying the appellant as a data controller. I don't see that any errors in approach or fact is have been asserted and identified in the decision undercuts the validity of the finding. I do not feel that even if the Respondent placed any reliance of the fact that it was the Data Protection Officer who acted to re-number the paragraph in the third iteration that this error would unseat fundamental decision that the Appellant was a data controller. This being so, I'm not concerned with whether the respondent was correct in identifying the judge as a joint data controller. The core of the finding is that the Appellant is a data controller, if it was an error to say that the judge was a data controller as well, and I am not saying that he was, to identify the Appellant as joint data controller rather than simply as a data controller working in conjunction with a party who might not be a data controller, I don't feel that this is a substantial error that vitiates the finding. The status of the Judge would only be relevant to my determination if I felt there was tenable case that the Judge was the sole data controller in respect of the dissemination of the personal data on the Appellant's website. Whatever argument might apply in respect of sole control by the Judge of the official record of the judgement held on the Court file - and even there, I don't believe it is the practice of the Appellant to revert back to the Judge who delivered the judgement every time the official record is sought to be accessed – I can no basis for saying that it is each individual Judge whose judgement who is on the data base who is the sole data controller of that judgement. Aside from anything else, this would mean there was no data controller as soon as the Judge retires or dies. More decisively again, even if putting up the convenience reference judgement was done as part of the function of a Judge and directly constitutes a role with the administration of justice, this is not the only reason for the judgement being uploaded, the purposes of the Appellant to facilitate court users is another purpose of the website and part of the Appelllant's statutory function. By this reasoning, even if the act is in part a judicial act, it is also in part an act of the Appellant for the purposes of the Appellant. The appellant can't escape the obligations for activities that would otherwise be governed by data protection by moving them under a cloak in pairing them with a judicial function. Since there is no basis on which I can see that the Judge is the sole data controller, it is not relevant for the question of whether or not the Appellant was in breach of its obligations as a data controller to decide if the Judge was also a data controller or not in respect of the dissemination of personal data on the Appellant's website.

64. This being so, I don't have to consider arguments based upon the regime that applies to judges as data controllers under the 2018 Act which is not in force, that is the GDPR Rules and the effect of s.160. I will though make the passing comment that I am not satisfied even under the GDPR that the assessment of obligations between individual Judges and the Appellant would be the same for the official records and convenient reference data bases. It might well the at the Judge would a data controller for the official records, with the Appellant as a data processor but that as concerns the "convenient reference" judgements data base the Appellant would be a data controller and the Judge might or might not be a joint data controller with the Appellant. These issues don't fall to be directly determined as consideration was only given to GDPR issues to consider the extent to which this might provide assistance in coming to a view on the decision before me, and my conclusion is that they don't have any true impact on the issues before me.

65. I'm satisfied the respondent was correct in identifying the appellant as a data controller this brings me to the issue of whether as a data controller, the appellant was in breach of s.2(1)(d), Section 2A and Section 2B(1) as found by the Respondent.

66. The first finding is that the Appellant was in breach of s.2(1)(d). In dealing with finding, it is necessary to outline the documents that were available to the respondent relating to this issue at the time the decision was made. These are the documents disclosed from the affidavits as exhibits in this

case. The respondent's investigation did seek an account as to these procedures and the various statements were made on behalf of the appellant that could relate to the appropriate procedures put in place to prevent a breach such as this occurring. The re-vitalising letter of complaint of the 25th of July 2016 enclosed a letter from the Apellant to the Notice Party, which isn't spefically identified but must be the letter of 21 October 2014 from the Appellant to the notice party solicitor. This letter was a response to a request that sought an explanation as to how the incident occurred and sought details of precautions now in place to ensure such incidents is not repeated. The answer to these queries, was primarily concerned with the issue of whether the Appellant had any control over the contents of the judgement or any discretion as to whether it could be processed. Notwithstanding, this, the response to give an indication of the procedures in place, stated: –

"As regards the approval and publication of a High Court judgement, the content is a matter solely for the judge who signs the judgment. The court service, when obviously highlighting any errors which are apparent, has no role in ensuring that a judge said regard to all the relevant matters in a written judgement. It is a requirement that a judge mark the judgment as not requiring any redaction prior to the court service processing same for publication on the website. This was done in this case so the court service had no option other than to proceed to process the judgment."

