



Case Reference: EA-2022-0184

First-tier Tribunal
General Regulatory Chamber
Information Rights

Heard: by CVP
Heard on: 2 February 2023
Decision given on: 28 February 2023

Before

TRIBUNAL JUDGE BUCKLEY

TRIBUNAL MEMBER PAUL TAYLOR

TRIBUNAL MEMBER EMMA YATES

Between

IAN DRIVER

Appellant

and

THE INFORMATION COMMISSIONER

Respondent

Representation:

For the Appellant: In person

For the Respondent: Eric Metcalfe (Counsel)

Decision: The appeal is dismissed.

REASONS

Introduction

1. This is an appeal against the Commissioner's decision notice IC-101602-Y9H8 of 9 June 2022 which held that Thanet District Council (the Council) was entitled to rely on s 40(5B) of the Freedom of Information Act 2000 (FOIA) to refuse to confirm or deny whether it held the requested information.
2. Mr. Driver applied to postpone the hearing due to the respondent's skeleton argument being provided the day before the hearing. I refused the application for the reasons already provided to the parties, but ordered that the start time be delayed to 12pm to allow further preparation time.
3. The tribunal was greatly assisted by the clear and focussed submissions made by both Mr. Driver and Mr. Metcalfe.

Factual background to the appeal

4. This appeal relates to a request for disclosure of personal data about a local authority Councillor ('Councillor X'). The appellant argues that if it is held by the Council, it is likely to reveal that Councillor X behaved improperly or unlawfully.

Requests, decision notice and appeal

The request

5. This appeal concerns the following request made on by Mr Driver on 4 February 2020:

Please confirm or deny whether Councillor (name redacted) has been required to pay money to the council in relation to any fly tipping incident(s).

If (name redacted) has paid the council any money in relation to any fly tipping incident(s) please tell me how much (redacted) paid to the council and when.

Please also provide me with copies of all communications between the council and (name redacted) about any fly tipping incidents which (redacted) has been linked to and any communications between officers, and/or any communications between council officers and councillors (other than (name redacted)) about (name redacted) and (redacted) links with any fly tipping incidents.

I understand that the council served a Section 108 (Environmental Protection Act 1990) on (name redacted) requesting (redacted) to provide information to assist in a criminal investigation into a fly tipping incident. I also understand that (name redacted) was interviewed under caution by officers of the council about a fly tipping incident. Please provide me with a copy of the Section 108 (Environmental Protection Act 1990) notice

which was served on (name redacted) by the Council. Please provide me with a copy of the recording of the under caution interview or a transcript of that interview with (name redacted).

Please provide me with copies of ALL of the pictures taken by the council of any fly tipped rubbish with which (name redacted) has been linked.

I understand that the matters described above took place between 2016-19.

The response

6. On 26 February 2020 the Council responded to the request and refused to confirm or deny whether it held the requested information relying on s 40(5B)(a)(i) FOIA. It upheld the position on internal review on 26 January 2021. Mr Driver referred the matter to the Commissioner on 20 April 2021.

The Decision Notice

7. In a decision notice dated 9 June 2022 the Commissioner decided the information requested, if held, was personal data. The Commissioner accepted that if the requested information was held, it would constitute criminal offence data in that it related to potential investigations of the commission of the criminal offence of fly tipping.
8. Criminal offence data can only be processed, which includes confirming or denying whether information is held, if one of the conditions of Schedule 1, Parts 1 to 3 of the Data Protection Act 2018 (DPA 2018) can be met. The Commissioner considered it likely that only two of the Schedule 1, Part 3, conditions might ever justify such processing of personal information of this type. These are:
 - 8.1. That the data subject had given their explicit consent for the public authority to provide a confirmation (or a denial) that information is held; or
 - 8.2. That the data subject has manifestly made the information public themselves.
9. The Commissioner was satisfied from the information provided by the Council that none of the conditions required for the processing of criminal offences data have been satisfied. Providing a confirmation or denial would breach data principle (a). The Council was therefore entitled to refuse to confirm or deny whether it held the requested information under s 40(5B)(a) FOIA.

Notice of Appeal

10. The grounds of appeal are:
 - 10.1. that the Commissioner should have concluded that the conditions in schedule 1, part 2 (substantial public interest conditions) are met.

- 10.2. That the Commissioner failed to take account of the appellant's rights as a journalist under article 10 ECHR.

The Commissioner's response

11. The appellant does not identify a basis under article 6(1) GDPR under which the council could lawfully confirm or deny whether it holds criminal offence data within the scope of his request. The only arguable basis is article 6(1)(f) i.e. that the processing is necessary for the legitimate interests of the public. The appellant would have to show that the interest in transparency and his own interests in receiving confirmation or denial were not overridden by the interests of fundamental rights and freedoms of the data subject. The appellant would also have to show that one of the conditions under Schedule 1 were met.
12. Paragraph 11(1) DPA 2018 (protecting the public against dishonesty etc.) requires that the processing be 'necessary for the exercise of a protective function' as defined by para 11(2). The Commissioner submits that FOIA is not in itself a 'protective function' intended to protect members of the public against any of the grounds in para 11(2).
13. The duty to confirm or deny in response to a FOIA request does not in itself make a disclosure lawful. Section 40(5B)(a)(i) FOIA is engaged where 'the confirmation or denial...would (apart from this Act) contravene any of the data protection principles.' The test is whether confirmation or denial 'otherwise than under' these laws would contravene a data protection principle.
14. Para 13(3) is not met in the appellant's case. Were the Council to provide confirmation or denial they would be doing so for the purpose of responding to a FOIA request, not for the purposes of journalism. Nor is the Council obliged to hold a belief that confirming or denying whether the requested criminal offence data is held would be in the public interest as required under para 13(1)(e).
15. Even if the Council were somehow obliged by virtue of article 10 ECHR to facilitate the disclosure of information in the public interest, the appellant would still have to show that disclosure was necessary for reasons of substantial public interest. The appellant has failed to demonstrate the concrete, wider benefits of potential disclosure of the information in question.
16. The Commissioner submits that para 36 of Schedule 1 cannot be relied upon as a condition for processing criminal offence data. Even though the appellant is not required to show a substantial public interest, para 13 also requires the controller to reasonably believe that the processing is necessary in the public interest.
17. Although the Council have no legal basis to confirm or deny whether the requested information is held and the exemption in section 40(5B)(a) FOIA applies, that does not prevent the Council from disclosing the requested information if it is satisfied

