Neutral Citation Number: [2021] EWCA Civ 42

Case No: C1/2019/2622 & C1/2019/2623

IN THE COURT OF APPEAL (CIVIL DIVISION)
ON APPEAL FROM THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
ADMINISTRATIVE COURT
The Honourable Mrs Justice Lieven DBE
[2019] EWHC 975 (Admin)

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 19/01/2021

Before:

LORD JUSTICE BEAN

LADY JUSTICE ASPLIN DBE
and
LADY JUSTICE ANDREWS DBE

- -

Between :

THE QUEEN (on the application of M)	**Appellant**
- and -	
THE CHIEF CONSTABLE OF SUSSEX POLICE	**Respondent**
-and-	
BRIGHTON & HOVE BUSINESS CRIME REDUCTION PARTNERSHIP	**Interested Party**

- -
- -

Eric Metcalfe (instructed by **Matthew Gold & Co Ltd**) for the **Appellant**
Elliot Gold and **Aaron Rathmell** (instructed by **Weightmans LLP**) for the **Respondent**
Hearing date: 17 December 2020

- -

Approved Judgment

Lady Justice Andrews:

Introduction

1. The Appellant was the claimant in these proceedings. At the time of Lieven J's judgment she was 16 years old and brought the claim by a litigation friend. She is an extremely vulnerable young person, who had gone missing from home on numerous occasions and was excluded from school. She has convictions for shoplifting and assault, and since 31 October 2017 she had been reported to the police for over 50 incidents of violence, theft, or anti-social behaviour, mostly if not all in the Respondent's area. Before this appeal could be heard, she turned 18; the first issue that we had to consider was whether, in those circumstances, the anonymity order made under CPR 39.2 and renewed by Nicola Davies LJ when she granted permission to appeal on 9 March 2020, should continue.

2. It became clear that, but for the Covid-19 pandemic, this appeal would have been heard some months before the Appellant's 18th birthday. Irrespective of other justifications which might exist for maintaining the order, the Court felt that she should not be disadvantaged by the impact of such unprecedented events on the timing of the hearing. Accordingly, as previously ordered, she shall continue to be known as "M" and no person shall identify her or any member of her family in any report of these proceedings.

3. However, we refused an application made at the hearing by Mr Metcalfe, on behalf of M, to extend the existing prohibition by precluding any identification of the town in which the relevant events took place or of the Interested Party, on the basis that this would "almost inevitably" lead to M's identification. We were not satisfied that it would, and in any event, we considered such additional interference with the principle of open justice to be unwarranted; the order that has been made is proportionate and suffices to protect M's legitimate countervailing interests.

4. The claim for judicial review fell into two parts. The first was a challenge to the lawfulness of the Respondent's safeguards for disclosing sensitive personal data to the Brighton & Hove Business Crime Reduction Partnership ("the BCRP") under an Information Sharing Agreement made in December 2018 ("ISA 2018"). The BCRP was joined as an Interested Party. It has taken no part in the proceedings, but the Respondent has relied upon evidence provided by its Business Crime Reduction Manager, Ms Lisa Perretta.

5. The Respondent is the public authority responsible for crime and disorder strategies in Sussex pursuant to section 5(1)(b) of the Crime and Disorder Act 1998. By section 6(1)(a) of that Act, she must "formulate and implement a strategy for the reduction of crime and disorder in the area (including anti-social and other behaviour adversely affecting the local environment)". To that end, it is important for the police to be able to engage in meaningful dialogue and share information with local businesses with a view to safeguarding against the risks of criminal and anti-social behaviour.

6. The BCRP is an organisation with more than 500 members, including local businesses, national and independent retailers, private security firms, public houses, bars and nightclubs. The structure and operation of the BCRP, and the provisions of documents produced by the BCRP which are relevant to the issue of data sharing, are

described in detail at paragraphs 13 – 18 of Lieven J's judgment. Its principal function is the management of an exclusion notice scheme, prohibiting persons from entering its members' commercial premises. The decision whether to exclude an individual is made by the BCRP Management Committee (also referred to as the Executive Committee). M was made subject to such an exclusion order on 7 November 2017 for a period of 12 months.

7. The Respondent may decide to share data relating to an individual with the BCRP for law enforcement purposes. As explained by Superintendent De La Rue in his witness statement, the purpose of the police sharing information with the BCRP is to inform the BCRP Management Committee of issues concerning particular individuals, in order for it to take a decision on whether they should be excluded. The Respondent does not share data directly with any BCRP member. If it decides to share data with the BCRP, that data can only be accessed by certain BCRP employees, all of whom have achieved level 2 non-police personnel vetting ("NPV"). This is addressed in section 4 of the ISA 2018, to which I shall refer later in this judgment.

8. Paragraph 4.10 of the BCRP Code of Practice provides that:

> "police will only disclose information to the local Partnership where there is a clear legal basis to do so and under the terms of the agreed Information Sharing Agreement. Information provided under partnership arrangements by police is for the prevention and detection of crime and prosecution of offenders and must not be used for any other purpose."

9. The police are not the only source of data that the BCRP may receive about an individual. Any member of the BCRP may provide information to the Management Committee, which may include, for example, CCTV footage; that information is not shared with other members. All requests for information, sharing of information and denied requests will be recorded. The information is required to be kept on a secure server within a secure location with a control access system, to which the general public has no access.

10. It is the BCRP Management Committee which usually decides what information to share with its members according to its own Data Sharing Policy. Once the information it has received about an individual reaches a certain threshold set for exclusion, the BCRP may decide to disclose specific data to its members to make them aware of any threat to their premises, and to ensure that the exclusion is effective. Any such onward disclosure is made via a secure intranet site and a secure mobile application. However, a decision to share with members the personal data of a person aged 14-17 must be taken by the Board of Management, consisting of a minimum of three persons, of whom at least one must be the BCRP chair or crime manager.

11. Not all BCRP members require access to the intranet. At the time of the hearing below, the number of members who were granted such access was 239 – under half the membership. Access to the shared data will be restricted to those members whose premises are likely to be affected by the exclusion order. Prior to consent to access being given, the member requesting it must sign a data integrity agreement (described in paragraph 18 of Lieven J's judgment) which forbids the sharing of information with any third party. Anyone who has not logged on to the intranet for more than six

weeks is removed, and every six months all members are "locked out" of the intranet and required to re-certify their adherence to the data integrity agreement to regain access to it.

12. The ISA 2018 was the latest in a series of information sharing agreements made between the Respondent and the BCRP from 2013 onwards, with a view to ensuring compliance with the relevant data protection regimes. Indeed, the claim for judicial review started life as a challenge to the lawfulness of its immediate predecessor, which was entered into in 2017. That challenge became academic when that agreement was superseded, and permission was granted to amend the claim. The challenge to the earlier version of the ISA was maintained, but (understandably) the arguments are dealt with briefly in the judgment below, and played very little part in this appeal.

13. Lieven J's decision is one of the first concerning the requirements of Part 3 of the Data Protection Act 2018 ("DPA 2018"). Among other matters, it involved consideration of (1) the scope and nature of the obligations under two of the six data protection principles set out in sections 34-40 of the DPA 2018, which give effect to Article 4(1) of the Law Enforcement Directive, Directive 2016/680 ("LED"), and (2) the additional safeguards required for the processing of "sensitive data" for law enforcement purposes under section 42 of the DPA 2018.

14. The main question for the High Court was whether the ISA 2018 met the requirements of Part 3 of the DPA 2018. In a well-structured, careful and clearly expressed judgment, Lieven J held that although there was room for improvement, on a holistic assessment, the ISA 2018 read together with its appendices (particularly Appendix 4) and a Legitimate Interest Assessment ("LIA") which was an appendix to that appendix, did provide sufficient safeguards and effective measures, including technological measures, to meet those requirements.

15. Mr Metcalfe submitted that the Judge was wrong to reach that conclusion. His chief complaint was that the ISA 2018 is not an appropriate policy document for the purposes of processing *sensitive* personal data relating to children and young persons under the age of 18. Mr Metcalfe was at great pains to stress that no objection was taken to the sharing of such data with the BCRP or the purposes for which it was shared, but rather that the focus of concern was the alleged inadequacy of the safeguards in place to avoid, among other undesirable consequences, its wider dissemination.

16. The second part of the claim was a discrete complaint about the unlawfulness of specific past disclosures of M's personal data, including sensitive personal data, allegedly made by the Respondent to the BCRP. The relevant disclosures were made prior to 25 May 2018, when the DPA 2018 came into force, and therefore the governing statute was the Data Protection Act 1998 ("DPA 1998"). The operative ISA was the 2017 version.

17. Section 2 of the DPA 1998 defined "sensitive personal data" as including "personal data consisting of information as to:

> (f) [the data subject's] sexual life;

(g) the commission or alleged commission by him of any offence; or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings."

18. Because this second claim was brought within the ambit of proceedings for judicial review, rather than as a private law claim, the Judge was faced with considerable difficulty in resolving contentious factual allegations; in particular, a strongly disputed allegation that the police had disclosed to the BCRP that M was considered by them to be vulnerable to child sexual exploitation ("CSE").

19. Lieven J made justifiable criticisms of the Respondent for non-compliance with the duty of candour, late disclosure of relevant material, and failure to disclose other obviously relevant material, including the actual record of disclosures made by the Police to the BCRP in respect of M on certain specific occasions. She also said (in my view with less justification) that the position remained unclear as to the terms of Operation C, a police operation of which M was one of the subjects, and the degree to which it was specifically targeted around young people who were at risk of CSE.

