SHERIFF APPEAL COURT

[2026] SAC (Civ) 17
GLW-SG5450-24

Appeal Sheriff O'Carroll

OPINION OF THE COURT

delivered by APPEAL SHERIFF O'CARROLL

in the appeal in the cause

EAST DUNBARTONSHIRE COUNCIL

Defender and Appellant

against

"PAUL PATON"

Claimant and Respondent

Defender and Appellant: McLaughlin, solicitor; EDC
Claimant and Respondent: Party

4 March 2026

Introduction

[1] In this somewhat unusual appeal, the claimant and respondent to the appeal ("the claimant") raised a claim for damages under simple procedure alleging the defender and appellant ("the Council"), acting as an education authority, breached his rights under data protection legislation by failing to rectify his inaccurate personal data as a result of which he suffered loss and damage. The sheriff found for the claimant and awarded damages. The Council appeals, arguing the sheriff erred in law in concluding that the personal data in question was that of the claimant, instead of that of his daughter, who was at the relevant time a primary school pupil. I refer to that child as Caitlin (which is not her real name) to

protect her identity. I have pseudonymised the name of the claimant for the same reason. This appeal was assigned to the Chapter 8 appeal procedure and proceeded by way of written submissions alone.

The background

[2] In 2019, Caitlin experienced unpleasant episodes of bullying at her primary school, which posed a risk to her physical safety and emotional well-being (the two "hazards"). The claimant raised his concerns with the head teacher. On 23 May 2019 the head teacher (acting as risk assessor) prepared a draft risk assessment on a standard form. That draft assessment recorded that a series of incidents in the school led to the claimant being very concerned about Caitlin's physical and emotional well-being. Sections of the form also include the identity of the school, the date, the description of the activity or hazard, the consequence of the hazard or risk, current control measures, recommended control measures, management action taken and implementations, training, personal protective equipment as well as the signatures of the manager and assessor. No issue was taken with most of the form.

[3] However, part of the form included an assessment by the risk assessor of the "severity of risk" of each hazard who assigned a "risk priority rating" graded as "high" or "medium" or "low". The draft risk assessment scored the "risk priority rating" of physical risk as "medium" and the "risk priority rating" of emotional well-being as "high".

[4] That draft risk assessment was copied to the claimant for his views. The claimant queried the risk priority rating scores in an email exchange with the risk assessor on 31 May 2019. The risk assessor explained that due to control measures put in place since the draft was created, the risk priority ratings were now lower and had changed to "low" (rather than medium) for physical hazard and "medium" (rather than high) for emotional well-being

hazard. The claimant responded saying he had assumed that the original scores would come down, thanked the assessor for confirming that reduction, whilst continuing to express concern that the risk priority rating for emotional well-being was as high as medium. He wanted to know what else could be done to bring that risk priority rating down. By email of the same day, the assessor said that the claimant should keep talking to Caitlin, monitor her media use and ensure that Caitlin had no further contact with the other child among other advice. There was no change expressed then to the reassessed priority risk ratings of low and medium.

[5] Unfortunately, all did not go well from there. Further events caused the claimant to make a formal complaint to the Council in June 2019 about various matters. As of August 2019, the Council's position continued to be that the risk priority rating for emotional well-being was medium. The Council rejected most of the complaints. The claimant then took them to the Scottish Public Services Ombudsman. The assessment of the risk priority rating continued to concern the claimant.

[6] Of some importance to this appeal is the admitted circumstance that at some stage, the Council prepared another risk assessment form, apparently dated 31 May 2019 ("the second version") which was in similar terms to the previously mentioned risk assessment. However, the second risk assessment form differed from the first version in two significant respects. First, the risk priority rating as regards Caitlin's emotional well-being was rated as low (rather than medium). In addition, the "recommended control measures" were boosted by an additional two sentences setting out actions which Caitlin's parents were advised to continue taking. The second version had not previously been provided to the claimant. It was the second version which was provided to the Ombudsman by the Council during the Ombudsman's investigation of the claimant's complaints.

[7] Following protected procedures, correspondence and litigation, with which this appeal is not concerned, on 19 June 2024 the claimant wrote to the Council's complaints unit complaining about the second risk assessment in that it incorrectly recorded the risk priority rating as regards his daughter's emotional well-being as low for emotional well-being. No complaint was made about the other contents. He sought rectification of this inaccurate data.

[8] The Council conceded that the risk priority rating as regards emotional well-being was wrongly recorded in the second version. However, the Council decided that it would not rectify that version and gave the claimant that decision in July 2024.

Legislation

[9] The claimant then raised proceedings claiming compensation relying on Article 82 of the United Kingdom General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018. Article 82.1 UK GDPR provides:

> "Any person who suffered material or non-material damage as a result of an infringement of this regulation shall have the right to receive compensation from the controller or processor for the damage suffered."