that it has complied with its obligations under DPA 2018 i.e. that the criteria in para 13 are met, it can legitimately, as a data controller, make a voluntary disclosure to a journalist without breaching DPA 2018. Alternatively the Council could disclose the requested information to a journalist on a discretionary basis outside of FOIA with conditions attached. The appellant's reliance on article 10 ECHR does not assist him.

18. If the tribunal were to consider disclosure to be lawful it would still be necessary to consider if it would be fair and transparent.

Mr. Driver's reply

19. Both parties agree that the requested data, if held, is criminal offence data.

20. Mr. Driver argues that the requested information can be lawfully processed without the need to secure the consent of the data subject and without the data subject having made the requested data public.

21. Mr. Driver relies on article 6(1)(f) GDPR.

22. Part 2, Schedule 1 DPA 2018 lists all the substantial public interest conditions which provide for the lawful processing of special category and criminal offence data. Mr. Driver relies on:

- 22.1. Preventing or detecting unlawful acts
- 22.2. Protecting the public against dishonesty etc.
- 22.3. Regulatory requirements relating to unlawful acts and dishonesty etc.
- 22.4. Journalism etc. in connection with unlawful acts and dishonesty etc.

23. Part 3, Schedule 1 DPA 2018 para 36 makes the processing of criminal offence data less stringent than the processing of special category data, by disapplying any requirement in a part 2 Schedule 1 condition that processing is necessary for reasons of substantial public interest.

24. A public interest which overrides the data subject's right to privacy must still be established via a balancing act.

Preventing or detecting unlawful acts

10. Preventing or detecting unlawful acts

(1) This condition is met if the processing –

(a) is necessary for the purposes of the prevention or detection of an unlawful act,

(b) must be carried out without the consent of the data subject so as not to prejudice those purposes, and

(c) is necessary for reasons of substantial public interest.

(2) If the processing consists of the disclosure of personal data to a competent authority, or is carried out in preparation for such disclosure, the condition in sub-paragraph (1) is met

25. If held by the Council, the processing of the requested data is necessary because it will reveal that Councillor X engaged in an unlawful criminal act which was contrary to paragraph 34 (Duty of care etc. as respects waste) of the Environmental Protection Act 1990.
26. The Council is the competent body for investigating and sanctioning those who breach the Environment Act 1990.
27. The Council, as the competent authority, holds records of the actions it has taken to enforce the Environment Act 1990. As the only organisation holding such records it is therefore necessary for the Council to process such data should it receive a legitimate data request.
28. With no alternative sources available to secure the requested data the processing will also be proportionate.
29. Processing is also necessary because there is a powerful, if not substantial, public interest in the conduct and behaviour of elected politicians.
30. The requested data, if it is held and disclosed, would likely reveal that Councillor X did commit a criminal act for which X was formally cautioned. The request therefore falls within the dictionary definition of "detecting".
31. If the requested data was to be disclosed, and if it establishes that Councillor X did act unlawfully, Mr. Driver intends to submit the data to the appropriate competent authorities (Kent County Council (KCC) and the Council) as a standards complaint under the terms of the Localism Act 2011. This action would engage the processing condition set out in paragraph 10.2 in that the processing is carried out in preparation for disclosure to a competent authority.

Protecting the public against dishonesty etc.

10. Protecting the public against dishonesty etc

1. This condition is met if the processing

- a. is necessary for the exercise of a protective function,
- b. must be carried out without the consent of the data subject so as not to prejudice the exercise of that function, and
- c. is necessary for reasons of substantial public interest.

2. In this paragraph, "protective function" means a function which is intended to protect members of the public against –

- a. dishonesty, malpractice or other seriously improper conduct,

- b. unfitness or incompetence,
 - c. mismanagement in the administration of a body or association, or
 - d. failures in services provided by a body or association
32. If the requested data is disclosed and confirms that Councillor X committed an unlawful act and if Mr. Driver published articles about X's unlawful acts this would amount to a protective act as:
- 32.1. his journalistic work may cause embarrassment to Councillor X leading to their resignation from office;
 - 32.2. this might cause X's political party to exclude X from membership, or not to select X as a future election candidate.
 - 32.3. this may be likely to cause voters not to support X if they were to stand for election again.
33. Mr. Driver will have exercised a protective function which will have alerted voters to the dishonesty, malpractice or other seriously improper conduct of Councillor X. It is necessary, if the data is held, for the Council to process it in order that Mr. Driver can play a protective role. The Council is the only body holding the requested information.
34. The public interest in having a healthy democratic system which includes accountable, transparent and honest elected politicians is strong if not substantial.

Regulatory requirements relating to unlawful acts and dishonesty etc.

12 Regulatory requirements relating to unlawful acts and dishonesty etc

(1) This condition is met if –

a) the processing is necessary for the purposes of complying with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has –

(i) committed an unlawful act, or

(ii) been involved in dishonesty, malpractice or other seriously improper conduct,

b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing, and

c) the processing is necessary for reasons of substantial public interest.