"The courts service has a number of protocols in place to protect the identity of parties in judgments in circumstances where this protection is apparent or required of [sic] statute. However, the content of a judgment is not a matter over which we have any direct or editorial control. In the circumstances where there is nothing apparent from a judgment that any identity be protected and when a judge indicates that a judgment requires no redaction is not possible for the court service to identify with any certainty situations such as that which pertained in the case of your client. Given how this issue arose I have brought the matter to the attention of the president of the High Court."

67. This letter of 21 October 2014 from which those quotes comes was specifically referred to in an email from the respondent to the appellant on 17 August 2016 and the appellant responded to this by letter of 9 September 2016 which again was primarily concerned with the issue of whether the appellant could be a data controller of the contents of a judgement but which also stated: –

"The court service uploads written judgements, as provided, to the court service website in accordance with procedures agreed with the judiciary."

"I would also like to bring to your attention that the Office of the Ombudsman carried out an investigation of this matter in 2014/2015 and having received reports on the matter decided to close the case."

"I attach for your information report which is provided to the Office of the Ombudsman on the matter which may be of assistance to you in carrying out your investigation."

68. The report for the office of the ombudsman presented to the Ombudsman by the Appellant was dated on 20 November 2014, contained the following statements: –

"... The judge provided the original judgement to the courts service which in line with procedures and practices agreed with the judiciary amounts to an instruction to the court service to process same which includes uploading to the court service website."

"In circumstances where there is nothing on the face of the judgment indicating that the identity of any person named therein is required to be protected and a judge does not indicate

that a judgment requires redaction is not possible for the court service to identify with any certainty circumstances such as that which pertained in this case."

"To this end, the Head of Supreme and High Court Operations has written to all judges regarding the importance of instructions in relation to redaction. In addition all staffinvolved in the processing of written judgements have been reminded of the need for vigilance in this regard so that they can, in so far as is possible, draw the judge's attention to any content that might need to be redacted before judgement is published."

69. It is noteworthy that this report describes the situation as being that the Judge did not indicates that redaction required, rather than stating that the Judge must indicate that no reaction is required and doesn't contain the statement as in the letter of the 21st of October, 2014 to the Notice Party that the Judge had done so. I could see how this would raise doubts in the mind of the Respondent as to exactly what procedures were in place.

70. In the course of communications that followed, the respondent on 26 October 2017 raise the query, inter alia:-

"In your letter, dated 09 September, 2016, you state that "the court service uploads written judgements, is provided to the court service website in accordance with procedures agreed with judiciary." Please now provide this office with a copy of these procedures."

71. The response of the appellant by email of 16 November 2017 was in the following terms: –

"Please find attached below a letter which sets out in writing the procedure agreed with judiciary in respect of uploading judgements in the court services website. You will note that this written instruction re-iterates the procedures which were already in place. I understand the letter issued to all members of the judiciary." (In passing I will say that I take as mean all members of the Superior Courts judiciary, although nothing seems to turn on that.)

72. The attached letter was a letter dated 19 November 2014 and was a letter from Supreme and High Court operations addressed to "Dear Judge." In its body it outlined the difficulty in the complaint to the ombudsman that had arisen in this present case without giving any indication of the identity of anyone involved. It contained the following statements: –

"For the avoidance of doubt Judges are asked to inform the office in writing that every judgement has been redacted or, if such is the case that no redaction is required, once this written statement is provided to the office, the judgement is published on the website "as sent"."