20. Ultimately, the Judge relied on two emails dated 3 October 2017 and 29 January 2018 which she decided, when put together, made it plain that the Respondent did give the BCRP information about M being vulnerable and at risk of sexual exploitation. She found that in this specific regard there had been a breach of M's rights under the DPA 1998, and (following a quantum hearing) awarded her £500 damages. However, she dismissed all the other complaints of past unlawful data sharing. Among other matters, she found that the (admitted) sharing of M's bail conditions with the BCRP under the ISA 2017 did not amount to sharing with "the public" in breach of section 49 of the Children and Young Persons Act 1933 ("the 1933 Act") and section 45(1) of the Youth Justice and Criminal Evidence Act 1999 ("the 1999 Act").

21. M appeals against that finding and against the quantum of the award of damages for the breaches that were established; with the permission of Dingemans LJ, the Respondent cross-appeals both against the Judge's finding that disclosure to the BCRP that there was intelligence that the Claimant was at risk of CSE amounted to the disclosure of sensitive personal information about M's sexual life contrary to the DPA 1998, and against the finding at paragraph 113 of the judgment that disclosure of M's falling within Operation C communicated to the BCRP that she was at risk of CSE or otherwise communicated anything in respect of her sexual life. The first issue on the cross-appeal obviously has wider implications and, as Mr Gold on behalf of the Respondent submitted, is a matter of considerable importance to the police.

22. Before turning to consider the relevant legal principles and the arguments, I should record our gratitude to both counsel for their efforts to illuminate this complex area of the law and to assist the Court to navigate a way through what the Judge rightly described as the "labyrinthine" statutory provisions.

Ground 1: Did the ISA 2018 meet the requirements of Part 3 of the DPA 2018?

1.1 The treatment of children's data under the GDPR and LED

23. The general processing of personal data is regulated by the General Data Protection Regulations ("GDPR") (Regulation (EU) 2016/679) whose terms are incorporated in Part 2 of the DPA 2018. The GDPR goes beyond the terms of its predecessor, Directive 95/46/EC, which sought to harmonise the protection of fundamental rights and freedoms of natural persons in respect of data processing activities, and to ensure the free flow of personal data between Member States. Among other matters, it aims to ensure a consistent level of protection for natural persons throughout the EU and to provide legal certainty and transparency for economic operators.

24. The GDPR specifically recognises the position of children and their vulnerability to misuse of data, particularly data that is posted online, in its recitals, including recitals 38, 58, 65 and 76. It acknowledges that children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned, and of their rights in relation to the processing of such data. For example, recital 38 refers to a need for specific protection to apply to the use of personal data of children for marketing purposes, or for creating personality or user profiles. The special risks and concerns identified in the GDPR relating to children and young persons are reflected in the Code of Practice issued by the Information Commissioner's Office relating to the design and development of online services likely to be accessed by a child, which came into force on 2 September 2020.

25. Article 6(i)(f) of the GDPR expressly provides that processing of personal data for a legitimate interest may be overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. That is an operative provision which creates substantive rights.

26. Although the LED was issued on the same date as the GDPR, there is no equivalent provision in the LED/Part 3 of the DPA 2018. The LED is solely concerned with the processing of personal data by competent authorities for specified law enforcement purposes, which include the prevention, detection or prosecution of criminal offences. By contrast with the GDPR, it contains no Articles specifically pertaining to children and young persons, vulnerable persons, or data relating to them; but this is understandable, as the concerns that arise about the uses to which their personal data may be put are largely different from those articulated in the GDPR and its recitals. Children are mentioned in some of the recitals to the LED as exemplars of "vulnerable persons," but they are not treated as falling into some separate special category or expressly afforded elevated protection.

27. Recital 37 to the LED provides that:

> "personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection, as the context of their processing could create significant risks to the fundamental rights and freedoms."
>
> It gives as an example of this, data revealing racial or ethnic origin. It goes on to state that appropriate safeguards for the rights and freedoms of the data subject [in respect of such data] could include:
>
> "The possibility to collect those data only in connection with other data on the natural person concerned, the possibility to secure the data collected adequately, stricter rules

on the access of staff of the competent authority to the data, and the prohibition of transmission of those data."

28. Recital 39 requires any information given to the data subject to be easily accessible and easy to understand, using clear and plain language. It states that "such information should be adapted to the needs of vulnerable persons such as children".

29. Recital 50 states that:

"The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and should be able to demonstrate that processing activities are in compliance with this Directive. Such measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons. The measures taken by the controller should include drawing up and implementing specific safeguards in respect of the treatment of personal data of vulnerable natural persons, such as children".

30. Recital 51 states, inter alia, that:

"The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation… where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs or trade union membership; where genetic data or biometric data are processed in order to uniquely identify a person or where data concerning health or data concerning sex life and sexual orientation or criminal convictions and offences or related security measures are processed…where personal data of vulnerable natural persons, in particular children are processed; or where processing involves a large amount of personal data and affects a large number of data subjects."

31. Recital 52 makes it clear that the likelihood and severity of any such risk to individual rights and freedoms should be evaluated objectively and by reference to the nature, scope, context and purposes of the processing.

32. Recital 53 specifically addresses the requirement that appropriate technical and organisational measures are taken to ensure that the requirements of the LED are met and specifies that, in order to be able to demonstrate compliance, the data controller should adopt internal policies and implement measures which adhere in particular to the principles of data protection by design and data protection by default.

1.2 The obligations of the Respondent

33. In this section, all references are to provisions of the DPA 2018 unless otherwise specified.

34. Section 3(2) defines "personal data" as data that relates to an identified or identifiable living individual. A data controller is a person who alone or jointly with others determines the purposes and means of the processing of the data. "Processing" is defined by section 3(4) as any operation performed on personal data, including its collection, recording, organisation, structuring, storage, retrieval, use, disclosure by transmission, dissemination and making available. Different controllers may be involved at different stages of data processing, to different degrees, and with different levels of responsibility. These concepts and definitions apply irrespective of whether the relevant data protection regime is the GDPR/Part 2 of the DPA 2018 or the LED/Part 3.

35. The processing of data for law enforcement purposes (including the prevention, investigation, detection or prosecution of criminal offences) by "competent authorities" (as defined by section 30 and schedule 7), which expression includes the Respondent, is regulated by Part 3 of the DPA 2018. However, the BCRP is not a "competent authority" and Part 3 does not apply to it. Any obligations it may have as a data controller in its own right are governed solely by the GDPR/Part 2 of the DPA 2018.

36. In Part 3, a data processor is defined as someone who processes data on a controller's behalf, other than an employee of the controller – i.e. an agent (section 32(3)). A controller may only use a processor who provides guarantees to implement technical and organisational measures that will meet the requirements of the DPA 2018 and protect the data subject's rights (section 59(2)). Processing must be governed by a written contract (section 59(5)). There are no similar requirements regarding the relationship between two or more data controllers (see section 56).

37. Section 35(8) defines the processing of certain types of personal data for law enforcement purposes as "sensitive processing". The types of personal data falling within that section are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data, and data concerning health or a person's sex life or sexual orientation.

38. Some, but not all, of these expressions are further defined. For example, "data concerning health" is defined in section 205(1) as "personal data relating to the physical or mental health of an individual, including the provision of health care services, which reveals information about his or her health status". Biometric data is defined as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images or dactyloscopic data." Not all photographs fall within that definition, but they may if they are used to create a digital profile, for example for facial recognition purposes. However, the expression "sex life" is not further defined.

39. These provisions reflect Article 10 of the LED and the particular risks to personal rights and freedoms identified in recitals 37 and 51.

40. Although the statute does not use the expression "sensitive personal data" it is a useful shorthand for describing data falling within the special categories referred to in section 35(8). Elsewhere in the DPA 2018, specifically in section 10 and Schedule 1, reference is made to "special categories of personal data" (describing the subject-

matter of Art 9(1) of the GDPR). Despite the overlap with "special category" data, "sensitive personal data" and "sensitive processing" are concepts which are confined to Part 3.

41. The challenge to the lawfulness of the ISA 2018 was made on the basis that the Respondent is a "data controller" and that to the extent the Respondent shared M's data with the BCRP, the BCRP was a "data processor" as defined by section 32. The importance of that characterisation lay in the fact that a data controller is legally responsible for the actions of a data processor, subject to certain statutory defences. The Judge was not wholly convinced by that analysis, considering that the much more natural reading of the situation was that once the information was passed on to it, the BCRP became a data controller in its own right, or that the Respondent and the BCRP became joint controllers of the data. However, she said that the Respondent was undoubtedly the data controller at the point that the information was passed on to the BCRP, and as such, the obligations under Part 3 of the DPA 2018 apply to her.

42. Although the ISA 2018 describes the BCRP and the Respondent as joint data controllers, and the Judge stated that this appeared to be correct, Mr Gold explained that the BCRP could not be a joint controller of the data for the purposes of Part 3 of the DPA 2018 because, as noted above, the BCRP is not a "competent authority". As data controllers, the two entities would be operating under two separate regimes, even if their control of the data was simultaneous rather than sequential. The ISA 2018 expressly recognises this.