(2) In this paragraph “act” includes a failure to act; “regulatory requirement” means –

(a) a requirement imposed by legislation or by a person in exercise of a function conferred by legislation, or

(b) a requirement forming part of generally accepted principles of good practice relating to a type of body or an activity.

35. The local authority standards committee is a regulator established by statute in order to oversee the behaviour of local authority councillors and to ensure that this behaviour complies with the local code of conduct and the Nolan principles. Mr. Driver intends to submit the data to the appropriate local authority standards committee for investigation. If the requested data exists it meets the processing condition set out in para 11(1) by assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has committed an unlawful act, or been involved in dishonesty, malpractice or other seriously improper conduct.
36. There is strong, if not substantial, general public interest in having effective political regulators in place to ensure that the behaviour of elected representatives is of the highest order. This public interest supports the efforts of journalists who work to uncover information which establishes wrongdoing by elected politicians and then passing on this information to the appropriate regulator. In this case the public interest in, and necessity for, processing the data is considerably enhanced because the allegations against Councillor X, if true, amount to extremely serious breaches of the TDC and KCC's Members' (councillors) Codes of Conduct.
37. If the withheld data proves the allegations against Councillor X to be true, there is a compelling necessity for, and public interest in, the processing of the requested data in order that the regulators can investigate and act.

Journalism etc. in connection with unlawful acts and dishonesty etc.

13(1) This condition is met if –

- a) the processing consists of the disclosure of personal data for the special purposes
- b) it is carried out in connection with a matter described in subparagraph (2),
- c) it is necessary for reasons of substantial public interest,
- d) it is carried out with a view to the publication of the personal data by any person, and
- e) the controller reasonably believes that publication of the personal data would be in the public interest.

(2)The matters mentioned in sub-paragraph (1)(b) are any of the following (whether alleged or established) –

- a) the commission of an unlawful act by a person;
- b) dishonesty, malpractice or other seriously improper conduct of a person;
- c) unfitness or incompetence of a person; d)mismanagement in the administration of a body or association;
- e) a failure in services provided by a body or association.

...

(4) In this paragraph-

...

"the special purposes" means-

- (a) the purposes of journalism;

...

38. Mr. Driver is a journalist. It was, and remains, his intention to use the requested information, should it exist, and be disclosed to him, to publish another article about Councillor X which will hopefully provide official corroboration of his earlier publications and allow Mr. Driver to provide a much fuller picture than previously.
39. The request complies with the requirements of para 13(1)(a), (1)(b) and (1)(d) DPA 2018.
40. It is clear that the request under this processing condition was necessary and proportionate as there is a strong public interest in disclosing misconduct and unlawful actions by an elected politician and in this case, if the allegations against Councillor X are true, the Council is the only organisation to hold the official corroborative information, required to support truthful, evidence based, journalism.

Fairness

41. Fairness of processing is determined by considering:-
 - whether the data subject has a reasonable expectation of confidentiality/privacy
 - whether the data subject's rights to confidentiality/ privacy override my rights to freedom of expression
42. The Council in its responses to the FOI request and internal review does not mention Councillor X's expectation of confidentiality.
43. **Bloomberg LP v ZXC** [2022] UKSC 5 states that a person under criminal investigation has prior to being charged, a reasonable expectation of privacy in respect of information relating to that investigation. According to Mr. Driver's tip off Councillor X admitted under caution that they had breached their legally required duty of care and were issued with a formal caution/warning that any further offences would be prosecuted and to pay around £750 as a fine. If this is true there was no possibility of Councillor X being subject to further investigations or being charged in relation to this offence.
44. Public figures, especially politicians, must have lower expectations of privacy/confidentiality than the ordinary citizen (**Couderc and Hachette Filipacchi Associés v. France** [2015] ECHR 992).
45. The ICO publication 'Request for personal data about public authority employees' provides further important guidance in relation to the confidentiality/privacy expectations of public authority employees which applies equally to local authority Councillors. 'Seniority' and 'public facing roles' are two factors related to a data subject's expectations of privacy/confidentiality.

46. At the time of my FOI request Councillor X occupied a very senior, public facing, political position in which they were involved in policy making and speaking on the behalf of the council. On this basis Councillor X could not reasonably expect to have a high expectation of privacy/confidentiality
47. Furthermore, the fact that Councillor X was involved in publicly representing the views of the Council on matters relating to fly-tipping law and regulations, when Councillor X themselves is alleged to have breached the same law and regulations will, if true, serve to reduce still further Councillor X's expectation of privacy/confidentiality.
48. The articles written by Mr. Driver, which he is sure Councillor X would have been aware of would, in his opinion, persuade a reasonable person to believe that if the allegations were true, then by exercising my FOI rights, he might eventually obtain copies of documents which incriminate Councillor X. Such a possibility would serve to significantly reduce Councillor X's expectation of confidentiality/ privacy related to this matter.
49. The findings in **DH v (1) Information Commissioner, (2) Bolton Council** [2016] UKUT 0139 (AAC) that it was not reasonable for a councillor to expect not to be identified where he is summoned for non-payment of council tax apply equally to a councillor who has not complied with the Environment Act duty of care requirement.
50. The disclosure of the data is likely to cause some reputational damage to Councillor X and may result in Councillor X being forced out of politics by voters and/or their party colleagues. This could be the cause of great embarrassment and distress to Councillor X and may result in loss of personal friendships and damaged relations with political colleagues. If Councillor X is forced to leave politics Councillor X will lose financial benefits. Although Councillor X and party colleagues were almost certainly aware of the two articles, Councillor X does not appear to have suffered any detrimental political consequences. There is no evidence from Councillor X about the future impact of disclosure.
51. Mr. Driver submits that the factors favouring processing of the data far outweigh Councillor X's expectation of and right to confidentiality/privacy.
52. The growing cost and incidences of fly-tipping in the Thanet area add to the weight of the general public interest in this matter. This local factor has been substantially added to the by the possibility that a very senior, public facing councillor, who:-
 - had collective cabinet responsibility for TDCs fly-tipping functions
 - had discussed and voted at a Cabinet meeting on the implementation of fixed penalty notices for householders who facilitate domestic fly-tipping
 - had spoken on behalf of the council against fly-tipping