"I would ask that every judge would ensure that no information that should not be put into the public domain is included in any judgement sent for publication. I have also directed court office staff who publish judgements on the website that if a judge has either not sent a covering note about redaction and distribution or used the stamp provided, the judgement must be returned to him/her with a request for written instructions in that regard."

73. This exchange contains the express statement on behalf of the Appellant, in the covering comments accompanying the letter, that this letter set out the procedures already in place. This is so even though the last line quoted about directions to Court Staff reads more like a new direction being given than a reminder. The letter does refer to stamps provided, which carries at least the implication

that these stamps had already been provided to the Judges. There is no suggestions that the stamps were being provided with this letter.

74. As far as I have been able to identify this is the totality of the information concerning the measures put in place as might constitute an appropriate measures to prevent inadvertent disclosure. The statements on behalf of the Appellant to the Respondent were to the effect that there was a practice which pre-dated the inadvertent disclosure that a Judge in sending a judgement to the Appellant would be taken as giving an instruction to have the judgement published on the website unless there was a specific instruction to the contrary. This judgement however would not be published in accordance with this instruction, unless there was an indication that no reaction was necessary or else that the judgement has already been redacted. In the e-mail of the 16th of November, 2017, it was expressly stated by the letter of the 19th of November, 2014 re-stated existing practice. Admittedly, this was not apparent on the face of the letter, but support for the existence of the practice prior to this inadvertent disclosure is found in the statement in the statement in the letter of the 21st of October, 2014 that the Judge did, and this can only be in reference to the first iteration, mark the judgement as not requiring redaction. The letter stated *"It is a requirement that a judge mark the judgment as not requiring any redaction prior to the court service processing same for publication on the website. This was done in this case..."*. I do note the use of the word requirement which appears to be a requirement set by the Appellant, and perhaps only binding on the judiciary by agreement but still a requirement as to publication on the website put in place by the Appellant. I make this last comment in respect of the issue of control exercisable by the Appellant. As concerns the appropriate procedures, the procedure described is that the Judge, who must be presumed to be the person who best knows the circumstances of the judgement, warrants in writing prior to publication that there is no need for redaction. I do understand it to be the Appellant's case that this was motivated, not by considerations of data protection legislation but by the intent that copies of judgements should be disseminated in conformity with courts orders and legal requirement of anonymity rather than for the purpose of data protection legislation, but if the procedures were sufficient to meet the requirement of s.2(1)(d), they would nonetheless exist as appropriate measures.

75. I will make the comment that in light of the particular relationship as exist between the judiciary and the appellant, with the constitutional and legal considerations, which all the parties maintained during the course of the hearings they were conscious of, it would seem to me to be an eminently appropriate procedure, that rather than have a person unfamiliar with the case, who is not a judge, reviewing and passing judgement on the judgement of the judge, that any considerations of any issues of anonymity and any restrictions on reporting that unseat the constitutional requirement that justice be done in public, would be made most appropriately by the judge hearing the case. A procedure that relied upon the appropriate measures being taken by the Judge would mean that the appellant as data controller will, in effect, be assigning out its appropriate measure duties but I do not see this as objectionable in principle. Generally, if a data controller could best provide appropriate measures by involving a third party, it would not be objectionable to do so. Whatever about generally, when the third party is already involved in the process and particularly in light of the special and sensitive relationship that exists between the Appellant and the Judiciary, such an "assignment out" of this function would seem completely appropriate. The assignment out of this responsibility, doesn't alter the fact that the legal responsibility for any breach of the Data Protection Acts still rests with the appellant. If a judge who is carrying out this duty, fails and marks as not needing a redaction, when in fact the judgement does require redaction, which is what the Appellant has asserted occurred in this case, the appellant as data controller is simply in the position of the variety of data controllers who have had good procedures in place but have been let down by lapses of employees. The fact that the judge is not an employee doesn't alter that position. It is a well settled settled principle of law that