43. Subject to that correction, I agree with the Judge that any onward processing of the data by its dissemination to BCRP members once a decision to exclude has been taken, is more naturally to be viewed as the act of a data controller, rather than that of an agent processing that data on behalf of the police. That analysis might affect questions of liability for breaches of the Data Protection Act 2018 that may arise in future. However, for reasons that it is unnecessary to address in this judgment, in this case nothing turned on the question whether the Respondent remained the controller of the data once it was passed to the BCRP.

44. It is important to keep in mind that there is a distinction between the obligations that arise under the GDPR/Part 2 of the DPA 2018 and those that arise under the LED/Part 3 of the DPA 2018, although there is a significant overlap between the two regimes. To give two examples of key differences, first, under the GDPR, data must be processed lawfully, fairly and transparently, but where data is processed for law enforcement purposes there is no requirement of transparency. Secondly, the rights of a data controller to process data for a law enforcement purpose cannot be overridden, provided that the relevant statutory tests are met, whereas, as mentioned in paragraph 25 above, the right to process data for a "legitimate interest" under the GDPR may be overridden by the personal rights and freedoms of the data subject, particularly if he or she is a child.

45. Section 34(3) provides that:

> "The controller in relation to personal data is responsible for, and must be able to demonstrate, compliance with this Chapter."

46. Section 56(1) requires the data controller to:

"Implement appropriate technical and organisational measures to ensure, and to be able to demonstrate, that the processing of personal data complies with the requirements of [Part 3 of the DPA 2018]."

47. Each regime has six data protection principles, which are broadly similar, but are couched in slightly different terms. The complaints of non-compliance in this case centre around the first and sixth data protection principles for the processing of personal data for law enforcement purposes. The first of these principles is addressed in section 35 which provides, so far as is material that:

"(1) … the processing of personal data for any of the law enforcement purposes must be lawful and fair.

(2) The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law and

(a) the data subject has given consent to the processing for that purpose, or

(b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority.

(3) In addition, where the processing for any of the law enforcement purposes is sensitive processing, the processing is permitted only in the two cases set out in subsections (4) and (5).

(4) The first case is where –

(a) the data subject has given consent to the processing for the law enforcement purpose as mentioned in subsection 2(a), and

(b) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

(5) The second case is where—

(a) the processing is strictly necessary for the law enforcement purpose,

(b) the processing meets at least one of the conditions in Schedule 8, and

(c) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42)."

48. The conditions in Schedule 8 include the following:

"1. Statutory etc. purposes

This condition is met if the processing

a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and

b) is necessary for reasons of substantial public interest.

2. Administration of Justice

This condition is met if the processing is necessary for the administration of justice.

3. Protecting Individual's vital interests

This condition is met if the processing is necessary to protect the vital interests of the data subject or of another individual.

4. Safeguarding of children and of individuals at risk

This condition is met if

(1) (a) The processing is necessary for the purposes of –

(i) protecting an individual from neglect or physical, mental or emotional harm, or

(ii) protecting the physical, mental or emotional wellbeing of an individual

(b) The individual is –

(i) aged under 18, or

(ii) aged 18 or over and at risk.

(c) The processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2) and

(d) The processing is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph 1(c) are

(a) In the circumstances, consent to the processing cannot be given by the data subject;

(b) In the circumstances the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) The processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph 1(a)."

49. Section 42(2) defines an appropriate policy document as a document produced by a controller which:

"(a) explains the controller's procedures for securing compliance with the data protection principles (see section 34(1)) in connection with sensitive processing in reliance on the consent of the data subject or (as the case may be) in reliance on the condition in question.

(b) explains the controller's policies as regards the retention and erasure of personal data processed in reliance on the consent of the data subject or (as the case may be) in reliance on the condition in question, giving an indication of how long such personal data is likely to be retained."

The word "explains" is used here in the sense of informing the reader what the procedures and policies are. So far as the first requirement is concerned, the document should set out the steps taken by the controller to comply with each of the six principles in respect of the processing of sensitive personal data for law enforcement purposes. So far as the second requirement is concerned, the document should state what the controller's policies are concerning the retention and erasure of sensitive personal data, including how long such data is likely to be kept.

50. The LED contains no requirement for an appropriate policy document; that requirement was introduced by the statute. However, the requirement creates a consistency of approach, because the GDPR/Part 2 of the DPA 2018 also contain requirements for such a document to be kept where "special categories" of personal data are processed for permissible purposes *other than* law enforcement purposes: Article 9(2) GDPR and DPA 2018 section 10 and Schedule 1. Such data cannot be processed on grounds of "legitimate interest" under Article 6 GDPR, so once again there is no question of the individual rights and freedoms of the data subject (particularly a child or young person) overriding the right to process the data once a permissible purpose is established.

51. The requirement for an "appropriate policy document" only arises under section 35 where the data to be processed is *sensitive* personal data. So far as the ISA 2018 was concerned, the only data pertaining to M shared with the BCRP that fell within the categories in section 35(8) was a photographic image of her which it was common ground constituted "biometric data".

52. Section 42(3) imposes three requirements on the *controller* that apply from the first processing of sensitive personal data until a period of six months from the cessation of the processing of such data, namely: to retain the appropriate policy document; to review and, if appropriate, update it from time to time; and to make it available to the Information Commissioner on request, without charge. Section 42(4) requires the *processor* of sensitive personal data to record "whether the sensitive processing is carried out in reliance on the consent of the data subject or, if not, which condition in Schedule 8 is relied on" and "how the processing satisfies section 35 (lawfulness of processing)".

53. The requirements of the sixth data protection principle under the LED/Part 3 of the DPA 2018 are essentially the same as those under the equivalent principle under the GDPR, which provides that:

"Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

The language of the sixth data protection principle under Part 3, set out in section 40, is the same, but appears in a slightly different order:

"personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage)."

54. That principle, which applies to all personal data, not just sensitive data, was considered by this Court in *CLG and others v Chief Constable of Merseyside Police* [2015] EWCA Civ 836, at a time when it was known as the seventh data protection principle (Schedule 2, para 7 of the Data Protection Act 1998). In that case, at [46] Moore-Bick LJ (with whom Fulford and Vos LJJ agreed) described the obligation as:

"a duty to put in place a system of measures to safeguard data that are appropriate having regard to the operations of the data controller and the nature of the data for which he is responsible. What is appropriate will vary from case to case."

55. Some further assistance in determining what is meant by "appropriate" is given by section 55(3), which states that appropriate technical and organisational measures must take into account the latest developments in technology, the cost of implementation, the nature, scope, context and purposes of processing, and the risks to individuals' rights and freedoms arising therefrom.

56. In *Various Claimants v WM Morrisons Supermarket Plc* [2017] EWHC 3113 (QB), Langstaff J observed at [67] that:

"… "appropriate" sets a minimum standard as to the security which is to be achieved. This is expressly subject to both the state of technological development and the cost of measures. Thus, the fact that a degree of security may technologically be achievable, which has not been implemented, does not of itself amount to failure to reach an appropriate standard … a balance has to be struck between the significance of the cost of preventative measures and the significance of the harm that might arise if they are not taken. This is itself intended to be a combination of the nature of the harm in itself and the importance of the data to be safeguarded from that harm".

The Court of Appeal in that case made some observations which are broadly consistent with that approach and are referred to in paragraph 60 of Lieven J's judgment, but I do not regard them as taking matters any further.

57. Lieven J set out verbatim the provisions of the DPA 2018 which lay down the relevant general obligations of controllers (and processors) under Part 3 with regard to data in paragraphs 62 to 64 of her judgment, and it is unnecessary to repeat that exercise here. I adopt her accurate summary in paragraph 80:

"[the Respondent] is required to implement the "appropriate technical and organisational measures" required under Part 3, including the requirement to demonstrate compliance (s.56); to implement the principles in an effective manner, and to integrate the safeguards necessary (s.57(1)); and to ensure that personal data is not made accessible to an indefinite number of people without an individual's intervention (s.57(5))."

58. Section 66(1) requires each controller and each processor to "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks arising from the processing of personal data." Specific requirements are set out in section 66(2) for measures relating to automated processing of data, but they are not relevant to the issues in this case.

1.3 Were those obligations satisfied by the Respondent?

59. As the Judge rightly recognised, the onus was on the Respondent to demonstrate compliance with the requirements of Part 3. In considering the compatibility of the ISA 2018 with those various requirements it is necessary to make two separate evaluations, namely:

    i) whether, to the extent that *sensitive* personal data was or might be shared with the BCRP, the ISA 2018 met the requirements for an "appropriate policy document" under section 42(2);

    ii) whether the system of "technical and organisational measures" implemented by the Respondent met the general requirements of "appropriateness" under Part 3. The general requirements apply to all personal data which is processed for law enforcement purposes, not just sensitive personal data; but the nature of the data would obviously be relevant when deciding whether the system afforded appropriate safeguards.

60. The technical and operational measures in question are not confined to the ISA 2018, although it is an important feature of them. The Respondent has a Privacy Notice and Fair Processing Notice, both of which are referred to in the ISA 2018 and were published on its website and accessible to members of the public at all material times. Its updated general appropriate policy document for law enforcement processing, based on the Information Commissioner's Office template, has been published on a different section of the website since 11 April 2019.