is alleged to have facilitated the fly-tipping of their own domestic waste which is said to have included about 100 bags, some of which contained confidential KCC and TDC reports and documents.

53. There is also a distinct possibility, as is suggested by the tip-off and Mr. Driver's two articles that this matter may have been deliberately covered up by the Council.
54. If the allegations are true then TDC, the enforcer of the Environmental Protection Act 1990, would have been under a legal duty to report Councillor X to the council's Standards Committee for breaching the councillors' code of conduct. If the requested data serves to establish that the council may have concealed data related to Councillor X's alleged misconduct or unlawful actions then in doing so those council officers responsible would have breached their statutory duty. This would add further weight to the public interest in the processing of the data.
55. The Council's concealment of any unlawful acts which had it had investigated and penalised would be contrary to the principle of open justice.
56. Paragraph 92 of the ECHR Guide on Article 8 of the European Convention of Human Rights (2022) states:

Article 8 cannot be relied on in order to complain of personal, social, psychological and economic suffering which is a foreseeable consequence of one's own actions such as the commission of a criminal offence or similar misconduct.
57. Linked to this is a restriction based upon the principles that confidentiality cannot protect inequity, as explained in the ICO guidance on section 41.

Transparency

58. The Council publishes on its internet site a Privacy Notice for Information Governance which sets out the circumstances in which it may process the personal data it holds. This includes the possibility that personal data, including special category and criminal offence data, may be processed by the council in response to FOI or EIR requests.

Skeleton argument of the Commissioner

59. Mr. Driver must show that the processing in question, i.e. to confirm or deny whether the Council held any data within the scope of the request, would not contravene any of the data protection principles. In particular, Mr Driver must show that the processing would be lawful, fair and transparent.
60. In relation to lawfulness Mr. Driver relies on article 6(1)(f) that the processing is necessary for the legitimate interests pursued by the controller or by a third party.

The burden is on Mr. Driver to show that such interests were not overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. Mr. Driver does not address this.

61. In any event, Mr. Driver has to show that one of the conditions under Schedule 1 were met.
62. Note: the Commissioner conceded in oral argument that Mr. Driver was correct to submit that paragraph 36 of Schedule 1 disapplies the requirement for a substantial public interest, and therefore we have omitted those arguments from the summary of the skeleton argument.

Paragraph 10 – preventing or detecting unlawful acts

63. There is nothing to show that processing data to require the Council to confirm or deny whether it holds data within the scope of this request is necessary for the prevention or detection of an unlawful act. The information, if held, is criminal offence data relating to an investigation. This is putting the cart before the horse.

Paragraph 11- protecting the public against dishonesty etc.

64. The definition of ‘protective function’ is broad, but not so broad as to encompass the actions of private individuals. The term ‘function’ must be read in the light of its use elsewhere in Schedule 1 and the GDPR: ‘function’ refers not simply to any activity undertaken by an individual but ‘ a duty attached to a role or an office; an official duty’. If Mr. Driver’s role in publishing articles about potential or suspected wrongdoing were within the scope of ‘protective function’ there would be no need for a separate condition pertaining to journalism.
65. Further it is unclear how Mr. Driver’s activity is intended to ‘protect’ members of the public from future acts of dishonesty. The disclosure is concerned with promoting accountability for past actions. To the extent that future actions might be prevented, disclosure is not ‘necessary’.

Paragraph 12 – regulatory requirements relating to unlawful acts and dishonesty etc.

66. Mr. Driver does not show why disclosure is necessary in order for the Council itself to undertake an investigation of any alleged wrongdoing.

Paragraph 13 – Journalism etc. in connection with unlawful acts and dishonesty

67. There is no obligation on the Council to hold a belief that confirming or denying whether the requested criminal offence data is held, would be in the public interest as required under para 13(1)(e).

Article 10 ECHR

68. It is clear from the decision of the Supreme Court in *Kennedy v Charity Commission* [2015] AC 455 that article 10 does not confer a right to access to state-held information. Whatever the merits of the approach in *Maygar Helsinki Bizottsag v Hungary* [2016] ECHR 975, the lower courts are bound to follow the Supreme Court's decision until such time as the Supreme Court reconsiders its position.

Evidence

69. We took account of an open and a closed bundle, plus a small number of additional closed documents.

Gist of closed session

70. As this is a 'neither confirm nor deny' appeal, very little of the closed session can be revealed without defeating the point of the appeal. The gist provided to Mr. Driver was as follows:

“The Commissioner made further submissions in closed concerning the Commissioner's investigation of the complaint and the Councils consideration of its obligations under DPA 2018 and the GDPR.”

Legal framework

Personal data

71. At the relevant time the GDPR, rather than the UK GDPR, was in force.

72. The relevant parts of s 40 of FOIA (in force at the relevant time) provide:

(5B) The duty to confirm or deny does not arise in relation to other information if or to the extent that any of the following applies -

(a) giving a member of the public the confirmation or denial that would have to be given to comply with section 1(1)(a)-

(i) would (apart from this Act) contravene any of the data protection principles, ...

