Neutral Citation Number: [2019] EWHC 975 (Admin)

Case No: CO/4645/2018

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
ADMINISTRATIVE COURT

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 15/04/2019

Before :

THE HONOURABLE MRS JUSTICE LIEVEN DBE

- -

Between :

The Queen (on the application of M by her Litigation Friend the Official Solicitor)	**Claimant**
- and -	
The Chief Constable of Sussex Police	**Defendant**
- and –	
BCRP	**Interested Party**

- -
- -

Eric Metcalfe (instructed by **Matthew Gold**) for the **Claimant**
Elliot Gold (instructed by **Weightmans LLP**) for the **Defendant**

Hearing dates: 27 February 2019

- -

Approved Judgment

Mrs Justice Lieven:

Introduction

1. This is a challenge to the decision of the Defendant, the Chief Constable of Sussex Police, to share data about the Claimant, M, with the Interested Party, a Business Crime Reduction Partnership in the Defendant's area (BCRP).

2. The Claimant is a vulnerable 16 year old girl. She has gone missing from home on a large number of occasions and was excluded from school. She has convictions for shoplifting and assault and according to the Police has since 31 October 2017 been reported for over 50 incidents of violence, theft or anti-social behaviour, largely or exclusively in the Defendant's area. She has been assessed by the local authority as being at risk of child sexual exploitation. She lives with her Mother, who has made a number of witness statements in this action.

3. BCRP is an organisation with more than 500 members. This includes a large number of local businesses including retailers both local and national and a number of private security firms, pubs, bars and nightclubs. The principal function of the BCRP is its management of an exclusion notice scheme, prohibiting persons from entering its members' commercial premises. The Claimant was made subject to an exclusion order on 7 November 2017 for a period of 12 months.

The Issues

4. The Claimant brings two analytically separate challenges. Firstly, she challenges the Defendant's Agreement to share information with the BCRP, in particular sensitive personal data, contrary to the Data Protection Act 2018 (Issue One). Secondly, she challenges the past disclosure of her sensitive personal data by the Defendant to the Interested Party (Issue Two).

5. Issue one is essentially forward looking, whereas issue two involves considering past decisions and actions. The position is somewhat complicated by the chronology. The Defendant has been in an Information Sharing Agreement with the Interested Party since at least 2013. As of November 2017, the ISA in force was version 10 (ISA2017). At this point the Data Protection Act 1998 was in force. The Data Protection Act 2018 then came into force on 25 May 2018. The Claim was lodged on 20 November 2018. The Defendant entered into a new Information Sharing Agreement in December 2018 (ISA2018). The position when the Claimant's sensitive personal data was shared by the Defendant with the BCRP is not entirely clear for the reasons I will explain below. However, it was agreed that the majority of the disclosure (at least 4 out of 5 occasions) about which the Claimant complains, took place before 25 May 2018, i.e. under the 1998 Act.

6. The upshot of this chronology is that Issue One is now focused upon whether the ISA 2018 meets the requirements of the Data Protection Act 2018. The question of whether the ISA 2017 met the terms of the 2018 Act is now only of historic interest (and potentially issues that may go to costs); whereas Issue Two largely concerns whether disclosures under the ISA 2017 were in breach of the DPA 1998.

7. I will focus below on the Issue One position, i.e. whether ISA 2018 meets the legal requirements of the DPA 2018, but where relevant for Issue One set out the differences under the earlier agreement and the DPA 1998. I will then turn to Issue Two, and whether the individual disclosures, which the Claimant complains about, occurred in breach of the DPA 1998 and DPA 2018, as applicable.

Disclosure

8. The other complicating factor in this case, which I should deal with at the outset, is the position on disclosure to the Court and the Defendant's duty of candour. As is well known in judicial review the Defendant is under a duty to "*assist the court with full and accurate explanations of all the facts relevant to the issue the court must decide*" (*R (Quark Fishing Ltd) v Secretary of State for Foreign and Commonwealth Affairs* [2002] EWCA Civ 1409 at para 50 Laws LJ). This duty extends to disclosure of "*materials which are reasonably required for the court to arrive at an accurate decision*" (*Graham v Police Service Commission* [2011] UKPC 46, para 18). In *R (Bancoult) v Secretary of State for Foreign and Commonwealth Affairs (No 2)* [2016] UKSC 35, Lord Kerr cited with approval the following summary:

> *"A defendant public authority and its lawyers owe a vital duty to make full and fair disclosure of relevant material. That should include (1) due diligence in investigating what material is available; (2) disclosure which is relevant or assists the claimant, including on some as yet unpleaded ground; and (3) disclosure at the permission stage if permission is resisted. … A main reason why disclosure is not ordered in judicial review is because courts trust public authorities to discharge this self-policing duty, which is why such anxious concern is expressed where it transpires that they have not done so* (Fordham, *Judicial Review*, 6th ed, 2012, p125)."

9. On 18 December 2018 Lang J granted permission for judicial review and ordered the Defendant to file Detailed Grounds of Defence and "any written evidence" within 28 days of the order, i.e. by 15 January 2019. No Detailed Grounds were filed, but the Defendant subsequently explained this was because they had intended to simply rely on the Summary Grounds. They did file three witness statements, but it was entirely clear to the Claimant (and subsequently to me at the hearing) that this evidence, together with the Summary Grounds of Defence, did not amount to full and fair disclosure of relevant material. The Claimant then issued a Part 18 request. The Defendant declined to respond to this on the basis that they said it did not touch on the primary question in the judicial review.