61. Other relevant documents include the BCRP's own Code of Practice and Privacy Notice, the BCRP's Constitution (which provides for control and review of BCRP functions generally, and data protection in particular) and the data integrity agreement to which BCRP members must subscribe in order to gain access to the intranet.

62. The Constitution contains an entire section, section 7, dealing with the position of "third party employees" (for example, where security services are outsourced by a participating business). It provides that third party staff who are employed/contracted by members, must have signed the same members' data and information disclosure declaration and data protection agreements as members. Disclosure of data to such third party employees must only be as provided by the DPA 2018 and only following assessment by the data controller (the Board of Management).

63. Under the BCRP Constitution, the decision as to the type of information that will be shared with participating members is made by the Executive (Management) Committee. One of the Respondent's Chief Inspectors sits on that Committee.

The ISA 2018

64. The ISA 2018 was created by the National Business Crime Centre in partnership with the Metropolitan Police Service Business Crime Hub and Information Sharing Support Unit. Its purpose is described as "an agreement to formalise Data Sharing Arrangements between Sussex Police and Sussex BCRP for the purpose of data sharing". It came into force on 18 December 2018. Prior to entering into the agreement, the parties were required to carry out a Data Protection Impact Assessment which:

    a) described the nature, scope, context and purposes of the processing;

    b) assessed necessity, proportionality and compliance measures;

    c) identified and assessed risks to individuals; and

    d) identified any additional measures to mitigate those risks.

65. Section 2 of the ISA 2018 defines the purposes for which the information is to be shared as "the prevention reduction and detection of crime and policing purposes within the area managed by [the BCRP]" and states that the agreement forms part of the strategy for the reduction of crime and disorder in the Respondent's area, as required by the Crime and Disorder Act 1998. It provides that information will be provided on a case-by-case basis, and only where considered necessary for the identified purpose. Information on the BCRP secure intranet site will only be accessible to members who have signed a data integrity agreement and who have read, and confirmed that they have read, the "must read" documents on that site.

66. Section 2.3 provides that personal data, special category data and criminal offence data (which expressions are defined in Appendix 1) will only be transmitted when deemed necessary in the immediate circumstances. When used by police, details of (a) what personal data is disclosed and (b) the reason for its disclosure will be recorded where possible on a secure system and retained for 6 months, and all police officers will be reminded of the Data Protection Principles in relation to transmission.

67. The introduction to section 3 of the ISA 2018 recognises the distinction between the regimes governing the processing of data by the Respondent (under Part 3 of the DPA 2018) and the processing of data by the BCRP (under the GDPR). The slightly different terms of each of the six data protection principles under the two regimes are set out in that section and, in respect of each principle, the agreement then addresses sequentially the legal obligations of "a competent authority" and "other bodies" and how those obligations are satisfied.

68. The Judge rightly pointed out in paragraph 30 of her judgment that section 3.1.6 refers to Article 6(f) of the GDPR, and that that appears to be the only specific reference to the position of children in the body of the ISA 2018 itself. However, she did not mention that this reference is specifically made in the context of explaining the lawful basis relied upon for sharing any personal data under the ISA (i.e. the first element of the first data protection principle). It appears under the heading "other bodies" (to whom the GDPR applies). The flow of information under the ISA 2018 is not all one way; the BCRP may provide information to the police, as well as to its members. For

the Respondent, however, the lawful basis for sharing the data with the BCRP emanates from Part 3 of the DPA 2018, under one or more of the law enforcement purposes, and not from Article 6 of the GDPR; and the "legitimate interest" test in the GDPR, which may be overridden by the personal rights and freedoms of a child, does not apply to her.

69. Section 3.1.3 is important. It makes it clear that the only images to be shared by the police are photographs taken when the individual has been detained at a police station for one of the offences listed in section 3.3; or images that have been captured on CCTV or Body Worn Camera footage, where the individual is suspected of having committed such an offence. Reference is made to the relevant provisions of the Police and Criminal Evidence Act 1984 and to the fact that when the image is taken, it is the policy and practice of the police force to inform individuals that the image may be used, disclosed or retained. There is also a reference to the privacy notice displayed on the police force website which makes it clear that personal information may be used by the police and shared with a variety of other agencies for the purposes of policing. This is to satisfy the "fair processing" requirements (of both regimes).

70. Section 3.1.8 specifically addresses the lawful basis for sharing "special category" or "sensitive" data. It provides the legal justification for sharing sensitive personal data in these terms:

"Section 6 of the Crime and Disorder Act 1998, the common law duties and core functions of the police, to prevent and detect crime and disorder provide the legal basis to share sensitive personal data to the extent that it is necessary for these purposes."

The section then accurately summarises the requirements of Part 3 of the DPA 2018, and specifically section 42(2) as they apply to the Respondent, and the requirements of Article 9(2) of the GDPR as they apply to other bodies (such as the BCRP in its capacity as a data controller). Whilst this paragraph makes no mention of children, young people or vulnerable persons, there is no reason why it should, as the operative provisions of the DPA 2018 and the two Directives do not require special category or sensitive data pertaining to such persons to be treated differently or given any form of heightened protection.

71. The requirement of necessity (the second aspect of the first data protection principle) is further considered under section 3.3, which specifically addresses the third data protection principle and contains the list of relevant types of offence. It states:

"Each image will be numbered and annotated with the name of the individual along with basic information about the type of offence committed and only other information deemed lawful and necessary will be included. No other information will be attached to the image, or supplied to [the BCRP].
…

Any personal data shared must be considered necessary for the identified purpose. Necessary means that if you can reasonably achieve the same purpose without sharing the data or all of the data, then you will not have a lawful basis. This means that data should only be shared with organisations to whom it is relevant and that the minimal amount of data should be shared for the purposes set out in this agreement".

72. Section 3.1.5. which specifically addresses the rights of individuals under Article 8 of the European Convention on Human Rights ("ECHR"), provides that:

> "the information to be supplied is proportionate for the needs of this agreement. The information is shared on a case-by-case basis, with only the minimum amount of information necessary, for the purposes of identifying and monitoring individuals within the [BCRP] area."

73. The sixth data protection principle is specifically addressed in Section 3.6, which accurately sets out the two versions under the different data protection regimes, and states that "measures to satisfy the Sixth Principle are detailed in Section 4 of this agreement".

74. Section 4, the salient parts of which are summarised in paragraph 31 of the judgment of Lieven J, is entitled "Description of arrangements including security matters". It describes how the relevant police team will extract the data and place it on a prepared information page, which will explain the information provided and the reason it is relevant; it will then be passed by secure email to the BCRP Manager or their authorised representative or uploaded directly onto the secure intranet site. It explains that the BCRP Manager or representative cannot extract the data unless they have been vetted to NPV 2 standard.

75. Although it acknowledges that all security officers employed at member venues will have licences from the Security Industry Authority and will have completed a DBS check, and that some of them may also be vetted to NPV 2 standard, section 4 goes on to state that the person (at the BCRP) disclosing the information *must give additional consideration and justify why it is necessary to share the information with someone who is not vetted*, based on the circumstances of the particular case. It also stipulates that the BCRP Manager must *ensure that information shared with members is the bare minimum to achieve the purpose and must give due consideration to the fact that members themselves may not be vetted to the same level, if at all*. (All emphasis added). The technical controls in the agreement are also stated to mitigate some of this risk.

76. The section goes on to state that information will not be shared to businesses outside of the secure intranet, which is accessed by password. Once accessed any further distribution and matters of security will be the responsibility of the person who has accessed the information, but it must be done in compliance with data protection law. The secure intranet site has met the police force standard of security and the requirements of the DPA 2018 and abides with guidance given by the Information Commissioner's Office. Correct use and disclosure of information is a condition of membership of the BCRP.

77. Section 4.6 describes in some detail how security incidents and breaches of the agreement must be reported and what action will be taken. Section 4.7 makes it clear that automatic time limits will be applied by the secure intranet database to photos and other intelligence held online, to ensure that information is not kept longer than necessary. The period for automatic deletion will either be specified by the uploader or applied by the scheme administrator, whichever is the shorter. The data must only be kept for as long as is necessary to achieve the purpose of sharing and will be determined on a case-by-case basis.

78. Section 4.8, another important section, provides that the BCRP Manager is responsible for ensuring that all agreed security agreements are complied with. All partners are responsible for ensuring the security controls are implemented and staff are aware of their responsibilities under data protection law.

79. Appendix 3 sets out the information that may be shared by the police with the BCRP. This includes, on the face of it, details of bail conditions relating to any known BCRP subjects. Bail conditions do not fall within the categories specified in section 35(8) of the DPA 2018 and are not subject to "sensitive processing", though they arguably fell within the definition of "sensitive data" under s.2 of the DPA 1998 referred to in paragraph 17 above. There is a bullet point in Appendix 3 which states that photographs can be exchanged *after* the BCRP relevant thresholds outlined in Appendix 4 have been met. They can only be displayed by the BCRP for up to a 12-week period unless further intelligence about criminal activity or anti-social behaviour by the individual concerned is submitted to the BCRP, or the individual is already subject to an exclusion notice.

80. The reference to Appendix 4 mentioned above is the only explicit cross-reference to that appendix. It is made in the specific context of sharing photographs/images which, by reason of the limitations on data that can be shared in respect of young people aged between 14-17 under the BCRP's own policy, referred to below, are the only relevant data pertaining to them that might constitute "sensitive data".