...

(7) In this section -

“*the data protection principles*” means the principles set out in—

(a) Article 5(1) of the GDPR, and

(b) section 34(1) of the Data Protection Act 2018;

“*data subject*” has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act);

“*the GDPR*”, “*personal data*”, “*processing*” and references to a provision of Chapter 2 of Part 2 of the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act (see section 3(2), (4), (10), (11) and (14) of that Act).

(8) In determining for the purposes of this section whether the lawfulness principle in Article 5(1)(a) of the GDPR would be contravened by the disclosure of information, Article

6(1) of the GDPR (lawfulness) is to be read as if the second sub-paragraph (disapplying the legitimate interests gateway in relation to public authorities) were omitted.

73. Processing includes 'disclosure by transmission, dissemination or otherwise making available' (section 3(4)(d) DPA).

74. Section 40(5B) relates to an absolute exemption (section 40(3A)(a)) and the public interest balance accordingly does not apply.

75. Personal data is defined in s 3 of the Data Protection Act 2018 (DPA):

(2) 'Personal data' means any information relating to an identified or identifiable living individual (subject to subsection (14)(c)).

(3) '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.

76. The definition of "personal data" consists of two limbs:

i) Whether the data in question "relate to" a living individual and

ii) Whether the individual is identified or identifiable, directly or indirectly, from those data.

77. The data protection principles are set out Article 5(1) GDPR. The first principle provides that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. Article 6(1) UK GDPR provides that processing shall be lawful only if and to the extent that at least one of the lawful bases for processing listed in the Article applies.

78. The most relevant basis here is article 6(1)(f):

Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which requires protection of personal data, in particular where the data subject is a child.

79. The case law on article 6(1)(f)'s predecessor established that it required three questions to be answered, which we consider are still appropriate if reworded as follows:

79.1. Is the data controller or a third party pursuing a legitimate interest or interests?

79.2. Is the processing involved necessary for the purposes of those interests?

79.3. Are the above interests overridden by the interests or fundamental rights and freedoms of the data subject?

80. Lady Hale said the following in *South Lanarkshire Council v Scottish Information Commissioner* [2013] 1 WLR 2421 about article 6(f)'s slightly differently worded predecessor:

27. ... It is well established in community law that, at least in the context of justification rather than derogation, 'necessary' means 'reasonably' rather than absolutely or strictly necessary The proposition advanced by Advocate General Póitares Maduro in *Huber* is uncontroversial: necessity is well established in community law as part of the proportionality test. A measure which interferes with a right protected by community law must be the least restrictive for the achievement of a legitimate aim. Indeed, in ordinary language we would understand that a measure would not be necessary if the legitimate aim could be achieved by something less. ...

81. Article 10 GDPR provides:

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

82. Section 11(2) DPA provides:

In Article 10 of the GDPR and section 10, references to personal data relating to criminal convictions and offences or related security measures include personal data relating to –
(a) the alleged commission of offences by the data subject, or
(b) proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

83. Section 10(5) DPA provides:

10 Special categories of personal data and criminal convictions etc data

(1) Subsections (2) and (3) make provision about the processing of personal data described in Article 9(1) of the GDPR (prohibition on processing of special categories of personal data) in reliance on an exception in one of the following points of Article 9(2) –

- (a) point (b) (employment, social security and social protection);
- (b) point (g) (substantial public interest);
- (c) point (h) (health and social care);
- (d) point (i) (public health);
- (e) point (j) (archiving, research and statistics).

(2) The processing meets the requirement in point (b), (h), (i) or (j) of Article 9(2) of the GDPR for authorisation by, or a basis in, the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1 of Schedule 1.

(3) The processing meets the requirement in point (g) of Article 9(2) of the GDPR for a basis in the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 2 of Schedule 1.

(4) Subsection (5) makes provision about the processing of personal data relating to criminal convictions and offences or related security measures that is not carried out under the control of official authority.

(5) The processing meets the requirement in Article 10 of the GDPR for authorisation by the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1, 2 or 3 of Schedule 1.

84. Schedule 1, Part 3, Paragraph 36 DPA provides:

Extension of conditions in Part 2 of this Schedule referring to substantial public interest

This condition is met if the processing would meet a condition in Part 2 of this Schedule but for an express requirement for the processing to be necessary for reasons of substantial public interest.

85. Schedule 1, Part 2, Paragraph 10 DPA provides:

10. Preventing or detecting unlawful acts

(1) This condition is met if the processing –

(a) is necessary for the purposes of the prevention or detection of an unlawful act,

(b) must be carried out without the consent of the data subject so as not to prejudice those purposes, and

...

(2) If the processing consists of the disclosure of personal data to a competent authority, or is carried out in preparation for such disclosure, (underlining mine) the condition in subparagraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place (see paragraph 5 of this Schedule).

86. Schedule 1, Part 2, Paragraph 11 DPA provides:

Protecting the public against dishonesty etc

(1) This condition is met if the processing –

(a) is necessary for the exercise of a protective function,

(b) must be carried out without the consent of the data subject so as not to prejudice the exercise of that function, and

...

(2) In this paragraph, “protective function” means a function which is intended to protect members of the public against –

(a) dishonesty, malpractice or other seriously improper conduct,

(b) unfitness or incompetence,

(c) mismanagement in the administration of a body or association, or

(d) failures in services provided by a body or association.

87. Schedule 1, Part 2, Paragraph 12 DPA provides:

Regulatory requirements relating to unlawful acts and dishonesty etc

(1) This condition is met if –

(a) the processing is necessary for the purposes of complying with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has –

(i) committed an unlawful act, or

(ii) been involved in dishonesty, malpractice or other seriously improper conduct,

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing, and

...

