



NCN: [2023] UKFTT 00480 (GRC)

Case Reference: EA/2022/0284

**First-tier Tribunal
General Regulatory Chamber
Information Rights**

Determined on the papers on 24 May 2023

Decision given on: 08 June 2023

Before

**TRIBUNAL JUDGE CL GOODMAN
TRIBUNAL MEMBER MR D PALMER-DUNK
TRIBUNAL MEMBER MS M SAUNDERS**

Between

DES MOORE

Appellant

and

(1) THE INFORMATION COMMISSIONER

Respondent

Decision:

The appeal is dismissed.

Decision Notice IC-131247-S9L9 is in accordance with the law.

REASONS

Background and Request

1. The National Fraud Intelligence Bureau (“NFIB”) is a police unit responsible for gathering and analysing intelligence about fraud in the United Kingdom. It analyses information from a variety of sources and where appropriate, “disseminates” intelligence reports to regional police forces for further investigation. The public can report fraud to the NFIB using Action Fraud, the national fraud reporting service. A person reporting fraud to Action Fraud will receive progress reports and be notified if their report is passed to a regional force.
2. On 26 June 2021, the Appellant made a request under the Freedom of Information Act 2000 (“FOIA”) to West Midlands Police (“WMP”) as follows:

“Request 1

For each month in the financial years 2019/20 and 2020/21, please provide the number of reports of fraud passed to you from the National Fraud Intelligence Bureau (NFIB) to investigate.

Request 2

Please provide the number of individuals charged with offences in connection with the reports identified in Request 1”.

3. WMP responded that providing the requested information would exceed the appropriate cost limit under section 12 FOIA, but voluntarily provided the information requested under Request 1. The number of reports varied each month from the lowest, 42, in December 2019 to the highest, 406, in April 2019. There were 102 reports in May 2019.
4. The Appellant narrowed Request 2 to:

“the number of individuals charged with offences in connection with the reports identified in Request 1 for the month of May 2019 only”.
5. WMP confirmed that it held some relevant information but withheld it in reliance on section 31(1)(a) and (b) FOIA (law enforcement) and section 40 (personal data). The decision was not changed on internal review, with WMP adding that there was a greater likelihood of revealing force investigative capability or vulnerability, and of identifying a specific individual, if the numbers charged in May 2019 were either very high or very low.

Decision Notice

6. The Appellant complained to the Information Commissioner.
7. On 22 September 2022, the Commissioner issued Decision Notice IC-131247-S9L9. The Commissioner decided that WMP was entitled to rely on section 40 FOIA to refuse to provide the information requested in Request 2. No further steps were required.
8. The Commissioner concluded that:
 - a. the withheld information was personal data because a “motivated intruder” would be able to identify the individuals to whom it related from a combination of the withheld information and other information “likely to be in, or come into, the possession of others, such as those with knowledge of the fraudulent activity” [paragraph 37];
 - b. the withheld information was also “criminal offence data” as defined in Article 10 UK General Data Protection Regulation (“UK GDPR”);
 - c. disclosure of the withheld information would be unlawful because none of the conditions in Schedule 1, Parts 1 to 3, Data Protection Act 2018 (“DPA”) were met, and would therefore breach the first data protection principle under Article 5(1)(a) UK GDPR;

- d. the withheld information was therefore exempt from disclosure under section 40(2) FOIA.
9. As the Commissioner found that the withheld information was exempt under section 40(2) FOIA, it did not go on to consider section 31 FOIA.

The Appeal

10. The Appellant appealed to the Tribunal.
11. The Appellant submitted with reference to the case of *NHS Business Services Authority v Information Commissioner and Spivak* [2021] UKUT 192, that the Commissioner had not explained how an individual could be identified from the withheld information. WMP was the second largest police force in the UK, policing almost 3 million people. Other forces, which received far fewer calls for service and disseminations from the NFIB had provided the equivalent information, even where there had been only one charge in a month.
12. In its Response, the Commissioner relied on the Decision Notice. It set out the relevant law, including the *Spivak* case, and suggested that a “motivated intruder” in this case might be an investigative journalist or a victim of fraud. Such a motivated intruder might obtain other information from individuals with knowledge of the fraudulent activity which, when combined with the withheld information, could enable them to identify the individuals charged with offences in May 2019 in connection with a NFIB report.