81. Appendix 4 to the ISA 2018 is the BCRP's "policy for processing personal data on children and minors on the basis of legitimate interest", which was adopted in May 2018. It specifically addresses the BCRP's position under the GDPR; that is unsurprising because to the extent that the BCRP is a data controller it is governed by the GDPR, not the LED. It is also unsurprising that the focus of the policy is on the situation in which the child's personal rights and freedoms might override any legal justification for the processing of the data, even though that situation does not arise where the data is "special category" (or "sensitive") as the case may be. This is because, as a data controller, the BCRP has an obligation to consider whether it should be processing data relating to children at all, and if so, what is its legal justification for doing so.

82. As Lieven J observed, much of Appendix 4 is concerned with the correct approach to be taken to the decision on whether children should be excluded from members' premises. However, there are aspects of it which deal with the decision whether data should be processed by the BCRP. Paragraph 12 states that the BCRP has set a minimum age of 14 for the processing of offender data. Importantly, Paragraph 13 states that the basis for the processing of children's data will be subject to a legitimate interest assessment, (to which it cross-refers, confusingly, as appendix 1) by a person with appropriate seniority to ensure that there is adequate consideration and accountability for the decision-making process.

83. The LIA, section J, identifies the nature of the data to be processed as "name, date of birth, photographic image, address, offences against BCRP members". Section T, entitled "Safeguards and compensating controls" provides that:

> "Until the threshold for exclusion is reached information will not be shared with members. Upon reaching the threshold, consideration will be given to whether

exclusion from all venues is required/appropriate. If not, information will only be shared with the relevant members. All members sign a binding data integrity agreement which prevents them from sharing information with third parties who are not Members of the BCRP. If the data integrity agreement is breached, procedures are in place to identify the guilty party and act accordingly."

That is plainly addressing the situation where a decision to exclude has been taken and the information is to be shared for the purpose of enforcing it. Those are the only circumstances in which the BCRP Management Committee (or, in the case of someone aged 14-17 the Board of Management) would authorise the data being made available to members via the secure intranet.

84. Paragraph 16(f) of Appendix 4 provides that the retention of data by the BCRP is limited to six months after the expiry of an exclusion notice for a person under the age of 18 and twelve months in the case of an adult.

The approach taken by the Judge

85. The first matter the Judge had to consider was whether the first and/or sixth data protection principles included a legal requirement to have "specific safeguards" in respect of the data (or sensitive data) of children. There is no such requirement in the body of the LED, nor in Part 3 of the DPA 2018, but Mr Metcalfe placed heavy reliance on the terms of Recital 50. He contended that section 57(1) of the DPA 2018, in particular, should be interpreted as requiring "specific safeguards" for children and young people, though he did not explain why that interpretation should not extend to all vulnerable persons, given that the recital in question only refers to children by way of an example of persons falling within that category.

86. Lieven J rejected that argument, although she took the recital into account as an aid to interpretation. Her approach, as reflected in paragraph 91 of her judgment, was to consider whether the safeguards in place through the ISA 2018 were sufficient to meet the terms of the 2018 Act, and in particular to do so where sensitive personal data was being shared and the interests of children were in issue. Thus she regarded the nature of the data, and the data subject, as material factors when considering whether the safeguards adopted were "appropriate".

87. I consider that approach to be correct. Recitals explain the reasons for the substantive provisions of the Directive which follow them, and they may shed light on how those provisions are to be understood. However, Recital 50 to the LED creates no substantive requirement as to the content of appropriate policy documents under sections 35(5) and 42(2), or the safeguards to be adopted in accordance with the sixth data protection principle. The text of the LED is accurately transposed into Part 3 of the DPA 2018, and it is not prescriptive about the measures that must be taken, so long as they are "appropriate". It does not attempt to micro-manage how a data controller complies with its requirements. Its recitals may be used as an aid to interpretation, but they cannot be treated as if they were operative provisions giving rise to substantive obligations, or be used to create such obligations in the guise of interpretation.

88. I can find nothing in *Elgizouli v Secretary of State for the Home Department* [2020] UKSC 10; [2020] 2 WLR 857 to support Mr Metcalfe's submission. In that case the

Supreme Court did not use the recitals to the LED to create substantive obligations that were not articulated in the body of the LED, but rather, relied upon them in an orthodox way as an aid to the interpretation of the relevant statutory provisions which implemented it.

89. The Judge approached the issue of deciding whether the safeguards adopted by the Respondent were sufficient to meet the statutory requirements and to protect M's rights by considering a number of factors, namely:

i) The nature of the data that can be shared under the agreement;

ii) The provisions as to who it can be shared with and control over any onward sharing;

iii) The requirements for the training and vetting of recipients of the data;

iv) The degree to which the specific interests of children are factored into the proportionality exercise; and

v) The reason or justification for the sharing.

She examined each of these factors in turn and then took a holistic view as to whether the safeguards she had identified were sufficient to meet the terms of the Act. She reached the conclusion that they were. That approach fully accorded with Sections 40 and 55 of the DPA 2018 and the objective evaluation envisaged in the Recitals to the LED.

90. Mr Metcalfe did not criticise that approach or take issue with any of the factors that the Judge regarded as relevant. Instead, he submitted that:

i) The Judge was wrong to accept that the only information that could be shared under the ISA 2018 in respect of a person aged 14-17 was the individual's name, date of birth, photographic image, address and offences against BCRP members;

ii) The LIA could not be relied on as an "appropriate policy document" (or part of an "appropriate policy document") because it was made explicitly for the purposes of the processing of data under Article 6(i)(f) of the GDPR and not for the purposes of processing sensitive data under Part 3 of the DPA 2018;

iii) The Judge did not address a lack of guidance or safeguards to prevent the 239 approved BCRP employees from sharing the data with "any number of their unvetted fellow employees";

iv) There was no factual basis for the Court's conclusion that Appendix 4 provided sufficient safeguards for the interests of children because it gave no guidance on what sharing was appropriate once a decision to exclude had been made.

Discussion

91. As to the first of these points, the Judge was entitled to make that finding on the evidence before her. This included evidence from Ms Perretta that the only information to be shared by the BCRP with its members once an individual reached the relevant threshold is "their image, name and date of birth together with the type of crime they are actively involved in". There was no reason why the Judge should not take the restrictions specified in the LIA at face value and treat them as circumscribing the various categories of information that the BCRP will process when the data subject is a young person aged 14-17. That is plainly what they were designed to do, even though the change from the 2017 ISA brought about by the restriction on the sharing of bail conditions might have been achieved in a less opaque manner.

92. Mr Metcalfe made the fair point that Appendix 4 and the LIA are not concerned with the passing of data by the police to the BCRP. Whilst that is true, those documents do limit the categories of data (from the police or other sources) that the BCRP would pass on to its members for the purposes of enforcement of an exclusion order made against a young person aged 14-17, and express consideration is given to when photographs might be disseminated. One might reasonably expect a senior police officer responsible for making the data available to the BCRP Management Committee to be conscious of those limitations, even though the documents could have spelled them out more clearly, and therefore to restrict the categories of data he or she supplied correspondingly. It is also pertinent that Section 3 of the ISA 2018 specifies that the data supplied should be limited to the minimum necessary for the law enforcement purpose.

93. In any event the Judge found that because of that opacity, the safeguard provided by limiting the categories of data that could be shared in respect of such young persons was unlikely to be very effective, if at all, *viewed in isolation*. She concluded at paragraph 96 that the safeguards in respect of what data could be shared were *not alone* sufficient to meet the requirements of the 2018 Act, but then correctly pointed out that it was necessary to consider all the various safeguards in a holistic manner. She was therefore alive to the deficiencies and practical risks arising from the fact that the category limitations were, as she put it, buried deep in the LIA, and took them into account in making her assessment.

94. Given that Appendix 4 is the BCRP's own policy, that this cross-refers to the LIA (and its requirements) in the context of data processing, that it has been specifically annexed to the ISA 2018 as a supplement to the Respondent's policy, and that no data relating to a person aged 14-17 can be shared with BCRP members without an express decision being taken by the Board of Management (comprising senior members who could be expected to be aware of those limitations), I consider that in practical terms the risk of other types of data, sensitive or otherwise, being shared with BCRP members is likely to be very small. The Judge also correctly identified that the only data on the list that could potentially fall within the ambit of "sensitive data" were the photographic images.

95. Mr Gold submitted that the two-stage process of information sharing is an important feature of the protection afforded to the data subject. Even if Appendix 4 read together with the LIA did not have the clear effect of restricting the information that

the police may share with the BCRP at stage 1, (which he submitted it did), that is not necessarily objectionable. There might well be a legal justification for the police to share other data about a young person with the BCRP Management Committee, for example, if there were safeguarding concerns. The more important restriction is on the dissemination of information to BCRP members, which is limited to certain types of data, is subject to both technical and non-technical controls and is on a "need to know" basis.

96. Mr Gold further submitted that there is no good reason why non-sensitive data should not be shared with BCRP members for law enforcement purposes if the tests of lawfulness and necessity are met and there are appropriate safeguards in place. The main focus of concern in this case was on the possibility of M's *sensitive* data (i.e. her photograph) being disseminated by BCRP members to their staff and employees (see paragraph 37 of the judgment of Lieven J) and therefore the theoretical danger that bail conditions, which are not sensitive data, might still be shared despite the changes brought about by the LIA, was an unnecessary distraction.