10. On 22 February 2019 the Defendant applied to rely on further evidence. This consisted of a second witness statement from Ms P of BCRP, together with a series of obviously highly relevant documents including the BCRP Constitution, Code of Practice, Data Integrity Agreement and Policy for processing personal data on children and minors on the basis of legitimate interest; as well as the ISA2018, which had been entered into on 18 December 2018. The only explanation for the extremely late disclosure of these documents was that there had been poor communication between BCRP and the Police. The Claimant did not object to the admission of this evidence, provided she was permitted to amend her Claim. I allowed the evidence to be admitted, ordered relief from sanction, and allowed the Claim to be amended to now cover the 2018 ISA.

11. However, even with this additional evidence it remains the case that it is virtually beyond doubt that there is further relevant material which still has not been disclosed. In particular, and this is important for Issue Two, the Court has not seen the actual record of disclosure from the Police to BCRP in respect of M on the occasions I refer to below. Further, the position remains 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 child sexual exploitation (CSE), which is relevant to one part of Issue Two.

12. The consequence of this apparent failure to properly comply with a duty of candour is twofold. Firstly, I cannot be confident as to precisely what was disclosed and in what terms to BCRP. Secondly, it has relevance to the weight I can attach to the various policy documents Mr Gold, who appears for the Defendant, relies upon to seek to persuade me that there are adequate safeguards in place, to ensure that the disclosure of material is in accordance with law. Given the difficulty which the Defendant appears to have had accessing the relevant documents for the purposes of disclosure, there must be some concern as to whether safeguards set out in those documents can be relied upon. I will return to this point when dealing with Issue One.

The Business Crime Reduction Partnership (BCRP)

13. The BCRP consists of an Executive Committee, a Board of Management and the members. One of the Defendant's Chief Inspectors is on the Executive Committee.

14. The members submit incident reports to the Board of Management, and the Police may also submit reports, whether of their own motion or on request. Once an individual reaches a certain threshold then certain information about them is shared with BCRP members via a secure intranet site and secure mobile application. The information that the BCRP holds on an individual (including M) comes from a variety of sources. The decision as to whether to exclude an individual is made by BCRP Management Committee.

15. There are a number of documents produced by the BCRP which are relevant to the issue of data sharing, including the Constitution, the Code of Practice, and the Data Integrity Agreement.

16. The BCRP has a constitution, signed in 2004. That provides that the Board of Management is the data controller for the BCRP. It appears that under the constitution it is the Executive Committee that decides the type of information that will be shared with participating members.

17. The BCRP also has a Code of Practice, which I understand applied at all relevant dates. The relevant parts are as follows;

    (a) Para 1.1 "This code of practice is to control the management, operation, compliance and use of data within the partnership."

    (b) Para 3.2 that

"*each member of the partnership is and remains bound by the code of practice and other operating protocols and any subsequent amendments to them".*

(c) Section 4 deals with partnership discipline;

a) Para 4.3 *"*All rules on confidentiality and data protection must be subject to written agreement and must be strictly adhered to by the data controller, employees of the partnership and all members. Noncompliance of the Date Protection Act 2018 may lead to criminal prosecution and/or civil actions for damages."

b) Para 4.5 "Partnership employees will receive training to ensure that a good standard of knowledge is maintained."

c) Para 4.6 "Any persons employed or considered for employment by the Partnership will be required to disclose prior convictions, if any, (and, if appointed, notify future convictions) in order that a judgement may be made relating to likely impact upon the integrity of partnership information. The parent company will assess whether the offence has a bearing on the nature of the appointment or continued employment."

d) Para 4.10 "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."

(d) Section 7 deals with third party employees and states at para 7.2 "Disclosure of data to such third party employees must only be as provided for under the Data Protection Act 2018 and only following assessment by the data controller. The decision to disclose will be on a case-by-case basis and should not be regarded as being available under an automatic authority.

(e) Section 9 deals with security/audit of data and states at para 9.6 "The partnership and its individual members will submit to inspections with a detailed audit report against the requirements and principles of the Data Protection Act and partnership operation protocols. The results will be made available. The Board of Management or other nominated representatives authorised on their behalf will be responsible for the audit process to ensure individual members maintain the appropriate standards of security and confidentiality."

(f) Sections 13 refers to the data protection principles in the 2018 Act.

(g) Section 14 sets out the data protection requirements including 14.2 "All staff who have access to personal data recorded by the partnership must be made aware of the following: ...

> b) Any such information must not be disclosed to <u>any</u> third party who has not signed the necessary agreements under any circumstances whatsoever. Doing so will constitute a breach of the Data Integrity Act 2018 and may result in prosecution
>
> ….
>
> e) Staff employed by members who are allowed access to the data must sign the data and information disclosure declaration to indicate that they have been advised of their statutory obligations and responsibilities."

18. The Data Integrity Agreement (DIA) is headed "*Data Integrity Agreement Confidentiality Agreement incorporating Partnership Protocols"*. The DIA requires members not to disclose data to non-signatory members and to ensure appropriate measures were taken to prevent unauthorised access to data.