legal liability for the performance of duties, may rest with the party bearing them, despite the fact that the actual performance has been delegated to third party. The position of employees who are sent to work on third party premises is an example, where the employer's statutory obligations concerning safety at work, will mean that the employer still bears the obligation to ensure a safe place of work, even though the premises is controlled by a third party. That is an analogy and precise principles of the health and safety regime, may or may not be of any assistance to the present case, but as concerns the general principle that statutory duties may be performed for the party bearing that duty, by a third party rather than a direct employee, but that the main party remains responsible for the breach, there seems no reason why this could not apply here. I am expressing no view as to the question, generally on the present circumstances, whether the third party has any liability to the main party for a failure by the third party that put the main party in breach of its statutory duty, this issue being in no way before me.

76. I am taking it then that the system described by the Appellant is that a judgement will only be published on its "convenient reference" data base, if the Judge who delivered the judgement positively indicates that there is no requirement for any no restriction on the full disclosure to the public that is the general and constitutional rule governing the pronouncement of judgements in the Courts. I am inclined to the view that if it fell to be determined by me, I would be inclined to hold that this would be complicance by the Appellant with its obligation unders s.2(1)(d).

77. It does not fall to me to come to a view on this, for any frailty in such a procedure was not the basis of the finding of a breach of s.2(1)(d) because the Respondent never addressed this issue. The respondent did not assess the measures and find them inappropriate, instead the respondent found these appropriate measures did not exist at all at the time of the inadvertent disclosure.

78. The finding at paragraph 14 of the decision of 13 June 2018 was that:

> **14. On request for a copy of the procedures agreed with judiciary in respect of uploading written judgements on the court service website, this office was provided with a letter dated 19 November 2014 which it states was provided to all members of judiciary. This letter request the judges inform, in writing, that every judgement has been redacted or if no redaction is required. It is clear these "agreed procedures" were in place only after the matter relating to the publication of your name arose.**

79. This does prompt the question as to whether in the course of an investigation pursuant to s.10 complaint, the onus is on the data controller to satisfy the investigator that the appropriate measures were in place or whether the investigator must come to a conclusion on the data it collects that it had been shown that the data controller failed to comply with its statutory obligations. This is probably well settled, and the Respondent does appear by this decision of the 13th of July, 2018 to decide matters by the standard of a failure of the Appellant to satisfy the Respondent of compliance, and did couch its ultimate finding on s.2(1)(d) at paragraph 27 in those terms. The finding in the decision at paragraph 14 was certainly not in those terms. There was a positive finding that these "agreed procedures" [the Respondent's quotation marks] were only in place after the inadvertent disclosure of the 12th of May, 2014. I am making a finding that this positive finding, even if made in a process that seeks the protection of the nomination inquisitorial, is not founded on the information available. Further, if an inquisitor finds an account so unpersuasive, that it is going to draw an inference to the direct contrary, in the course of making a finding that will impose liability, I am of the view that fair procedures would require that the subject of the investigation put a notice of this. If this issue was raised, it might well have been that the appellant could offer direct proof that the judgement delivered on the 9th of May, 2014 was marked was marked no redaction necessary which could go to

prove the procedures were in place prior to the 12th of May, 2014 or could otherwise show that the practice existed prior to the unauthorised disclosure. In this context, I do note that the letter of November, 2014 contained a reference, as quoted above, to the use of stamps provided. One avenue by which the appellant might demonstrate that the practice predated this unauthorised disclosure would be to demonstrate when the process of issuing stamps to the judiciary commenced. This opportunity didn't arise, because the respondent didn't notify the appellant, that it was considering taking the statements made by the appellant as proof of the contrary of what they asserted. I am satisfied that the finding at Paragraph 14 of itself, renders the finding of a breach of s.2(1)(d) invalid.