97. There is considerable force in those submissions, and it probably makes no difference to the overall analysis and conclusion if the restrictions in the LIA only applied to onward transmission of data between the BCRP and its members. However, as I have said, the findings made by the Judge were properly open to her and there are no grounds for disturbing them on appeal.

98. Mr Metcalfe's second submission, on which he placed considerable reliance, seems to me to be based upon a fundamental misconception. He contended that because Article 6(i)(f) of the GDPR deals solely with data processing for reasons of "legitimate interest", whereas the only reasons why special category data can be processed are dealt with in Article 9(2) of the GDPR, a policy document addressing the processing of non-sensitive data (as Appendix 4 and the LIA clearly do) cannot be relied on as, or as part of, an "appropriate policy document" in respect of processing of special category data under Article 9(2), let alone under the equivalent provisions of the LED/Section 3 of the DPA 2018 relating to sensitive data. The document was deficient because it made no reference to Article 9 nor to the processing of special category or sensitive data.

99. It seems to me that this submission favours form over substance. What matters for the purposes of demonstrating compliance with section 42(2) of the DPA 2018 is the *substance* of the policy document relied on, and whether in circumstances where the data to be processed is or might be characterised as "special category" or "sensitive" data (as the case may be), the document (a) explains the controller's procedures for securing compliance with the data protection principles in respect of such data, and (b) explains the controller's policies as regards the retention and erasure of such data. The key question, therefore, is whether the document relied on addresses the processing of data which are or may qualify as sensitive data, even if it addresses the processing of other data as well.

100. I cannot read Appendix 4 and the LIA in the restricted way advocated by Mr Metcalfe. His submission conflates the substantive legal justification relied on for processing data in the first place, with the procedures that the data controller is required to explain in the "appropriate policy document", i.e. steps which are designed to ensure that the processing of data complies with the requirements of Part

3 DPA 2018. If the document (including documents that are incorporated by reference or annexed to it) makes it clear what those procedures are, it does not matter if it does so in the context of addressing the processing of data generally or the processing of data for which there is or may be a different legal justification. The fallacy lies in the erroneous assumption that the processing of sensitive data must be addressed separately.

101. The controller has no obligation to maintain any policy document to explain how he complies with the same six data protection principles in connection with the processing of non-sensitive personal data for law enforcement purposes. Therefore, if Appendix 4 were treated as being restricted to non-sensitive data it would be surplus to requirements, and there would have been little point in including it as an appendix to the ISA 2018. Indeed, it would be a little odd if the ISA 2018 contained none of the compulsory information required in respect of sensitive data but had an appendix entirely devoted to matters that were not required by the statute at all and, on Mr Metcalfe's approach, had no direct relevance to processing even of non-sensitive data for law enforcement purposes.

102. In principle, there is no reason why the document on which a data controller relies as his appropriate policy document should not address the processing of <u>all</u> types of personal data, or why the controller's procedures for securing compliance with the requirements of the DPA 2018 should not be the same both for sensitive and non-sensitive data, so long as they meet the requisite minimum standard of "appropriateness". If a competent authority adopts general procedures which are of a standard appropriate to safeguard sensitive data, then they will necessarily also be of a standard appropriate to safeguard other data. The reverse may not always be true, but that will depend on an examination of the procedures in question.

103. Section 42 of the DPA 2018 merely requires the document to explain what those procedures are. The *adequacy* of those procedures is addressed under different provisions. There is no requirement that separate policies and procedures be followed for different types of data, or for the data controller to have a range of ISAs depending on the nature of the data to be shared.

104. There is the further complication that a photograph may or may not fall within the definition of "special category" data or "sensitive data" (depending on whether it is biometric data) and therefore in some circumstances Article 6 of the GDPR rather than Article 9(2) would apply to processing of that data by the BCRP and section 42(2) of the DPA 2018 would not apply to its processing by or on behalf of the Respondent. In those circumstances it makes sense to have one overarching policy and process to avoid debate about which of the two regimes should be applied.

105. We were shown a copy of the Information Commissioner's Office guidance and template for an "appropriate policy document" for Part 3 law enforcement processing. The guidance states:

> "If you conduct sensitive processing for a number of different LE purposes you do not need a separate policy document for each condition or processing activity – one document can cover them all. *You may reference policies and procedures which are relevant to all the identified processing.*" [Emphasis supplied].

Mr Gold pointed out that the definitions of the data to be shared in the ISA 2018 are narrower than those in the ICO's own appropriate policy document template.

106. The Judge was not obliged to disregard Appendix 4; it is not legally irrelevant. In my judgment she was right to conclude that the ISA 2018, read together with its appendices and the LIA, satisfies the requirements of section 42(2). Anyone reading those documents would know what, in practical terms, the Respondent's officers and the BCRP will do to make sure that they comply with the six data protection principles both generally and in the case of a data subject aged 14-17. Each of those principles is specifically addressed and discussed. They would have been told, among other matters:

i) All the types of data that the police might share with the BCRP under the ISA 2018;

ii) The purposes for which that information might be shared;

iii) How the decision to share the information would be taken and by whom;

iv) why the police would share with the BCRP an image of any data subject that would or might be classified as biometric data;

v) the circumstances in which the image would have been taken and what steps would have been taken to notify the data subject of the uses that might be made of it;

vi) the legal justification relied upon for sharing it;

vii) that the correct legal test for "necessity" would be applied when deciding whether to share it;

viii) who would have access to it and under what circumstances;

ix) what technical and other security measures had been put in place to safeguard against the risks of unlawful access or dissemination; and

x) how long it would be kept for, what records of its processing would be kept, and when it would be erased.

107. Almost all the information listed above appears in the body of the agreement, which also includes a section that addresses the treatment of sensitive data. Section 4 accurately sets out the legal test for allowing "sensitive processing". That test is the same irrespective of the age of the data subject. In the present case it seems to me that the police would easily be able to justify disclosure of a photographic image as "strictly necessary" for a law enforcement purpose and as falling under one or more of the categories in Schedule 8 of the DPA 2018 even if the circumstances in which that image was obtained (as described in section 3 of the ISA 2018) did not amount to consent by the data subject to their use. An exclusion scheme of the type operated by the BCRP in the public interest would patently be unworkable without an image enabling the excluded person to be identified.

108. Appendix 4 (and the LIA) contain *additional* information about the treatment by the BCRP of data pertaining to children and young persons. They indicate that (i) no data at all will be processed/shared with its members in respect of a child under 14 years; (ii) the only data that may be processed in respect of a young person aged 14-17 is limited to name, date of birth, image and the type of offence with which they are associated; and (iii) the BCRP will keep any data relating to a young person for half the time after expiry of an exclusion notice (six months) that they would if it related to an adult. The reference to processing clearly applies to processing after a decision to exclude has been taken (as well as to any processing before that decision is made).

109. Appendix 4 also makes it plain that exclusion is very much a last resort. The default position is for the young person not to be excluded but diverted to other options which, as Mr Gold pointed out, would result in their data not being shared with BCRP members at all, since it would only be shared after a decision had been taken by the Board of Management to make an exclusion order.

110. Appendix 4 contains considerations that are specifically directed at the GDPR requirements of lawfulness and necessity. Those same requirements and the same considerations arise under data protection principle 1 in Part 3 of the DPA 2018. There is express recognition that children are vulnerable and deserving of specific protection. Given that the balancing of individual rights and freedoms against the "legitimate interest" in processing the data affords an additional layer of protection to the data subject against the data being processed in the first place, which the DPA 2018 does not require if the data is "sensitive personal data" or "special category data", it cannot be a justified ground of complaint that the policy is framed in terms whereby sensitive data is also afforded that additional protection when the subject is a child or young person.

111. Mr Metcalfe's third point is based on an erroneous premise; the Judge plainly considered all the measures that were in place to safeguard against unlimited and unlawful dissemination by those with access to the intranet. She had described all the various measures taken by the BCRP to ensure that its members were fully aware of their data protection obligations before they accessed the information, earlier in her judgment. She addressed the adequacy of the safeguards against onward transmission in paragraphs 98-100. She described the BCRP Code of Conduct provision that access to staff is granted on a "need to know" basis as a "somewhat crude safeguard because of the very wide element of judgment involved", but after examining the training and vetting requirements for those staff who would receive the data (pointing out that the persons most likely to need to have the data would be the security staff responsible for enforcing the exclusion notice), the technical safeguards, and the sanctions for inappropriate onward transmission, she concluded that the safeguards were sufficient.

112. That was a conclusion she was entitled to reach, and there was ample evidence to support it. There was no need for any additional guidance to be given, as any member requiring access to the data would know what constraints were to be put on its dissemination and use by its employees or contractors, and they would be required to confirm that they agreed to the Data Integrity Agreement. Section 4 of the ISA 2018 is alive to the risks, and describes the measures taken to safeguard against them, which include, but are not limited to, the means of discovering who is responsible for any breaches and the sanctions available.

113. Although the Judge did not say so, I note that all four of the examples of the types of safeguard which might possibly be regarded as appropriate for sensitive personal data, referred to in Recital 37 to the LED, were present in this case. The Judge rightly recognised that the safeguards had to be proportionate to the legitimate objective of public protection to be served by passing the information on to those responsible for operating the exclusion order. No error of law or principle has been identified in her approach to deciding that they were proportionate, and thus appropriate, even for sensitive data pertaining to a young person aged 14-17.