19. On 9 November 2017 the Police and BCRP entered into an Information Sharing Agreement (ISA.) This replaced an earlier agreement. The most relevant provisions of the November 2017 ISA are as follows (ISA2017):

<u>Data Sharing Agreement 2017</u>

20. Paragraph 2.1 of the Agreement states that its purpose is *"to enable action to be taken against crime and anti-social behaviour within [the area]"* and will *"incorporate measures aimed at"*:

- *Facilitating the secure sharing of photographs and incident data between [the Defendant] and members of [BCRP] Scheme.*
- *Facilitating the collection and exchange of relevant information*
- *The pursuit of civil or criminal proceedings – either by [the Defendant] or [BCRP]*.

21. Paragraph 4.1 states that the Agreement fulfils the requirements of *inter alia* section 115 of the Crime and Disorder Act 1998, article 8 of the Human Rights Act 1998, and sections 29(3) and 35(2) of the Data Protection Act 1998. Paragraph 2 cites the decision of *Hellwell*, including the reference to distribution of "*the plaintiff's photograph … to only persons who had reasonable need to make use of it*".

22. Paragraph 6 sets out the types of information the Defendant will share materially as follows:

- *Details of any incident relating to criminal and/or anti-social behaviour linked to a member of the BCRP, these being sanitised of personal identifiable data …*

- ….

- *Details of any missing persons, wanted on warrant or recall to prison sanitized with no detail of the crime committed as long as relevant to the BCRP scheme.*

- *Details of those with CBO's may be passed on to the BCRP for dissemination to its members.*

- *Details of any bail conditions relating to any known BCRP subjects or police operations relating to the BCRP.*

- *If Sussex Police wish to raise an individual that has not met the BCRP threshold for intel purposes they can do on the authorisation of an Inspector or above however the BCRP have the right to refuse to do so if they believe it not to be relevant to the scheme.*

- *Photographs can be exchanged after the BCRP has received 3 reports of any criminal and/or anti-social behaviour against or in the direct vicinity of its members premises within an 8 month period or at the point the BCRP's ban criteria has been met irrespective of age on the daytime economy.*

- *Photographs can also be exchanged for a watch/targeted list for both daytime and night time economies if there has been 1 incident of violence against a BCRP member premises or at the point the BCRP's ban criteria has been met irrespective of age on the night time economy.*

- *Addresses can be exchanged as long as the BCRP ban criteria has been met irrespective of age ….*

- *Photographs can also be exchanged for a watch/targeted list for both daytime and night time economies if deemed appropriate by BCRP data controller if there has been 1 incident of the following which has impacted on a BCRP Members premises and has been reported officially to Sussex Police:*

    - *Possession with intent to supply drugs*
    - *Theft from person*
    - *Hate crime*
    - *Threats/acts of violence*
    - *Threats/acts of sexual assault/inappropriate behaviour*
    - *Possession of offensive weapon*

- *Photographs should only be displayed by the BCRP for up to a 12 week period at which stage the photograph will be removed unless further intelligence and/or incidents of criminal activity and/or anti-social behaviour is submitted to the BCRP or the individual is subject to a ban whereby the photograph can remain out for the length of the ban.*

23. Paragraph 7 provides as follows:

7.1 The information shared must not be disclosed to any third party or used as part of any investigation without the written consent of the partner that provided the information. It must be stored securely and destroyed when it is no longer required for the purpose for which it is provided.

7.2 The information shared must not be copied, shared or distributed in any way to any other person or business.

7.3 There must be a clear audit trail which covers the whole process when information is shared.

- *[The Defendant] will keep a record of photographs circulated to [BCRP] Scheme. This record will include information covering the decision to circulate each photograph.*
- *The BCRP must ensure an adequate audit trail is in place to record disclosures.*
- *The photograph will be displayed for the length of time permitted as per above criteria and then securely or automatically destroyed.*
- *BCRP will have an audit trail of any images they have provided that are stored onto third party electronic device such as IDScan. [The Defendant] and/or BCRP have the right to remove this data immediately if deemed necessary to do so.*

24. Paragraph 8.4 further provides that:

Police photographs are confidential documents and their use is restricted by an obligation to the data subject not to display them publicly. Photographs must be treated as confidential by the [BCRP] member and viewed only by the appropriate members of their staff. Photographs must not be copied, altered or manipulated in any way.

25. Paragraph 8.6 provides that:

The [BCRP] Scheme member will comply with the requirements of use, safekeeping and maintenance of provided data. Should there be any failing in these requirements, it is the responsibility of the [BCRP] Data Controller to notify [the Defendant] immediately. If there is a breach of these requirements, [the Defendant] may require the [BCRP] member to surrender all data held.

26. Paragraph 10 provides as follows:

10.1 Partners to this agreement undertake that personal data shared will only be used for the specific purpose for which it is requested. The recipient of the information is required to keep it securely stored and will dispose of it when it is no longer required.

10.2 ….

10.3 The recipient will not release the information to any third party without obtaining the express written authority of the partner who provided the information.

10.4 …

10.5 All data held must be reviewed by the partner at least every twelve months for validity and relevance. Data which is no longer valid or relevant must be returned to [the Defendant].

Information Sharing Agreement 2018 (ISA2018)

27. The ISA was reviewed, at least in part in order to comply with the Data Protection Act 2018 and the General Data Protections Regulation 2018 (GDPR), and the ISA 2018 was entered into in December 2018.

28. ISA 2018 states in section 1 that its purpose is inter alia to ensure compliance with Data Protection legislation. It sets out the purposes of sharing information at section 2, and says that decisions will be made on a case by case basis. Section 2.3 states that the shared information is only available to members who have signed the Data Integrity forms and read the "must read" information.