80. I should indicate that I am coming to this view with no personal knowledge from my service as a Judge sa to what procedures were in place. I had not declared and not sitting as Judge in November, 2014 and since them as a Circuit Court Judge, I have no involvement of any kind with the procedures that apply to the submission and publication of written judgements on the Courts Services website and I have no need to be informed of these procedures. These procedures and the commentary about written judgements by O'Donnell J. in DPP v Nash relates to the Superior Court as are established directly under the Constitution.

81. Moving beyond that finding of the absence of procedures, there is to my mind a more fundamental failure with the finding of a breach of s.2(1)(d) at the first paragraph in the section numbered 27 in the decision. This states: –

> **27. On the facts established, the court service has not demonstrated that your personal data in the form of your name was processed in accordance with section 2 of the acts given the unauthorised disclosure of your name in the judgement.**

8.2 This might possibly be read as a finding based on the established fact that the procedures were only put in place after the unauthorised disclosure, which as just indicated is a flawed finding, however another reading is that the decisive fact in establishing that there was non-compliance with section s2, meaning by the terms of decision a breach of s.2(1)(d) is that there was unauthorised disclosure of the notice party's name in the judgement. I am holding that this is the effect of the finding and that it isn't in accord with the statutory regime. The mere fact of an unauthorised disclosure doesn't establish a breach of s.2, the very next words of the decision make it clear that an unauthorised disclosure can occur even if section 2 were deemed satisfied, yet the terms of the decision in the first paragraph of Paragraph 27 is as stated. It seems to me here that the Respondent fall on this specific issue, into the error which the Appellant contended tainted the whole procedures, of conflating the fact of the failure to adhere to the terms of the Court order of the 30th of January, 2014 with the issue of whether a data protection breach occurred. . I am satisfied that those words quotation "given the unauthorised disclosure of your name in the judgement" render the finding quoted above bad in law. I'm of the view that this is so even if, the respondent was entitled to conclude the procedures only came into place after 12 May 2014. However I also remain of the view that the Respondent was not entitled to come to that conclusion.

8.3 In contrast, as concerns the finding of a breach under section 2A, I find the respondents reasoning that the dissemination of the notice party's name on the website was not required either for the administration of justice or for the performance of the function conferred under an enactment or necessary for the performance of any other function of a public nature, has not just not been showd to be wrong, but in fact, the reasoning of the Respondent is coercive on this isuse. I can see no error in the conclusions drawn that there was a breach of section 2A. There being a breach of section 2A, if sensitive personal data was disclosed, there was a breach of section 2B and the appellant in these

proceedings conceded that the matters disclosed did constitute sensitive personal data. The finding of a breach of section 2B may if there is no other flaw be upheld.

84. Regardless of the validity of that reasoning, the Appellant has also made the case that the investigations conducted by the Respondent might provide a foundation for a finding of a breach, that there can be no such finding due to an absence of fair procedures in the course of the investigations.

85. The appellant relies upon a number of instances is demonstrating a lack of fair procedure. It is contended that the Appellant was given insufficient detail as to the facts and law being asserted by and on behalf of the Notice Party in the making of the complaint. Following the revitalising letter of complaint of the 25th of July, 2016, the Appellant wasn't shows the exact terms of the complaint but it was summarised and the Appellant made a response on the 9th of September, 2016 and enclosed the report to the Ombudsman and this was summarised for the Notice Party. In response a detailed letter was sent by the notice party's solicitors, that in particular made a detailed legal challenge to the contention of the appellant that it not a data controller. In addition, this letter contended *"The court service admitted that [the notice party's] sensitive personal data was neither processed fairly nor lawfully since the court order was in place making such publication illegal."* The footnote to this assertion identified this admission as being the letter of 21 October 2004 which accompanied the revitalising letter of 25 July 2016. This assertion found its way into the decision of 13 July 2018, the fact of the assertion of the admission being specifically noted at paragraph 6. It has been averred on behalf of the Appellant and it has not been this contradicted that at no stage was the outline of the legal submissions contained in the letter of 9 September 2016 communicated to the Appellant, and nor was the fact that it was being asserted that that the appellant had made an admission. The appellant also makes the case that it was not notified of the email exchanges as to asserted continuation or renewed unauthorised disclosure which are referred to in the decision at paragraph 12. The appellant also makes the case that once the respondent decided that the recently published authority of the Wirtshaftakademie Schleswien-Holstein case already referred to was of decisive import in coming to view on this case and in circumstances were the decision only issued in June 2018, the fair procedures would have required the Respondent to bring this to the notice of the Appellant. The Appellant also contends that the fact that the Respondent was considering findings under s.2(1)(d), s.2A and s.2B was not notified to the appellant in advance of the findings, so thereby denying them an opportunity to respond. As concerns the s.2(1)(d) finding, I have previously referred to the fair procedures issue arising from the conclusion at paragraph 14 concerning the existence of the agreed procedures on 12 May 2014 which I believe is of significance.