Determination on the papers

13. All parties consented to this matter being dealt with on the papers and the Tribunal decided that it was fair and in the interests of justice to do so.
14. In reaching its decision, the Tribunal took into account all the evidence and submissions before it. The Tribunal had before it an open bundle of 81 pages, including information received by the Appellant from other police forces in response to Request 1 and 2. We had a small closed bundle, consisting of an unredacted copy of WMP’s response to the Commissioner dated 5 August 2022 which contained the withheld information
15. The Tribunal considered whether to adjourn in order to obtain more information from WMP. We noted that the overriding objective in Rule 2 of the Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 includes dealing with cases in a way which is proportionate, avoids unnecessary formality and seeks flexibility, uses the special expertise of the Tribunal effectively, and avoids delay so far as compatible with proper consideration of the issues. We decided, that on balance we had sufficient information and expertise to make a fair and just decision on the appeal.

The Law

Freedom of Information Act 2000

16. Section 1(1) FOIA gives individuals a right to information from a public authority unless it is “exempt information”.
17. Section 40 FOIA provides:
...
(2) Any information to which a request for information relates is... exempt information if—
 - (a) it constitutes personal data... and
 - (b) the first, second or third condition below is satisfied.

(3A) The first condition is that the disclosure of the information to a member of the public otherwise than under this Act—

(a) would 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 UK GDPR, and

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

18. Section 40(2) FOIA is an absolute exemption in relation to the first condition in section 40(3A). This means that the public interest balancing test under section 2(2)(b) FOIA does not apply.

UK GDPR and Data Protection Act 2018

19. The first data protection principle under Article 5(1)(a) UK GDPR is that personal data shall be:

“processed lawfully, fairly and in a transparent manner in relation to the data subject”

20. Processing is lawful under Article 6(1) UK GDPR only if one of the relevant lawful bases apply, in particular:

“(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data...”

21. Article 10 UK GDPR provides (in so far as relevant) that processing of personal data relating to criminal convictions and offences based on Article 6(1):

“shall be carried out only under the control of official authority or when the processing is authorised by domestic law providing for appropriate safeguards for the rights and freedoms of data subjects...”

22. Section 11(2) DPA provides:

“(2) In Article 10 GDPR and section 10, references to personal data relating to criminal convictions and offences... 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.”

23. Section 10(4) DPA provides that section 10(5) makes provision for processing relating to criminal convictions and offences not carried out under the control of official authority. Section 10 (5) provides that:

“(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.”

What is personal data?

24. Section 40(7) FOIA provides that “personal data” has the same meaning as in Section 3 DPA, namely:

“(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.”

25. The General Data Protection Regulation (EU) 2016/679 addresses identifiability in Recital 26 as follows:

“The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.”

26. In *NHS Business Services Authority v Information Commissioner and Spivak* [2021] UKUT 192, Upper Tribunal Judge Jacob considered whether a patient could be identified from a list of dispensaries which had dispensed a particular medication. Having considered the relevant authorities in relation to the application of section 3 DPA and Recital 26 in these circumstances, Judge Jacob described the issue before him as:

“whether any person was identifiable from the [withheld data] when taken together with other information by someone who was motivated to identify one or more of the persons within the data using all the means reasonably likely to be used.” [paragraph 3]

27. Judge Jacob identified that an “inquirer” in the circumstances of *Spivak* might be a researcher, lobbyist or journalist, someone wanting to market a relevant product to the individual, or a family member of a patient. In other cases, this has been described as a “motivated intruder” (for example, *Information Commissioner v Magherafelt District Council* [2013] AACR 14) or a “determined person with a particular reason to want to identify the individual... using the touchstone of, say, an investigative journalist...” (*Craigdale Housing Association v The Scottish Information Commissioner* [2010] CSH 43, at paragraph 24).

28. Judge Jacob proposed that the test for the Tribunal to apply was not a test of “remoteness or significance or likelihood” (paragraph 21) but one of “whether it is possible to identify a specific individual solely by relying on the data available”. He went on:

“Identifying a pool that contains or may contain a person covered by the data is not sufficient. Saying that it is reasonably likely that someone is covered by the data is not

sufficient. Still less is it sufficient to say that it is reasonably likely that a particular individual may be one of the pool. Linking any specific individual to the data in any of these circumstances does not rely solely on the data disclosed and other data available by reasonable means; it involves speculation.” [paragraph 22]

29. If a break in the chain between the information and the data subject can be bridged only by speculating or guessing, Judge Jacob concluded that the data subject is not identifiable from the information. This situation was “especially likely to arise when there is a pool of potential subjects”.

Powers of Tribunal

30. The powers of the Tribunal in determining this appeal are set out in s.58 of FOIA, as follows:

“(1) If on an appeal under section 57 the Tribunal considers -

(a) that the notice against which the appeal is brought is not in accordance with the law, or

(b) to the extent that the notice involved an exercise of discretion by the Commissioner, that he ought to have exercised his discretion differently, the Tribunal shall allow the appeal or substitute such other notice as could have been served by the Commissioner, and in any other case the Tribunal shall dismiss the appeal.