29. Section 3 sets out the legal basis for sharing, and what specifically will be shared. It says that the law allows the Police and BCRP to be joint data controllers in relation to data shared under the agreement. The various data principles in the 2018 Act are then set out in Section 3.

30. Section 3.1.6 refers to Article 6(f) of the GDPR and that the necessity test may be overridden in particular where the data subject is a child. This appears to be the only reference to the particular position of children in the ISA 2018 itself.

31. Section 4 is headed "Description of arrangements including security matters". Mr Gold relies on this section for the safeguards on the sharing of data. The key parts are as follows:

    (a) Only if the BCRP manager or representative has been NPV2 (National Police Vetting) vetted can s/he extract the data direct and the manager and relevant staff must be vetted to that standard;

    (b) Information will not be shared to businesses outside the secure intranet, and once accessed any further distribution will be the responsibly of that person but must be done in compliance with data protection law;

    (c) Security officers of BCRP members will have valid licences from the Security Industry Authority, and will be DBS checked.

(d) The BCRP manager must ensure that information shared with members is the bare minimum.

32. The ISA 2018 has a series of appendices, including appendix 3 "How/what information will be shared and constraints". Information shared will include details of bail conditions and photographs subject to the relevant thresholds.

33. Appendix 4 is headed "Policy for processing personal data on children and minors on the basis of legitimate interest". This Appendix starts with a background section that sets out the principles on protecting the rights of children and in particular the issues around the age of criminal responsibility. However, the Appendix is principally concerned with the correct approach to the decision on exclusion of children from premises, rather than being about the approach to information sharing after an exclusion notice. There is a reference at para 13 to "*the basis for processing of children's data will be subject to a Legitimate Interest Assessment [see Appendix 1]".* In the copy of the ISA 2018 before the Court this appendix was in a totally different place, and not attached to the agreement at all. Further, the reference to appendix one is highly confusing because there is an appendix one to the ISA, which is a quite different document.

34. The Legitimate Interest Assessment document is plainly focused on data processing under the GDPR, rather than on the specific issues of data sharing under the ISA 2018. In principle the same factors arise but the questions are not always focused on the correct issue. So question 3C on the "balancing test": *is the processing likely to negatively impact the child's rights? Answer No. Not on their rights under the GDPR. Their rights to enter our Members' premises is tacit and can be withdrawn at any time under the Common Law."* It is easy to see that the question as to whether a child's rights may be infringed by sharing his/her photo or bail conditions, is quite a different one and the balancing exercise different. Most importantly the impact on the child from that data sharing may be entirely different and potentially much more wide ranging, than the impact from excluding them from certain premises.

35. Section J of the Legitimate Interest Assessment states: "*What is the nature of the data to be processed? Does data of this nature have any special protection under GDPR? Answer: Name. Date of birth. Photographic image. Address. Offences against BCRP Members. The processing of children's data enjoys special protection under the GDPR but UK derogations allow the processing of such data for the purposes of the prevention of crime and disorder."* This section is important because Mr Gold submits that this is where the data that can be shared is limited, and therefore bail conditions are no longer to be shared under the agreement. Although I accept this may be the intention, the change is buried deep in the document, with no signposting that such a major change has taken place.

36. Section T states as follows: "*Safeguards & compensating controls. … 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."*

The process of data sharing

37. The Defendant's position is that all the sharing of data complied with the Data Protection Acts. The BCRP used an industry standard secure database with end-to-end encryption and individual password protection. Given that the Claimant's concerns arise not about the transmission of data from BCRP to wholly external parties, but rather the transmission from BCRP members to their staff and employees, I need say no more about the security systems between BCRP and external third parties.

38. Ms P on behalf of the BCRP explains in her second witness statement how data is managed within the organisation. The BCRP receives incident reports from its members via online reporting to a secure database. Whenever data is received or processed the individual is informed by privacy statement and warning letter, which informs them that any further offences may result in an exclusion notice.

39. Once an individual reaches a certain threshold then their image, name, date of birth and type of offence will be shared with BCRP member via the secure intranet. At this point the Police may be asked to provide a photographic image. For minors the decision to share information with members is taken by the Board of Management consisting of three people with at least one of them either being the Chair of the BCRP or the Crime Manager.

40. Members can access the intranet site either via computer or on an App for smartphones. Out of the 500 members of BCRP 239 members have sought and been granted access to the intranet. If members do not log on for 6 weeks they are automatically removed. Every 6 months members are locked out of the intranet and are required to re-certify their adherence to the data integrity agreement, before they are allowed to regain access.

Evidence of M's data having been shared

41. The evidence of the Police is that pursuant to the ISA they shared the following data on the Claimant with the BCRP:

    (i) "C was observed in an assault/violence/affray [Def 57];

    (ii) C observed in the act of breach of police bail, assault and stealing of a handbag [Def 56];

    (iii) C observed in an act of assault/violence/affray, assaulting a young woman [Def 54];

    (iv) C observed in an act of assault/violence/affray, assaulting a woman [Def 52];

    (v) 7th June 2018 at 6:02. C observed in an act of assault/violence/affray, kicked two police officers [Def 51]."