[10] It is of some importance to note that the claimant's claim against the Council relied on the proposition that the data which he claims was false or inaccurate was his personal data, that accordingly he was the data subject and that accordingly he had the right to seek rectification. The right to rectification derives from Article 16 GDPR which provides as follows:

> "The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement."

[11] Section 3 of the 2018 Act defines the following terms:

> "Personal data means any information relating to an identified or identifiable living individual…"
>
> "Identifiable living individual means a living individual who can be identified directly or indirectly, in particular by reference to (a) an identifier such as a name, an identification number, location data or an online identifier or (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual".
>
> "data subject means the identified or identifiable living individual to whom the personal data relates".

It is accepted by the parties that the Council is the data controller responsible for deciding the purposes for which the personal data is processed and the means as well as the data processor. These definitions are for present purposes the same as those found in Article 4 UK GDPR.

[12] Notwithstanding its previous refusal to rectify, once the action had been raised, during the course of proceedings, the Council conceded that the disputed data was incorrect and now agreed that it should be rectified. The Council however maintained its position that the data in question was not the personal data of the claimant and therefore the claimant's claim for compensation should fail.

The sheriff's decision

[13] Against that background the sheriff found for the claimant and awarded damages. The sheriff decided that the data in dispute was the personal data of the claimant. In so deciding, he took into account the statutory definitions of personal data and data subject: see above. He also considered two court decisions being *Nowak v Data Protection*

Commissioner [2018] 1 WLR 3505 (Court of Justice of the European Union) and *Ashley* v *Revenue and Customs Commissioners* [2015] 4 WLR 29 (Kings Bench Division).

[14] *Nowak*, was a case about the right of a trainee accountant, who had sat and failed an accountancy examination, to obtain his examination script and examiner's comments. The court held that the examination script and comments did amount to personal data entitling Mr Nowak to rights of access. At paragraphs 27 to 54, the court held that Mr Nowak was entitled to that information since he was a natural person who could be identified either directly through his name or indirectly through an identification number. What matters, said the court, is whether an identifiable individual can be identified by the data in question by reference to some other factor. He also had a right to rectification (but not so as to enable him to have an incorrect answer marked as correct). The court held that personal data encompasses all kinds of information, not only objective but also subjective in the form of opinions and assessments, providing that the information "relates" to the data subject: paragraph 34. Information relates to the data subject where the information "by reason of its content, purpose or effect is linked to a particular person": paragraph 35.

[15] In *Ashley*, the claimant made a wide-ranging subject access request, seeking his personal data processed by HMRC, in connection with an enquiry into his tax return. Issues arose as to which of the information sought was personal data including whether data (which did not itself directly identify the claimant) held by the Valuation Office was also personal data of the claimant. The court held that the relevant question was whether the information itself met the criteria of "relating to an identified or identifiable natural person" and not whether the overarching processing that was taking place, or the reason for processing, were related to such an individual. It held that the "relating to" requirement will be satisfied where the information by reason of its "content, purpose or effect" was

linked to a particular person. The concept of information being linked to the data subject was to be construed broadly although it had to have some limitations and accordingly an indirect or tenuous link was unlikely to suffice. However, information which would not, when viewed in isolation, meet the definition of personal data, might do so where it was interlinked or connected to material that was itself the personal data of the relevant individual. The court also held that in cases of difficulty or ambiguity, it would be appropriate to consider whether affording rights of access to the individual would serve the legislative purposes.

Analysis and discussion

[16] What the case law and the two cases cited demonstrate in my view is that the correct approach to determining whether a right to access and associated rights exist, once the controller or processor of the data is identified, is firstly to identify the data to which access and rectification is sought. Then decide whether that data is personal data or not considering the statutory definition and wide interpretation of personal data adopted by the courts. Then, the task is to identify who is the subject of the data, that is to say the identified or identifiable person to whom the data relates. Then determine whether the data subject is entitled to rights of access or rectification or any other rights provided by the data protection legislation. Then, ascertain whether that that right has been asserted and exercised. Then, where the asserted right has been refused or blocked in some way, determine whether the data subject has a remedy and if so what and on what basis. Remedies include access, erasure, rectification, blocking and compensation, among others.

Whose personal data?