86. It appears to me in the main, that a breach of fair procedures in the course of the decision-making process will only be relevant if has a appreciable impact upon the decision-making process. It is in these circumstances that a failure in procedures, such as the failure to allow a party to address the relevant issue can result in the decision being condemned. It is not fully clear that even an egregious error in fair procedures will render a decision invalid, if it held that the failure in fair procedures had no impact upon the decision. Against that, if there was a complete failure to notify a person at all the procedure was underway, I would foresee very little prospect of it being said that the failure to notify the person would have no effect on the process. I will also comment though, that the requirement of fair procedures can't be sidestepped simply by asserting that the process is inquisitorial rather than adversarial. If a decision is being made that will impose penalty or liability upon an entity entitled to protection of their procedures,, then even though the requirements of fair procedures are contextual, the brandishing of the word inquisitorial isn't a shield against challenge. In making submissions as to the law, there was a tendency on the part of the Appellant to explain why the response made by the respondent should not be accorded weight rather than making a positive case based on actual

consequences of the failings in procedures. In the course of the arguments as to the applicable law the Appellant sought to distinguish the decisions of Grange v. Information Commissioner [2018] IEHC 108 and the National Maternity Hospital v Information Commissioner [2007] 3 IR 643 is relied upon by the respondent and put forward the case of Shatter v. The Data Protection Commissioner [2017] IEHC 670 , were the High Court held that the appellant had not had not received the benefit of their procedures, because a document that was identified as vital and decisive was not disclosed that appellant. Meenan J held:-

> *"Fair procedures require that, at least that a copy of this document would also be shown to the appellant. This was not done. As a result, the appellant was deprived of an opportunity to make any observations or submissions concerning the central piece of evidence in the complaint."*

87. Applying this test of centrality, I can come to firm conclusions as concerns fair procedures. The first is the view I have already expressed that if the respondent was going to interpret statements made on behalf of the appellant is proving the contrary, the appellant should have been given indication of this to be afforded an opportunity to respond. If it had been the case, that the notice party had put forward some document that contradicted the statements of the appellant, then clearly the appellant should have been put on notice of such a document. If however the contradiction comes not from an independent document but from the assessment by the respondent that the lack of persuasiveness of the appellant's document, proves the contrary, I feel the appellant should be given opportunity respond to that. The issue of fair procedures was not the sole ground upon which I formed the view that the finding on s.2(1)(d) should be condemned.

88. The second area where I feel there may be a significant breach of fair procedures, although this may affect the extent of the decision rather, rather than the fact of the decision, arises from the nondisclosure of emails and communications which the deponent in behalf of the notice party has averred were sent to the Respondent, and I am taking it are the emails referred to in paragraph 12 of the decision. These emails indicate that the second iteration of the judgement in this case was published on the website, when this case was never put to the Appellant and the Appellant was never where this case was being made. The Appellant's understanding was that the sole unauthorised disclosure was that which occurred on 12 May, 2014 and was removed from the website on 14 May 2014 with the communication to the various libraries to whom the copy of the judgement had been sent, requesting deletion being made on the 15 May 2014. The only indication of any disclosure beyond was the name of the notice party being published in the Irish Medical Times with this being traced back to the website and which on an understanding of the Appellant on the basis of what awas put to the Appellant was the disclosure between the 12th and 14th of May 2014.