42. The Police in their Detailed Grounds of Defence said that "at no point on any occasion" have they disclosed any data to the BCRP stating that C is a person who is sexually vulnerable and/or at risk of sexual exploitation. This is a contentious issue in the case, so I need to set out the factual material in a little detail.

43. The Police have been conducting an initiative or operation called Operation C in the area. As described in the Detailed Grounds of Defence this is a police-led initiative to reduce the violent behaviour of a defined group of young women, which included the Claimant. The Detailed Grounds state that this is neither an operation involving children per se nor sexual vulnerability per se.

44. The Claimant went missing on a number of occasions in or around August 2017 and there were reports to the Council that she had been seen in the presence of older men. She was placed by the Council on the Child Sexual Exploitation risk register. When she went missing in October 2017 the Defendant emailed the BCRP to report that the Claimant was missing, stating that "*[i]t was concerning due to the company she is now keeping XXX, [the Claimant] whom both have intel for CSE risks*". The BCRP replied to the email, stating that it would "*distribute to members via our website*". The Claimant subsequently returned home.

45. In November 2017, local media reported that the Claimant was missing from her home and that police were seriously concerned for her welfare. On the same date, the Defendant emailed the BCRP asking for its help to locate the Claimant. The Claimant was subsequently located and taken into interim foster care.

46. In November 2017, the BCRP served the Claimant with an exclusion order by reference to numerous reports of her anti-social behaviour. The effect of the order is that the Claimant is not permitted to enter the premises of any BCRP member within the exclusion zone.

47. On 11 December 2017, the BCRP emailed the Defendant complaining about the activities of young people involved in assaults. Among other things it stated that "BCRP members are frustrated at the amount of theft occurring but now the level of violence. We are appreciative that there are huge vulnerability issues and we are encouraging members to keep a duty of care hat on as well but staff are stating that [they] are afraid to come to work".

48. On 12 December 2017, the BCRP emailed an alert to its members asking them to report any incidents concerning the Claimant. The BCRP also circulated a notice containing the Claimant's photo (among others) and referring to reports of her involvement in criminal activity. The notice stated that "[w]e are working very closely with partner agencies to ensure that the appropriate action is taken in regards to these females. We therefore ask that ANY incidents (regardless of the severity) concerning these females are reported to police."

49. On 14 December 2017, a social worker with Children's Services emailed the Defendant to express concern that its alerts for missing girls, including their names and photographs, remained accessible online even after they had been found. The Defendant replied that "once the missing persons have been found and cancelled on the Sussex police website it will link stating they have been found. What we have no control over is if the link is shared prior to this by third parties then we cannot stop this linking". On 15 December 2017, a manager with Children's Services replied to the Defendant, stating that "this said protocol of the police … might well put [young people] at risk".

50. On 21 February 2018, the Claimant was arrested on a charge of assault and granted bail. An order was made under section 45 of the Youth Justice and Criminal Evidence Act 1999 prohibiting the Claimant's identification. Following this, the Claimant's solicitor became aware that the BCRP was sharing the Claimant's data by means of its app. This data included:

    a. C's full name and date of birth;
    b. her bail conditions;
    c. her status as a "top 10" offender;
    d. that she is "known" for "theft/fraud"; and
    e. that she is named in relation to Operation C, directed at vulnerable young women in the local area who are allegedly involved in anti-social and/or criminal behaviour.

51. There were a series of emails between BCRP, the Police and the Council in March and April 2018. The Council raised concerns that M's bail conditions had been revealed, and were now being posted on social media. The Defendant does not argue that up until mid 2018 it was informing BCRP about M's bail conditions, and as I explain below Mr Gold argues that this was lawful.

52. On 21 May 2018, the Claimant's solicitors sent pre-action letters to the Defendant and BCRP, together with notices under section 10 of the Data Protection Act 1998 requiring them to cease processing her personal data on the basis that the processing was contrary to the requirements of the 1998 Act, article 8 ECHR, in breach of the anonymity requirements of section 45 of the Youth Justice and Criminal Evidence Act 1999, and causing her damage and distress.

The law

The Data Protection Act 2018

53. The law in this field is complex, and the statute labyrinthine, so I will have to set out large parts below. Part 3 of the Data Protection Act 2018 ('the 2018 Act') sets out the relevant provisions for the handling of data.

54. The Defendant is a '*competent authority*' for the purposes of Part 3 of the Act: see section 30(1)(a) and paragraph 5 of Schedule 7 to the 2018 Act.[1] It is a data controller within the meaning of section 32 (1) and (2) of the Act. Section 32(3) provides that a data processor under Part 3 is "*any person who processes personal data on behalf of the controller (other than a person who is an employee of the controller)*".

55. Sections 34-40 set out the six data protection principles which correspond to those under Article 4(1) Law Enforcement Directive (LED). In relation to the first data protection principle, section 35 provides materially as follows:

    (1) The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair.

[1] The Defendant's area being listed under section 2 and Schedule 1 of the Police Act 1986.

(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 either -

(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).

…
(8) In this section, "sensitive processing" means—

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual
(c) the processing of data concerning health;
(d) the processing of data concerning an individual's sex life or sexual orientation.

56. Schedule 8 provides materially as follows:

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

(1) This condition is met if—

(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 well-being 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).

(3) For the purposes of this paragraph, an individual aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the individual—

(a) has needs for care and support,

(b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and

(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

(4) In sub-paragraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual.

5 Personal data already in the public domain

This condition is met if the processing relates to personal data which is manifestly made public by the data subject.