114. As to the fourth and final criticism made by Mr Metcalfe, it appears to depend on his submission that there was a legal requirement to put in place specific safeguards in respect of the processing of sensitive data of children and young persons. There is no such requirement, but in any event Appendix 4 and the LIA do provide sufficient safeguards to address any specific concerns regarding the dissemination of M's photograph. Appendix 4 was not considered by the Judge in isolation, but as part of her holistic assessment of the variety of safeguards that the Respondent and the BCRP put in place. That was the correct approach. She rightly recognised that it addressed the relevant factors pertaining to children, even if the focus was upon deciding if those factors should weigh against processing the data at all. She identified that there is no specific consideration given in Appendix 4 itself to what sharing of data is appropriate once the decision to exclude has been made, but the LIA, to which the appendix cross-refers, does address that issue both in terms of limiting the categories of data that can be shared for any purpose and in section T, which can only apply once a decision to exclude has been taken.

115. The Judge was entitled, standing back, to take the view she did that so long as the nature of the data shared remains as in the LIA, and the safeguards she had identified exist as to onwards transmission, the sharing is proportionate, and the Respondent had demonstrated compliance with the requirements of the DPA 2018. For those reasons I would dismiss the appeal on Ground 1.

Ground 2: Was the ISA 2017 compatible with the requirements of the DPA 1998 and the DPA 2018?

116. It is possible to deal with this ground of appeal more shortly. Whilst he did not formally abandon it, Mr Metcalfe did not seek to press it if the Court was not persuaded by Ground 1. It is of historic interest only. The Judge set out the relevant provisions of the ISA 2017 at paragraphs 20-26 of her judgment. She then addressed the position in respect of that agreement in paragraph 105. Despite recognising its deficiencies, including the absence of clear processes by which the specific interests of children were considered, the Judge rightly found that the principal safeguards she had identified in the ISA 2018 were present in its predecessor, in particular the controls over what was shared and in what format, and over onward transmission. She concluded that those safeguards were sufficient to meet the requirements both of Part 3 of the DPA 2018 and the DPA 1998.

117. Once it is established that there is no specific legal requirement for the interests of children and young persons, or for sensitive personal data, to be addressed separately, it is demonstrated that the principal deficiencies complained of by Mr Metcalfe did not exist. There is no basis, therefore, for interfering with the Judge's conclusion on

this issue, which is backed by a proper evaluation of the relevant materials and sound reasoning.

118. In his written submissions on this ground, Mr Metcalfe contended that there was an inconsistency between the Judge's findings that the safeguards were appropriate and her findings on the second issue that "there was no evidence that [the Respondent] properly weighed up the impact on [M] of sharing [her risk of CSE] or whether there were sufficient safeguards to ensure against onward transmission [of that information]." However, the Judge's findings on the second issue were of a specific breach of the requirements of the DPA 1998; a breach can occur notwithstanding the existence of appropriate safeguards, because those safeguards are not absolute. They set a minimum standard, and sometimes they will fail to provide the protection they are designed to provide.

119. A finding of a failure by a data controller to consider whether the safeguards against onward transmission of certain data were sufficient, is not incompatible with a finding that the safeguards were generally appropriate. I would dismiss the appeal on Ground 2 also.

Ground 3: Was the sharing of bail conditions with BCRP members or their employees or contractors sharing with "members of the public"?

120. Section 49(1) of the 1933 Act concerns "restrictions on reports of proceedings in which children or young persons are concerned". It provides that:

> "No matter relating to any child or young person concerned in proceedings to which this section applies shall while he is under the age of 18 be included in any publication if it is likely to lead members of the public to identify him as someone concerned in the proceedings"
>
> A child or young person who is the defendant in proceedings before a youth court is "concerned in proceedings to which this section applies".
>
> "Publication" is defined in section 49(3) as including:
>
> "any speech, writing, relevant programme or other communication in whatever form, which is addressed to the public at large or any section of the public".

121. Section 45(3) of the 1999 Act confers a similar power on the court to direct that:

> "no matter relating to any person concerned in the proceedings shall while he is under the age of 18 be included in any publication if it is likely to lead members of the public to identify him as a person concerned in the proceedings."
>
> Such an order was made in the case of M following her arrest on a charge of assault in February 2018.

122. As the Judge found in paragraphs 50-52, following those events, M's solicitor became aware of the fact that the BCRP was sharing data relating to M, which included her bail conditions, with its members, via its mobile application. The local Council, whose Children's Services were involved with M, reported to the police and the BCRP its concerns about the fact that the bail conditions had been revealed and were

allegedly being posted on social media. The Respondent accepted that the police had informed the BCRP about M's bail conditions on three occasions, in February, March and April 2018, (all of which pre-dated the coming into force of the DPA 2018) but contended that this was lawful.

123. The Judge held that the sharing of that information was limited to BCRP members and that any employees or third party contractors of those members who received it did so in their employment (or contractual) capacity and subject to safeguards which limited its use to that within that capacity. They were not receiving it as a section of the public and the sharing was not "likely to lead members of the public to identify [her] as someone concerned in the proceedings". Therefore, the sharing of information was lawful. M challenges that analysis.

124. Mr Metcalfe contended that the references to "a section of the public" in the statutes are references to the general public, as opposed to persons acting in an official capacity, discharging public functions, such as the police. Since the BCRP is a private body, dissemination of information by the police to the BCRP and between the BCRP and its members constitutes a publication to a section of the public. He submitted that it was open to the Respondent to ask the court for an exception to be made to the order, if it were considered necessary to share the information for law enforcement purposes, and that the interpretation adopted by the Judge effectively gave the Respondent a discretion to make such a disclosure provided this was done securely and to those individuals who the Respondent was satisfied would not disclose it further. This would "drive a coach and horses" through the schemes of the 1933 and 1999 Acts and permit the Respondent rather than the courts to have the "last word" on when such information could be published.

125. Mr Metcalfe relied on the principle referred to by Lord Bingham CJ in *McKerry v Teesdale & Wear Valley Justices* [2000] EWCA Crim 3553 that "the privacy of a child or young person involved in legal proceedings must be carefully protected, and very great weight must be given to the welfare of such child or young person." He submitted that section 3 of the Human Rights Act 1998 required the Court to interpret the statutory provisions in a manner that was compatible with the child or young person's right to privacy.

126. I find it somewhat odd that this complaint is confined to the bail conditions, whereas if Mr Metcalfe's approach were the correct one, the sharing of M's name and any still or moving picture of her would also have been prohibited. Those are categories of information pertaining to the identity of the child or young person involved in legal proceedings which are specifically mentioned in the statutory provisions on which reliance is placed.

127. It would also be a curious state of affairs if the police were permitted to share certain data about a child or young person with the BCRP for law enforcement purposes under Part 3 of the Data Protection Act 2018 at any time when the data subject was not involved in legal proceedings, but unable to do so without the express permission of the court once that individual had been charged with a criminal offence.

128. The purpose of these provisions of the 1933 and 1999 Act is to protect children and young persons who are involved in the criminal justice system from being identified in reports in the media (including social media) of or about the criminal proceedings.

The case of *McKerry*, to which Mr Metcalfe referred, concerned an application by a newspaper to lift reporting restrictions relating to a 15-year-old defendant, and involved the balancing of the competing principles of open justice and the child's rights to privacy.

129. Whilst the definition of "publication" is a wide one, it is limited to publication to the public, or a section of the public. Mr Gold submitted that the disclosure of information for law enforcement purposes to the BCRP, its members and their employees or third party contractors (who are contractually bound to keep it confidential) is no different in kind from dissemination of that information to other private individuals who might have a legitimate interest in knowing it, such as staff in the Children's Services department of the local authority. He relied on various authorities on the meaning of "public" or "section of the public", in different statutes, including the case of *Dockers Labour Club v Race Relations Board* [1976] AC 285 referred to by the Judge, to demonstrate that those words will often connote a distinction between a group of private individuals, on the one hand, and the community at large or a section of the community, on the other. He submitted that it is not apposite to equate BCRP members and certain of their employees or contractors who receive information for defined purposes and subject to various safeguards, with members of the public or a section of the public who may read, watch or listen to publications or programmes of a kind which might be the target of reporting restrictions.

130. In my judgment, Lieven J's analysis was patently correct, for the reasons that she gave; members of the BCRP, their employees and third party contractors did not receive the information as members of the public, but in a private capacity, subject to contractual and other constraints limiting its use and precluding it from coming into public circulation. The correct dividing line is not between internal communications within public authorities, and all other communications; or between police officers or others carrying out a public function, and civilians; but between private communications and publications to the general public. The rights of the child or young person are already sufficiently taken into consideration when the decision is taken by the BCRP to disseminate the information to its members. I would therefore dismiss the appeal on this ground also.

The Cross-Appeal

131. Ground 4 of the appeal only arises in the event that the cross-appeal is unsuccessful, and therefore it makes sense to consider the cross-appeal next.

132. As noted above, there is no expanded definition of the expression "sex life" (or "sexual life", which is the expression used in the DPA 1998). However, the natural understanding of that expression is that it relates to someone's own sexual behaviour, preferences, and lifestyle choices in that area, not to the fact that they are or have been at risk of being sexually abused or exploited by others. It is also difficult to envisage why data about the existence of that type of risk would be regarded as deserving of special protection and requiring specific justification which might act as a fetter on its dissemination. Having said that, if it were to be regarded as sensitive information, the police would probably have little difficulty in relying on Schedule 8 to the DPA 2018 to justify sharing such information with, for example, appropriate safeguarding agencies, without the need to obtain the consent of the data subject.