(2) In this paragraph “act” includes a failure to act; “regulatory requirement” means –

(a) a requirement imposed by legislation or by a person in exercise of a function conferred by legislation, or

(b) a requirement forming part of generally accepted principles of good practice relating to a type of body or an activity.

88. Schedule 1, Part 2, Paragraph 13 DPA provides:

Journalism etc in connection with unlawful acts and dishonesty etc

(1) This condition is met if –

(a) the processing consists of the disclosure of personal data for the special purposes,

(b) it is carried out in connection with a matter described in subparagraph (2),

(c) ...

(d) it is carried out with a view to the publication of the personal data by any person, and

(e) the controller reasonably believes that publication of the personal data would be in the public interest.

(2) The matters mentioned in sub-paragraph (1)(b) are any of the following (whether alleged or established) –

(a) the commission of an unlawful act by a person;

(b) dishonesty, malpractice or other seriously improper conduct of a person;

(c) unfitness or incompetence of a person; d) mismanagement in the administration of a body or association;

(e) a failure in services provided by a body or association.

...

(4) In this paragraph-

...

“the special purposes” means-

(a) the purposes of journalism;

...

89. Article 10 of the European Convention on Human Rights provides:

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

90. In *Maygar Helsinki Bizottsag v Hungary* [GC] 18030/11 8 November 2016, the European Court of Human Rights recognised that Article 10(1) might, under certain conditions, include a right of access to information, including in circumstances where access to the information is instrumental for the individual's exercise of his or her right to freedom of expression, in particular "the freedom to receive and impart information" and where its denial constitutes an interference with that right.

91. Like the Upper Tribunal in **Moss v Information Commissioner and the Cabinet Office** [2020] UKUT 242 (AAC) ('**Moss**') (at paragraph 59) we consider ourselves bound by the rules of precedent to follow the view of five members of the Supreme Court in **Kennedy v Charity Commission (Secretary of State for Justice and others intervening)** [2014] UKSC 20, as well as the Court of Appeal in **Kennedy** and two if not three members of the Supreme Court in **BBC v Sugar** (No.2) [2012] UKSC 4 that domestic law does not consider Article 10(1) extends to include a right of access to information. We are also bound by the Upper Tribunal decision in **Moss**.

The role of the tribunal

92. The tribunal's remit is governed by s.58 FOIA. This requires the tribunal to consider whether the decision made by the Commissioner is in accordance with the law or, where the Commissioner's decision involved exercising discretion, whether he should have exercised it differently. The Tribunal may receive evidence that was not before the Commissioner and may make different findings of fact from the Commissioner.

Issues

93. Can the tribunal apply the case of **Maygar Helsinki Bizottsag v Hungary** [2016] ECHR 975, and, if so, what is the impact of the right to access information under article 10 ECHR?

94. Would confirming or denying that the requested information was held constitute the disclosure of a third party's personal data relating to criminal convictions and offences?

95. Would confirming or denying that the requested information was held meet the requirement in Article 10 of the GDPR for authorisation by the law in that it meets one of the following conditions in Part 2 of Schedule 1 DPA:

Schedule 1, Part 2, Paragraph 10: Preventing or detecting unlawful acts

95.1. Is confirmation or denial necessary for the purposes of the prevention or detection of an unlawful act?

95.2. Must confirmation or denial be carried out without the consent of the data subject so as not to prejudice those purposes?

Schedule 1, Part 2, Paragraph 11: Protecting the public against dishonesty etc

95.3. Is confirmation or denial necessary for the exercise of a function intended to protect members of the public against –

95.3.1. dishonesty, malpractice or other seriously improper conduct,

95.3.2. unfitness or incompetence,

95.3.3. mismanagement in the administration of a body or association, or

95.3.4. failures in services provided by a body or association?

95.4. Must confirmation or denial be carried out without the consent of the data subject so as not to prejudice the exercise of that function?

Schedule 1, Part 2, Paragraph 12: Regulatory requirements relating to unlawful acts and dishonesty etc

95.5. Is confirmation or denial necessary for the purposes of complying with, or assisting other persons to comply with a regulatory requirement i.e.

95.5.1. a requirement imposed by legislation or by a person in exercise of a function conferred by legislation, or

95.5.2. a requirement forming part of generally accepted principles of good practice relating to a type of body or an activity?

95.6. Does the regulatory requirement involve a person taking steps to establish whether another person has –

95.6.1. committed an unlawful act, or

95.6.2. been involved in dishonesty, malpractice or other seriously improper conduct?

95.7. In the circumstances, can the controller not reasonably be expected to obtain the consent of the data subject to confirmation or denial?

Schedule 1, Part 2, Paragraph 13: Journalism etc in connection with unlawful acts and dishonesty etc

- 95.8. Does confirmation or denial consist of the disclosure of personal data for the purposes of journalism?
- 95.9. Is it carried out in connection with the alleged or established:
- 95.9.1. commission of an unlawful act by a person;
 - 95.9.2. dishonesty, malpractice or other seriously improper conduct of a person;
 - 95.9.3. unfitness or incompetence of a person;
 - 95.9.4. mismanagement in the administration of a body or association;
 - 95.9.5. failure in services provided by a body or association?
- 95.10. Is it carried out with a view to the publication of the personal data by any person?
- 95.11. Does the controller reasonably believe that publication of the personal data would be in the public interest?
96. Is the appellant pursuing a legitimate interest or interests?
97. Is the confirmation or denial necessary for the purposes of those interests?
98. Are the legitimate interests overridden by the interests or fundamental rights and freedoms of the data subject?
99. Would confirming or denying that the requested information was held be fair?