57. Section 40 sets out the sixth data protection principle as follows:

The sixth data protection principle is that 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).

58. The requirement to have appropriate technical and organisational measures was previously known as the Seventh Data Protection Principle (para 7 of Schedule 2 of the Data Protection Act 1998). In *CLG & Ors v Chief Constable of Merseyside Police [2015]* EWCA Civ 836, the Court of Appeal (Moore-Bick LJ, Fulford and Vos LJ concurring) held that the principle:

"46 .... relates to the implementation of appropriate systems for ensuring the protection of personal data. .... The language in which the seventh data protection principle is cast ("appropriate . . . measures shall be taken against . . . unauthorised or unlawful processing") is not apt to impose an absolute duty to prevent the misuse of data. It imposes no more than 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.

59. In *Various Claimants v WM Morrisons Supermarket Plc* [2017] EWHC 3113 (QB The claimants brought a private law action against their employer alleging, among other things, breach of the Seventh Data Protection Principle (namely the requirement to take "*appropriate technical and organisational measures ... against unauthorised or unlawful processing of personal data*". Langstaff J analysed that requirement as follows:

"67. The seventh principle does not impose a duty to take "reasonable care" as such. Those words do not appear in the Statute. This might suggest that the draftsman was aiming at a rather different target when he required that "appropriate" measures be taken. This word comes from the Directive: it is likely therefore to bear an autonomous meaning, which will apply in each Member State of the EU to whom it is addressed. However, it is clear that the principle is a qualified one. The mere fact of disclosure or loss of data is not sufficient for there to be a breach. Rather, "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: an example might be if particular security measures might be introduced which are very costly at the present stage of development, whereas after a few more years the cost might reduce significantly, as is the case with many new technologies. However, the following words in DPP7 indicate that 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.

68. Though, as I have pointed out, the words "reasonable care" are not employed, there is a resonance here of the common law approach to the tort of negligence, where the standard of reasonable care is to be judged by balancing the magnitude of the risk of the activity in question (itself a combination of the likelihood of injury and the severity of it should it occur) against the availability and cost of measures to prevent the risk materialising, and the importance of the object to be achieved by performing those actions. That approach is accordingly indicative of the standard which should apply here, whilst remaining mindful that it is being applied in the field of data protection and it is, in general terms, of considerable importance that data be kept secure.

60. On appeal, the Court of Appeal (Etherton MR, Bean and Flaux LJ) added a further observation concerning the requirement to take "*appropriate*" measures:

41. What is "appropriate" is related to the state of technological development and the cost of implementing any measures as well as the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage, and the nature of the data to be protected: Schedule 1 Part II para. 9. Importantly, under DPP 7 the data controller must take "reasonable steps" to ensure the reliability of any employees of his who have access to the personal data: Schedule 1 Part II para. 10. The DPA, therefore, expressly recognises the potential liability of a data controller for the wrongful processing of data by his employees. Instead, however, of imposing a vicarious liability, which is a strict liability irrespective of the employer's fault, it imposes a primary liability on the employer restricted to taking "reasonable steps" to ensure the reliability of the relevant employees. Further, section 13(3) provides that it is a defence to an action by an individual for compensation from the data controller for breach of any of the requirements of the DPA that the data controller has taken such care as in all the circumstances was reasonably required to comply with the requirement concerned. In effect, so far as concerns civil liability, the liability is based on fault or culpability: cf. criminal liability under section 55 of the DPA.

61. Section 42 sets out the further safeguards required in respect of the processing of sensitive data

(1) This section applies for the purposes of section 35(4) and (5) (which require a controller to have an appropriate policy document in place when carrying out sensitive processing in reliance on the consent of the data subject or, as the case may be, in reliance on a condition specified in Schedule 8).

(2) The controller has an appropriate policy document in place in relation to the sensitive processing if the controller has produced a document 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.

(3) Where personal data is processed on the basis that an appropriate policy document is in place, the controller must during the relevant period-

(a) retain the appropriate policy document,

(b) review and (if appropriate) update it from time to time, and

(c) make it available to the Commissioner, on request, without charge.

(4) The record maintained by the controller under section 61(1) and, where the sensitive processing is carried out by a processor on behalf of the controller, the record maintained by the processor under section 61(3) must include the following information—

(a) 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,

(b) how the processing satisfies section 35 (lawfulness of processing), and

(c) whether the personal data is retained and erased in accordance with the policies described in subsection (2)(b) and, if it is not, the reasons for not following those policies.

(5) In this section, "relevant period", in relation to sensitive processing in reliance on the consent of the data subject or in reliance on a condition specified in Schedule 8, means a period which—

(a) begins when the controller starts to carry out the sensitive processing in reliance on the data subject's consent or (as the case may be) in reliance on that condition, and

(b) ends at the end of the period of 6 months beginning when the controller ceases to carry out the processing.

62. Chapter 4 of Part 3 of the Act sets out the general obligations of controllers and processors, including:

56 General obligations of the controller

(1) Each controller must 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 this Part.

(2) Where proportionate in relation to the processing, the measures implemented to comply with the duty under subsection (1) must include appropriate data protection policies.

(3) The technical and organisational measures implemented under subsection (1) must be reviewed and updated where necessary.

57 Data protection by design and default

(1) Each controller must implement appropriate technical and organisational measures which are designed—

(a) to implement the data protection principles in an effective manner, and

(b) to integrate into the processing itself the safeguards necessary for that purpose.