133. Some assistance as to what the expression means is found in the recitals to the GDPR and LED, particularly recitals 71 and 75 to the former, and recital 51 to the latter, which refer to protecting the rights and freedoms of natural persons, particularly against discrimination and damage to reputation. The GDPR is particularly concerned with the unfair exploitation of personal data by commercial interests, and with discrimination.

134. The categories of "sensitive" personal data or "special category" data also mirror the protected grounds against discrimination under EU Directives 2004/43/EC and 2000/78 EC and the Equality Act 2010. Mr Gold also referred to recital 97 of the LED which expressly states that its provisions are without prejudice to rules on combating sexual abuse and sexual exploitation of children, referring to Directive 2011/93/EU. He submitted that this drew a material distinction between an individual's sexual life, on the one hand, and the risk of sexual abuse or exploitation, on the other.

135. Both the GDPR and the LED also refer to the protection of personal data in the context of the right to respect for private and family life under Article 8 ECHR, which includes a right to establish and develop relationships with others: see e.g. *Niemietz v Germany* (1993) 16 EHRR 97 at [29] and *Von Hannover v Germany* (2005) EHRR 1 at [50]. In that context, sexual orientation and sexual life have been described as "important elements of the sphere protected by article 8… [which] protects a right to identity and personal development and the right to establish and develop relationships with other human beings and the outside world" (see *PG v United Kingdom* (2008) 46 EHRR 51 at [56].

136. All these matters are essentially concerned with personal autonomy in terms of sexual identity, lifestyle choices and behaviour. The fact that someone is at risk of being sexually abused or exploited could be viewed as the diametric opposite of what was intended to be protected under this heading. The behaviour which led to someone taking the view that the risk exists may be a different matter.

137. Mr Metcalfe submitted that "sex life" encompassed information about being at risk of sexual harm in the same way as information about being at risk of contracting a particular disease would be information about someone's health. I did not find that a persuasive analogy, even if he were right that information about a risk to future health is sensitive information, (a matter which we do not need to decide).

138. I also consider that there is a great deal of force in Mr Gold's contention that to treat an individual's perceived risk of being the victim of sexual crime, as opposed to any other crime, as "sensitive" data with all the attendant requirements of Part 3 of the DPA 2018 (or the equivalent requirements under s.9(2) GDPR) would have a chilling effect on the willingness by charities, voluntary groups and other organisations to keep a record of and share information with the police which is critical to promoting safeguarding of vulnerable persons, for fear of being subject to data protection litigation.

139. For all those reasons I consider that the Judge was wrong to find that informing the BCRP that there was intelligence that M was at risk of CSE was disclosure of her "sexual life" and thus unlawful disclosure of sensitive personal data. She was therefore wrong to find that there had been a breach of M's data protection rights

under the DPA 1998 and of her rights under Article 8 ECHR and to grant declaratory relief. The cross-appeal should therefore be allowed on that ground. It follows that there is no basis for the award of damages and Ground 4 of the appeal does not arise.

140. I would merely add for the sake of completeness that I consider the Judge was right, for the reasons that she gave in her supplementary judgment, to make a nominal award in the sum of £500, and I would have dismissed the appeal on that ground in any event.

141. The second ground of the cross-appeal is of little importance in the light of that finding. However, in deference to Mr Gold's arguments, I am persuaded that the Judge also fell into error in holding that Operation C was concerned, as such, with young women vulnerable to CSE, such that any reference to M being of interest to that operation necessarily disclosed that she was at risk of CSE.

142. The two emails relied upon by the Judge are described by her in paragraph 113 of the judgment. The first email, sent on the afternoon of 3 October 2017, makes no reference to Operation C. It was a request by the Brighton & Hove Vulnerability Team to the BCRP to put out an urgent missing person alert relating to a young person who had been reported missing by her mother 2-3 days previously. Superintendent De La Rue explained in his witness statement that the Vulnerability Team was a divisional police team whose work included trying to reduce the vulnerability of people who regularly went missing, and generally associated risks. It forwarded a report which the Vulnerability Team had been emailed shortly beforehand (by someone whose identity has been redacted) which stated, among other things, that this was concerning due to the company she was now keeping, naming two other people including M, "both of whom have intel for CSE risks". (Although it probably does not matter, in paragraph 44 of her judgment the Judge appears to have mis-read the email as referring to M herself on an occasion when she went missing from home.)

143. The person at the BCRP to whom the email was sent (presumably the Manager or another NPV 2 vetted administrator) responded by saying "I will distribute to members via our website. Please could you let me know if she is located". There is no direct evidence of what was posted on the website on this occasion, but the evidence of Ms Perretta was that the "missing person alert" would display an image, a name, description, and any information relating to the missing person's potential whereabouts. She exhibited examples of such alerts. She was emphatic that the BCRP would not reveal to its members any concerns that someone was vulnerable to CSE.

144. The second email was from the BCRP Manager or one of the vetted representatives to the police and was dated 29 January 2018. The subject is "Operation C – M." It reports, among other matters, that M had been seen in a highly intoxicated and an emotional state on the street in the early hours of the morning on the previous Sunday, and that earlier (that night) a security guard had "put her on the NightSafe Radio and raised issues around her vulnerability." It indicated that attempts had been made to obtain assistance for M from the police, without success, and that the sender was concerned by this.

145. The Judge said that the clear implication of that email was that those receiving it knew that Operation C was concerned with young people who were said to be

vulnerable. She acknowledged that taken by itself the email could merely be reflecting "the fact that it was obvious to the security guard that M was at risk of exploitation by reason of her conduct at the time" but nevertheless found that putting the two emails together "it was plain that [the Respondent] did give BCRP information about M being vulnerable and at risk of sexual exploitation".

146. I regret that I am unable to find any proper evidential foundation for the Judge's conclusions in respect of what the BCRP (and its members) must have been told about Operation C, let alone discern why she thought the first email lent support to her interpretation of the second email. She appears to have based her conclusions on a number of flawed assumptions, namely (i) that the January email was an email from the police to the BCRP, rather than vice versa, as was in fact the case, (ii) that the reference to "vulnerability" in that email was a specific reference to the risk of CSE, (iii) that there was a link between the vulnerability ascribed by the security guard to M, and the sender's identification of her as a subject of Operation C and (iv) that the reference to Operation C must have meant that the police had disclosed to the BCRP that the subjects of that operation were sexually vulnerable and at risk of CSE.

147. Even if one regards the reference to "those receiving it" as a simple mistake and that what the Judge meant to say was "those sending it", the reasoning is unsound. At most, the January email indicated that a person known to the BCRP Manager/administrator who sent it to be one of the subjects of Operation C, had been seen in the early hours of the morning behaving in a way that (quite understandably) led to the raising of concerns, including safeguarding concerns, about her. An intoxicated and emotionally distressed female alone on the street in the early hours of the morning would be vulnerable to assault (including sexual assault), theft, abduction, or causing herself accidental or even deliberate personal injury, to name but a few obvious risks. The email conveyed nothing about the ambit of Operation C, let alone what the police had told the BCRP or the BCRP had shared with its members about Operation C or its subjects in the past. The email from the Vulnerability Team sent the previous October, which makes no mention of Operation C, does not supply a missing link in the chain.

148. There is no indication that in reaching the conclusions that she did, the Judge had taken account of the evidence of Superintendent De La Rue which explained that Operation C, which ran until June 2018, and appears to have had a measure of success, concerned a group of young people, most of them female, who were initially flagged up *by the BCRP* to the police as a cause of concern, because they were causing problems for their members by committing thefts, violent offences and antisocial behaviour both in the daytime and at night, and that behaviour was escalating. It appears to have been initiated following an assault on the manager of a local fast-food restaurant. The focus of the police operation was on identifying those responsible for and reducing the violent offending.

149. The police operation was designed to focus specifically on addressing the offending behaviour of the 7 core members of the group, of whom M appears to have been one. The Superintendent's evidence was that as well as law enforcement the operation had a supportive strand, and that officers were allocated to try and engage with each of the girls and divert them from offending and unsafe behaviour. In that context, he explained that many of the girls were reported missing on a regular basis and were engaged with by the Vulnerability Team.

150. The contemporaneous emails on which the Judge relied were not inconsistent with the Superintendent's evidence, nor with the evidence from Ms Perretta, the BCRP Business Crime Reduction Manager, which described Operation C as a police-directed operation that targeted "youth violence and disorder." As she explained, informing a BCRP member that an individual was "part of Operation C" was done to warn them of the increased risk of violence or anti-social behaviour from them, so that they could take precautions against it or call the police.

151. The Judge was therefore unjustified in drawing the inference that any reference to M being a subject of Operation C was enough in and of itself to reveal that the police considered her to be sexually vulnerable or at risk of CSE. However, that minor aberration does not affect the outcome of the cross-appeal, because even if she had been entitled to reach that conclusion, the information was not "sensitive data".

Conclusion

152. I would dismiss the appeal and allow the cross-appeal.

Lady Justice Asplin:

153. I agree.

Lord Justice Bean:

154. I also agree.