89. I am satisfied that the requirements of fair procedure require a clarification to the decision of 13 June 2018, that the unauthorised disclosure relates only to the disclosures that occurred between the 12th and 15th of May, 2014 and that no other unauthorised disclosure by the Appellant has been established. This may or may not have any significance in any subsequent proceedings founded in the Data Protection Act 1988 and 2003, but as far as this decision of 13 June 2018 is concerned. It can only apply to the disclosure between the 12th and 15th May, 2014.

90. In this context I know the notice party filed an affidavit to the effect the disclosure was more extensive than that which occurred between the 12th and 15th of May 2014 but these matters could not properly be the subject matter of the decision of 13 June 2018. This might, depending upon what the facts were objectively, and I am making no finding about that, mean that the Respondent did more harm to the notice party than to the Appellant by failing to adhere to fair procedures in dealing with

Appellant on this issue, but that doesn't alter the fact there was a material breach of fair procedures as concerns any assertion of unauthorised disclosure after 15 May 2014.

91. I am not however persuaded that the other assertions of fair procedures unseat or can serve to condemn the decision. It seems to me that the fact that the notice party was seeking to construe the letter of 21 October, 2014 as an admission should have been made known to the Appellant by the Respondent. However, I believe that although this was a breach of fair procedure it was not a breach that here the appreciable impact upon the decision that was reached. Otherwise, I accept that the nature of the process undertaken by the Respondent, is one where there is a fact-finding process by the respondent who then applies her expertise in the operation of the data protection regime, including her view of the applicable law, and comes to a conclusion whether breach occurred. I accept the contention on behalf of the Respondent that the Respondent is not obliged during the fact finding process to set out any view of the law to the complainant or to the person whose conduct is being considered. The process engaged in by the Respondent in forming a view of the law, is not done in the nature of an adversarial dispute such as would occur in the Courts where there would be an exchange of legal submissions. I also accept that in the context of data protection that a full exchange of all communications and submissions by each party could often be an inadvisable and is not appropriate to the nature of the process. In particular, I don't see any basis on which the respondent would be under a duty to indicate what authorities of the Court of Justice it finds to be persuasive and so was to ask the notice party and the party whose conduct is being considered for their views as to the law. It is open to either side to make legal submissions and in this case both sides did, although submissions in the behalf of the appellant were not made a firm of solicitors. The respondent had an obligation to consider these and an entitlement to take them into account if they were found to be persuasive, and was obliged to set out the basis of the legal reasoning upon which the Respondent ultimately decided, so as to afford an appeal on the law and I'm satisfied that the respondent did so. In any event as far as nondisclosure of the law is concerned, since I have found the reliance on the Wirtshaftsakademie Schleswig Holstein case was justified, the fact that there was no opportunity to make submissions to the contrary could not be taken as affecting the ultimate decision.

92. In conclusion although this process did result in a decision that contained some errors and it was reached in in a manner that involved several breaches of fair procedures, in that matters that should have been notified to the Appellant by the Respondent were not notified, that nonetheless the decision did validly reach the conclusions, that the Appellant was a data controller and that there was a breach under section 2A and 2B. However, the finding that there was a breach of s.2(1)(d) must be condemned and there must be an express statement that the extent of the breach is limited to the unauthorised disclosure is occurred between the 12th and 15th of May, 2014.

93. I will hear submission as to the appropriate form of order.

[APPROVED, CIRCUIT COURT APPROVAL

NOT AN INSTRUCTION FOR PUBLICATION]