(2) The duty under subsection (1) applies both at the time of the determination of the means of processing the data and at the time of the processing itself.

(3) Each controller must implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is used.

(4) The duty under subsection (3) applies to—

(a) the amount of personal data collected,

(b) the extent of its processing,

(c) the period of its storage, and

(d) its accessibility.

(5) In particular, the measures implemented to comply with the duty under subsection (3) must ensure that, by default, personal data is not made accessible to an indefinite number of people without an individual's intervention.

63. Section 59 provides materially as follows:

(1) This section applies to the use by a controller of a processor to carry out processing of personal data on behalf of the controller.

(2) The controller may use only a processor who provides guarantees to implement appropriate technical and organisational measures that are sufficient to secure that the processing will—

(a) *meet the requirements of this Part, and*

(b) *ensure the protection of the rights of the data subject.*

(3) …

(4) …

(5) The processing by the processor must be governed by a contract in writing between the controller and the processor setting out the following—

(a) the subject-matter and duration of the processing;
(b) the nature and purpose of the processing;
(c) the type of personal data and categories of data subjects involved;
(d) the obligations and rights of the controller and processor.

(6) The contract must, in particular, provide that the processor must—

(a) *act only on instructions from the controller,*
(b) ensure that the persons authorised to process personal data are subject to an appropriate duty of confidentiality,

64. Section 66 of the Act reads as follows:

(1) Each controller and each processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks arising from the processing of personal data.

(2) In the case of automated processing, each controller and each processor must, following an evaluation of the risks, implement measures designed to—

(a) prevent unauthorised processing or unauthorised interference with the systems used in connection with it,

(b) ensure that it is possible to establish the precise details of any processing that takes place,

(c) ensure that any systems used in connection with the processing function properly and may, in the case of interruption, be restored, and

(d) ensure that stored personal data cannot be corrupted if a system used in connection with the processing malfunctions.

65. In relation to the interpretation of the 2018 Act, Part 3 seeks to implement the UK's obligations under the Law Enforcement Directive (the LED). There is a somewhat complex issue, raised very fairly by Mr Metcalfe, as to the interaction between the LED and the 2018 Act, and whether the UK relied upon an "opt-out", see El-Gizouli v Secretary of State for the Home Department [2019] EWHC 60 (Admin) [178]. However, quite apart from the fact that the relevant Secretary of State is not a party to this action, I do not think it is either necessary or appropriate for me to try to decide the relationship between the LED and the 2018 Act. As I explain in the next paragraph, the terms of the LED appear to me to have a limited relevance in this case.

66. The only relevance of the LED is as an aid to interpretation of the provisions of Part 3 of the 2018 Act, it is not suggested to me that there is any mistransposition of the provisions of the LED and it is therefore not necessary to set out the detail of its provisions. In interpreting the provisions of the DPA 2018 Mr Metcalfe places considerable on recital 50, which states;

> *"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."*

67. It is in my view appropriate to take into account this recital in interpreting the provisions in the DPA 2018, but to the degree Mr Metcalfe is arguing that there is a legal requirement to have "specific safeguards" in respect of the data of children because of the terms of recital 50, I bear closely in mind that this is a recital, and there is no such requirement in those terms in the articles of the Directive.

68. Mr Metcalfe also relied on the UN Convention on the Rights of the Child (UNCRC), as an aid to construction of the Data Protection Acts, and the scope of the UK's obligations in terms of respecting children.

Crime and Disorder Act 1998

69. Mr Gold relies on the terms of the Crime and Disorder Act 1998 to establish the legitimate purpose of the ISAs and the data sharing. The Defendant is an authority responsible for crime and disorder strategies in Sussex under section 5(1)(b) of the Crime and Disorder Act 1998. Accordingly, it is obliged by section 6(1)(a) of that Act to "*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)*".

Children and Young Persons Act 1933

70. Mr Metcalfe referred me to s.49 of the Children and Young Persons Act 1933, which he says was breached by the sharing of bail conditions. That states;

> *(1) 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 the proceedings.*
>
> *(2) The proceedings to which this section applies are—*
>
> *(a) proceedings in a youth court;*
>
> ….
>
> *(4) For the purposes of this section a child or young person is "concerned" in any proceedings if he is—*

(a) a person against or in respect of the proceedings are taken, or

(b) a person called, or proposed to be called, to give evidence in the proceedings.

71. A similar provision exists in s.45(1) of the Youth Justice and Criminal Evidence Act 1999. Mr Metcalfe argued that the sharing of M's bail conditions with the BCRP was a breach of section 49 of the 1933 Act and of s.45 of the 1999 Act. Mr Gold argued that the employees with whom the bail conditions were shared were not "members of the public" and the bail conditions were not part of proceedings covered by the Act.

72. I was somewhat concerned about the scope of these submissions, and the potentially wide consequences for other cases as to who was or was not a member of the public for the purposes of s.45. I therefore asked counsel at the end of the hearing to do further research on the meaning of "members of the public". I am very grateful to both of them for the further written submissions and authorities with which they provided me.

73. There are a number of cases which deal with the meaning of the "the public" or "members of the public". They are all considering the meaning in their specific statutory context, and have to be read with that in mind. However, probably the most relevant case is *Dockers Labour Club v Race relations Board [1976]* AC 285, where despite the very large number of club associates (approximately one million) the House of Lords held that the club did not provide services to a section of the public because each associate had been subject to a separate procedure which therefore differentiated them from a member of the public.