[17] In this appeal, the parties and the sheriff narrowed the issue in dispute to a single question: was the disputed data the personal data of the claimant or of Caitlin? In doing so, all concerned appear to have assumed that the question was binary, that the data could be the personal data of only one or the other. However, as frequently occurs in practice, any given piece of information may amount to personal data simultaneously of more than one person. See the useful discussion in Jay, *Data Protection Law and Practice* (5th Edition), at paragraphs 13-033 et seq. Information may inextricably form personal data of two or more persons. In the *Novak* case for example, the court noted that the personal data sought by Mr Novak was also the personal data of the examiner. In *DB* v *General Medical Council* [2019] 1 WLR 4044, the independent expert report obtained by the GMC regarding the competence of a GP's treatment, sought by the patient who alleged negligent treatment, was simultaneously the personal data of the patient and the GP (and it might be said, though not argued, that of the author as well). Another example might be a joint bank account statement: that will comprise the personal data of each joint account holder. In this appeal, the Council itself states in its submission, correctly, that the disputed data was also that of the head teacher. The legislation itself makes specific provision for access rights in such cases of mixed personal data: see Articles 5 and 15 of GDPR and Schedule 2, Part 3, paragraph 16 to the 2018 Act. See also paragraph 17 of Part 3 for specific provision made in the case of education officials, (such as risk assessor in this case) which removes the reasonableness test as regards the disclosure of that education official's personal data in certain circumstances. Accordingly, it cannot be said that if the information comprised the personal data of Caitlin, it cannot also be the personal data of the claimant.

Caitlin's personal data

[18] In my view, it is obvious that the data comprising the risk priority rating for emotional wellbeing was Caitlin's personal data. That is because it was information, comprising data, which related to an identifiable individual. She was identifiable from that information because of the other data which the Council as data controller held on her. That other data included but was not limited to the other information in the risk assessment. She was a pupil in the appellant's school. The Council held other records on her. It was a scoring - an opinion - (whether objective or subjective matters not), by an employee of the Council, about a specific risk posed to Caitlin's well-being, (her "mental identity"): see *Nowak,* paragraph 34; Article 4(1) UK GDPR. She was the subject of the data and was therefore entitled to the usual statutory rights.

The claimant's personal data

[19] That data was also the personal data of the claimant, in the particular and unusual circumstances of this case. The data by reason of its content, purpose or effect related to the claimant in that the information linked to the claimant: see *Nowak* paragraphs 34 and 35. That is explained by the sheriff's findings in fact made after hearing evidence and considering the documentary evidence placed before him. There is no appeal concerning these findings of fact, or indeed any other finding of fact. The sheriff held that the purpose of the data was not only to inform the Council's employees' decisions regarding the safety and well-being of Caitlin, it was also to satisfy the claimant, as one with parental responsibilities, that those matters were being adequately dealt with by the Council's officers. As the sheriff also found, the data formed one of the bases on which the recommended control measures in the risk assessment was formulated. Those measures

included a reference to the claimant as the parent who initiated the process, whose identity and concerns are recorded at the outset of the risk assessment and who was enjoined to assist in the control measures designed to ensure the safety of his daughter, a pupil at the Council's school. The sheriff found in fact that the content and the extent of the recommended control measures directly related to the risk priority rating in question. Furthermore, given that Caitlin was at the time a primary school pupil, it is obvious that the claimant, as her father, required to exercise his parental responsibilities, which included responsibilities for his daughter's well-being and safety. In the circumstances of this unusual case, it is clear that the personal data was mixed personal data being that of Caitlin, her father, the claimant (and the head teacher).

[20] The reasoning of the court in *Ashley*, especially at paragraphs 161 and 162, supports this contention. That is, the data held by the school personal to the claimant, including but not limited to the personal data of the claimant contained in the risk assessment form, linked him directly to the disputed data. The close connection between the disputed risk priority rating and the claimant's involvement in the making of the risk assessment and the risk control measures made it his personal data.

[21] Of course, standing the provisions of the legislation noted above, in a mixed data situation, the data controller, before disclosing the data, requires to carry out an evaluative exercise before deciding whether to disclose personal data, which is also that of another, to the requester. On the facts of this case however, that question does not arise. That is because the data had already been disclosed to the claimant while he was exercising parental rights. Further, there would have been no sensible argument that it was not reasonable to disclose such mixed data to the claimant. In any event, he supplied the written consent of his daughter in 2024 when making the formal rectification request.

[22] Therefore, the claimant being a data subject had the right to seek rectification. The Council accepts that rectification was required. It accepts the data was not rectified without undue delay. In terms of Article 82 UK GDPR, the claimant was entitled to seek compensation as a person who had suffered loss and damage as a result of a breach of the Council's statutory duties. There is no appeal against the finding of the sheriff that the claimant suffered loss and damage and there was a causal connection between that and the Council's breach of its data protection statutory responsibilities. The sheriff awarded damages on that footing. There is no appeal against the quantum.

[23] Accordingly, it follows that this appeal must fail. The appeal is refused. No submissions were made as regards expenses. Since the claimant was unrepresented and the appeal proceeded by way of written submissions alone, I expect that there will be no motion for expenses by either side. However, I will reserve the question of expenses meantime and will pronounce an interlocutor accordingly unless a motion to contrary effect is made within 14 days of the date hereof.