Oral submissions

100. The parties primarily reiterated the points made in the pleadings and written submissions.

Article 6(1)(f)

101. In relation to article 6(1)(f) Mr. Driver argued that his legitimate interest lay in the fact that as a local journalist he wished to publish an article which, if the data is held, would reveal misconduct and unlawful activity by a senior politician, in an area of powerful national and local interest, with environmental and health consequences, where that politician has spoken out against such unlawful activities and voted in favour of introducing stricter legislation. Confirmation or denial is necessary and proportionate because, if the information exists, the only organisation who holds it is the Council.
102. Mr. Driver accepts that the Councillor would face quite serious reputational damage, might lose their political position, and could be caused some fairly serious harm and distress. Mr. Driver submits that harm and distress cannot be relied upon where it is a foreseeable consequence of one's own actions by the commission of a criminal offence or other misconduct.

103. Mr. Metcalfe did not make oral submissions on article 6(1)(f) on the basis that it was not necessary to do so, in keeping with the Decision Notice.

The conditions in Schedule 1, Part 2 DPA

104. The parties agreed that the requirement to demonstrate substantial public interest is disapplied for criminal offence data.

Prevention and detection of unlawful acts

105. Mr. Driver argued that if the Council were to confirm or deny that it held the data, this would be an act of detection because confirmation would reveal or expose an unlawful act. Whilst action may have been taken by the Council it has not been made public. Detecting and exposing unlawful acts plays an important role in the future prevention of unlawful acts, acting as a deterrent and leading to greater scrutiny and review of processes which aim to reduce and prevent similar acts in the future.
106. Mr. Metcalfe submitted that confirmation or denial is not necessary to prevent or detect an unlawful act. If the information is held, then any offence in question has already been detected and cannot be prevented. The fact that disclosure might have a deterrent effect does not mean confirmation or denial is *necessary* to prevent a future unlawful act. It has not been shown that confirmation or denial must be carried out without the consent of the data subject so as not to prejudice the purposes of detecting or preventing an unlawful act.

Protection of the public against dishonesty

107. Mr. Driver argues that individuals, and not just the state, can and do regularly act to protect other people from dishonesty and improper conduct. An individual has the right to make a citizen's arrest. Journalists are recognised as acting as a 'public watchdog' protecting the public from a wide variety of harms including dishonesty and misconduct.
108. Restricting the public protection role to the state is too narrow an interpretation of paragraph 11. This would mean that an area of the state that was corrupt and wished to cover up dishonesty or wrongdoing would not be able to be challenged by private individuals or the media. The references to the use of 'function' in other parts of the legislation are tenuous - if paragraph 11 had been intended to exclude the private citizen it would have said so.
109. Mr. Driver argues that disclosure of a past event will play a role in preventing future similar events.
110. Mr. Metcalfe argues that the definition of 'public function' is not so broad as to encompass the actions of private individuals, and that it has to be read in the

light of how the term is used elsewhere in Schedule 1 and the GDPR. It is an official function conferred, not necessarily by statute, on a public body for the protection of the public. If there is any issue about the conduct of the Council it can be brought to the Ombudsman and confirmation or denial is not necessary to pursue that complaint.

Paragraph 12 - regulatory requirements

111. Mr. Driver argues that it has been suggested to him that the data, if held, is in effect being 'covered up' and has not, as it should have been, referred to the standards committee to take the appropriate action. There is only one way to ensure that this is dealt with and that is by way of confirming or denying that the information is held.
112. Mr. Metcalfe submits that it is simply not necessary to confirm or deny in order for the Council to undertake an investigation. There is no situation in which confirming or denying assists the Council or any external body to undertake an investigation.

Paragraph 13 - journalism

113. Mr Metcalfe submits that the requirement that the Council reasonably holds the belief that publication of the personal data would be in the public interest is fatal to Mr. Driver's appeal, because there is no indication that the Council holds any such belief.
114. Mr. Metcalfe argues that this requirement reflects the particular unusual and specific treatment given to criminal offence data in UK law, giving the authority processing the data the right to determine for itself by reference to its own reasonable belief that the publication of the personal data would be in the public interest. In the event of a body deliberately covering up wrongdoing, this requirement would not prevent the investigative functions of external supervisory bodies, giving other avenues for people who wish to challenge a body's refusal to disclose.
115. Mr. Driver submitted that the reasonable belief of the authority could be challenged. In not processing the information the authority is not taking a reasonable position and has not taken account of all the public interest factors highlighted by Mr. Driver.

Discussion and conclusions

Article 10 of the European Convention on Human Rights

116. In the light of the binding authority set out under 'Legal Framework' above, Mr. Driver's arguments based on article 10 and **Maygar** do not assist him. Domestic

law does not consider Article 10(1) extends to include a right of access to information.

Would confirming or denying that the requested information was held constitute the disclosure of a third party's personal data relating to criminal convictions and offences?

117. It is accepted that the requested information, if held, would be personal data relating to criminal convictions and offences. Given the terms of the request, including the fact that the Councillor is named in the request, if the authority were to confirm that the requested information was held this would disclose a third party's personal data relating to criminal convictions and offences.

Would confirming or denying that the requested information was held meet the requirement in Article 10 of the GDPR for authorisation by the law in that it meets one of the conditions in Part 2 of Schedule 1 DPA?

118. Mr. Driver does not assert that the conditions of consent (paragraph 29) or data in the public domain (paragraph 32) are present. There is no evidence before us that could support a conclusion that either of those conditions is satisfied.