(2) On such an appeal, the Tribunal may review any finding of fact on which the notice in question was based.”

31. The Tribunal stands in the shoes of the Commissioner and takes a fresh decision on the evidence before us. The Tribunal does not undertake a review of the way in which the Commissioner’s decision was made.

Discussion

32. The reasons for the Tribunal’s decision are set out in full below. There is no Closed Annex. Our findings were made on the balance of probabilities. The Tribunal applied the law as set out in paragraphs 16 to 31 above.
33. The Appellant did not dispute that the withheld information related to criminal offences nor that none of the conditions in Parts 1, 2 or 3, Schedule 1 DPA applied.
34. The main issue for the Tribunal was whether the withheld information was “personal data”. The Tribunal applied the law as set out in paragraphs 24 to 29 above. In particular, we applied the guidance of Upper Tribunal Judge Jacob in *Spivack* and asked ourselves whether any individual would be identifiable from the withheld information “when taken together with other information by someone who was motivated to identify one or more of the persons within the data using all the means reasonably likely to be used”. We noted that the test was whether it was possible to identify a specific individual solely through the available data, without guesswork or speculation.
35. We accepted the Commissioner’s submission that a possible “inquirer” might be a journalist investigating a particular fraud or offender, or WMP’s response to fraud or charging rates more generally. The inquirer might also be a victim of fraud, someone who had made an Action Fraud report, or someone accused of or involved in fraudulent activity, who wanted to identify the person charged with a particular offence. Alternatively, the inquirer might be someone who knew an individual charged with an offence in May 2019 who wanted to identify the type of offence, and whether the charge was the result of a NFIB report.

36. The Tribunal found that the means reasonably likely to be used by a motivated inquirer would include:
- a. data and statistics published by organisations such as NFIB, Action Fraud and WMP, and available through FOIA requests, about reporting and investigation of fraud, charging and outcomes, broken down, for example, by date, year and type of fraud;
 - b. information available publicly about NFIB and WMP policy and practice on referring, investigating and charging fraud offences;
 - c. information published by WMP or the media about offences charged in May 2019;
 - d. information about charges in May 2019 available from the relevant Court;
 - e. personal knowledge of fraud reported to NFIB and from progress reporting to victims by NFIB and WMP; and
 - f. personal knowledge of individuals charged with fraud offences by WMP in May 2019.
37. The Tribunal took into account that WMP is the second largest police force in the UK, policing almost 3 million people. However, we also accepted that the ease with which a motivated inquirer could identify an individual from the withheld data would depend upon the number of individuals charged. The smaller the number, the easier the task.
38. The Tribunal noted that other police forces had provided information in response to Request 2, even when there was only one charge in a month. This was not the issue before the Tribunal and we did not know why other forces had taken this approach. Public organisations are entitled to disclose information voluntarily beyond that which is required under FOIA, if they wish.
39. The Tribunal did not accept, as suggested by the Commissioner, that the Appellant had selected May 2019 because he had a particular interest in that month. There was insufficient evidence to support this, and the Tribunal noted that the Appellant had only narrowed Request 2 at WMP's suggestion and that he had made the same request of multiple police forces.
40. The Tribunal concluded, taking into account all the evidence before us which included the withheld information in the closed bundle, that a motivated inquirer of the type identified above would be able to identify an individual from the withheld information, when that information was taken together with the considerable other information available about NFIB reports and WMP charges as identified in paragraph 36. An investigative journalist could combine the withheld information with information from sources, including victims of fraud and contacts of offenders, and from other public reports and FOIA requests, to identify those individuals charged in May 2019 in connection with a NFIB report. A victim of fraud or acquaintance of an offender would have personal knowledge about an offence and the relevant police investigation to combine with the withheld information.
41. We found therefore that the withheld information relates to an identifiable individual, and as a result, is "personal data" as defined in section 3 DPA.
42. The withheld information relates to criminal offences (section 11(2) DPA) and disclosure would not meet the requirement in Article 10 UK GDPR because no condition in Part 1, 2 or 3 of Schedule 1, DPA, is met. Disclosure would not be lawful under Article 6(1) UK GDPR and would therefore contravene the first data protection principle in Article 5(1)(a). The first condition in section 40(3A) FOIA is satisfied and the withheld information is exempt information under section 40(2). The duty to disclose in section 1(1)(b) FOIA does not apply and WMP were entitled to withhold the requested information.

43. The Decision Notice is in accordance with the law and the appeal is dismissed.

Signed Judge CL Goodman

Date: 08/06/2023