119. It was agreed between the parties that there are no requirements of substantial public interest where the data is criminal offence data, as a result of paragraph 36 of Schedule 1 DPA.

Schedule 1, Part 2, Paragraph 10: Preventing or detecting unlawful acts

120. We conclude that confirmation or denial is not necessary for the purposes of the prevention or detection of an unlawful act. First, we accept that if the authority holds the information, the unlawful act in question has already been 'detected'. We do not accept that the making public of either that act or of any action that was taken as a result of that act forms part of the detection of that unlawful act. This is wider than the natural meaning of 'detection of an unlawful act'.

121. The use of the singular – 'prevention or detection of an unlawful act' rather than 'prevention or detection of unlawful acts' – suggests to us that the section refers to a particular unlawful act, rather than unlawful acts in general. This interpretation is supported by the requirement, in paragraph 10(1)(b), that the processing 'must be carried out with the consent of the data subject so as to not prejudice those purposes'. That paragraph makes sense if a particular unlawful act is being prevented or detected. If that is so, Mr. Driver's submissions about the general deterrent effect in relation to future acts would not fall under paragraph 10.

122. In any event, although we accept that the making public of such an act might act as a deterrent for future similar acts, or might lead to other changes that might reduce the risk of similar acts taking place in the future, we do not accept that

this means that confirmation or denial is reasonably necessary for the prevention of future unlawful acts.

123. Further, we do not accept that it has been shown that confirmation or denial must be carried out without the consent of the data subject *in order* not to prejudice the purposes of prevention or detection of an unlawful act.
124. For those reasons paragraph 10 does not apply.

Schedule 1, Part 2, Paragraph 11: Protecting the public against dishonesty etc.

125. We are not persuaded that Mr Driver is exercising 'a function' intended to protect members of the public against dishonesty etc. We accept Mr. Metcalfe's submission that, in this context, the use of the word 'function' entails some duty attached to a role or an office or an official duty. In our view it is intended to refer to bodies exercising a protective function that has been conferred on them, by statute or otherwise. This is supported by other uses of the word 'function' within the DPA.
126. Although we accept that Mr. Driver's purpose as journalist is, at least in part, to protect members of the public against dishonesty, we do not accept that he is exercising such a 'function'. In our view, this is an artificially wide interpretation of that word. We do not accept that the IPSO editor's code confers on Mr. Driver, as a journalist, a protective function.
127. In addition, we do not accept that it has been shown that confirmation or denial must be carried out without the consent of the data subject *in order* not to prejudice the exercising of that function.
128. For those reasons paragraph 11 does not apply.

Schedule 1, Part 2, Paragraph 12: Regulatory requirements relating to unlawful acts and dishonesty etc

129. Even assuming that the Council holds this information and is engaging in a 'cover up', we do not accept that confirmation or denial is reasonably necessary for the purposes of assisting the Council to comply with a regulatory requirement.
130. We accept that there may be a relevant 'regulatory requirement' imposed on the Council or its standards committee, but we do not accept that it is reasonably necessary for the Council to confirm or deny to the world whether it holds this information in order to assist itself or its standards committee, or in order for Mr. Driver to assist it or its standards committee, to comply with that requirement. Even assuming Mr. Driver is correct in asserting that there has been a cover up and that the Council is reluctant to act, we do not accept that

confirmation or denial would assist the Council to comply with a regulatory requirement. The Council or its standards committee could take action without public confirmation or denial. If Mr. Driver's 'tip off' suggests that the Council has improperly failed to take action, this could be referred to, for example, the Ombudsman.

131. For those reasons paragraph 12 does not apply.

Schedule 1, Part 2, Paragraph 13: Journalism etc in connection with unlawful acts and dishonesty etc

132. We accept that confirmation or denial consists of the disclosure of personal data for the purposes of journalism, and that it is carried out in connection with the alleged commission of any unlawful act by a person (and other matters falling within paragraph 13(2) and with a view to the publication of the personal data.

133. One of the requirements of paragraph 13 is that the controller reasonably believes that publication of the personal data is in the public interest. This necessarily contains two elements: (i) that the Council believes that publication is in the public interest and (ii) that that belief is reasonable.

134. There is no evidence or even any indication before us upon which we could infer or base a conclusion that the Council believes that publication of the personal data, if it exists, is in the public interest. The condition cannot be satisfied without that belief.

135. Mr. Driver asks us to consider whether or not it would be reasonable for the Council to conclude that it is not in the public interest to publish. That is not the question that we are required to answer.

136. Although it appears unsatisfactory that a public body has the right to determine for itself, by reference to its own reasonable belief, that the publication of personal data would or would not be in the public interest, we accept that this arises from the peculiar treatment of criminal offence data. Further we accept Mr. Metcalfe's point that a body deliberately covering up wrongdoing is not left immune to challenge. The data protection regime would not prevent or hinder the investigative functions of external supervisory bodies, giving other avenues for people who wish to challenge a body's refusal to disclose.

137. For that reason, paragraph 13 does not apply.

Conclusions

138. As none of the conditions in the Schedule are satisfied, confirmation or denial would breach the first data protection principle and section 40(5B) applies. We do not need to go on to consider article 6(1)(f). This was the conclusion reached

by the Commissioner, albeit that he did not consider the same conditions, and for those reasons we agree that he reached the right conclusion.

139. A closed annex has been provided. In the annex we deal with a particular issue raised by the Commissioner in closed which ultimately has had no bearing on our decision, but was, for reasons explained in the closed annex, appropriate to record. We are unable to provide a gist of the closed annex without revealing whether or not the information is held by the Council and therefore defeating the purpose of the proceedings.

Signed Sophie Buckley

Date: 22 February 2023

Judge of the First-tier Tribunal