74. Mr Metcalfe quite rightly pointed me to the strong public policy lying behind s.49, and the importance of assisting children and young persons' rehabilitation if they have offended, see *McKerry v Teesdale and Wear Justices [2000]* EWCA Crim 3553.

75. In my view the sharing of the bail conditions with BCRP and relevant employees, was not sharing with the public and was not "likely to lead members of the public to identify [her]" within the meaning in the CYPA. Those who received the information did so in their capacity either as BCRP members, or their employees or contractors, and did so on terms that were directly linked to those contracts. They were therefore not receiving the information on the bail conditions as members of the public, and they were not entitled to further disseminate the information to members of the public. Therefore there was no breach of the CYPA or the 1999 Act.

Grounds of Challenge/ Submissions

76. The Claimant advances two separate issues. Firstly, that the Defendant's Information Sharing Agreements (both November 2017 and December 2018) fail to provide sufficient safeguards to prevent the unlawful processing of the Claimant's sensitive personal data, and as such breach the 2018 Act. Secondly that there has been an unlawful and disproportionate disclosure of the Claimant's sensitive personal data.

Issue One

77. As I have explained above, in relation to the first issue the focus is now on the ISA 2018, and whether it complies with the DPA 2018. The Claimant's argument is that the Defendant's arrangements for sharing data failed to have appropriate technical and organisational measures to prevent unlawful sharing of sensitive personal data of the claimant and/or allows the unlawful processing of the same data.

78. The Claimant's argument proceeds in the following states. Firstly, the Defendant is the controller of the Claimant's personal data under s.32, and to the degree it shares M's data with BCRP, then BCRP is processing the data on the Defendant's behalf within the meaning of s.32(3).

79. Secondly, the Defendant therefore must be able to demonstrate compliance with the Data Protection Principles, see s.34(2).

80. Thirdly, the Defendant 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)).

81. It is Mr Metcalfe's submission that the 2018 ISA fails to afford specific safeguards, in particular to children and young people. He refers to the fact that the only reference in the ISA 2018 itself to children, is the reference to article 6(f) of the GDPR. He then argues that there is nothing to prevent the authorised person within BCRP from sharing the data with their fellow employees, and the discretion is left entirely, or largely, to the authorised person. He also argues that the Legitimate Interest Assessment is entirely about the GDPR and the decision whether or not to exclude, and it does not deal with children or young people who have already been excluded and/or entered the criminal justice system.

82. Mr Metcalfe also argues that the 2018 ISA breaches article 8 ECHR because there is an interference with the Claimant's right to privacy under article 8(1) for which the lack of safeguards and disproportionate impact mean that there is no justification under article 8(2). He also argues that there if there is a breach of the 2018 Act, then the interference is necessarily not in accordance with law and therefore again does not meet the requirements of article 8.

83. He further argues that there is a breach of EU law because there is a breach of article 8 of the EU Charter of Fundamental Rights (article 8 covers data protections). I cannot see that the Charter adds anything material to this case, which are not in any event covered by the statutory requirements and/or the broad scope of article 8 ECHR. Mr Metcalfe did not point me to any specific provisions of either the Charter or caselaw concerning it, which would lead to an analytically different argument. I therefore am not going to consider it further.

84. In my view the key question under Issue One is whether the ISA 2018 complies with the requirements of the 2018 Act. The balances that need to be made under the 2018 Act are themselves compatible with article 8(2) ECHR (and it is not suggested otherwise), so I cannot see that article 8 ECHR adds much if anything to the exercise,

save that the caselaw on article 8 emphasises the need to protection the rights of children.

85. Mr Metcalfe also relies on the UN Convention on the Rights of the Child. The rights and interests of children, and M in particular, need to be given great weight in the balance that is struck. However, there are no specific provisions of the UNCRC which add to that general consideration on the facts of this case. Therefore, as with article 8, although I have had regard to the UNCRC I do not think that it adds anything to the overall balance.

Conclusions on Issue One

86. It is clear that the burden of showing compliance with the 2018 Act falls on the Defendant, under s.34(2). Mr Gold argued that the approach of the Court should be that in *Gillick v West Norfolk Health Authority* [1986] 2 AC 112 and *Munjaz v Merseyside NHS trust* [2006] 2 AC 148, namely that the agreement is only unlawful where it would give rise to a serious risk of breach of the DPA 2018. However, it does not seem to me that that is the correct approach.

87. There is a requirement on the data controller to show compliance with the data principles, under s.43(3). Therefore there is a legal requirement on the controller to have in place a system with appropriate safeguards that meets the terms of the 2018 Act. That is not at all the same as a statutory scheme or test where there will only be a breach if there is a serious risk of the statutory duty being breached in any particular case. Of course it does not follow that to satisfy the statutory test there must be no risk of an individual breach ever occurring. But the statute itself incorporates the concept of safeguards, and an element of proportionality will apply when determining whether the safeguards are sufficient to achieve compliance with the 2018 Act. In my view trying to incorporate a *Gillick* type approach, by which there is only a breach of the Act if there is a serious risk of individual breaches occurring, does not accord with either the structure or the purpose of the Act.

88. There was a debate before me as to whether the Defendant remained the data controller of the information once it had been shared with the BCRP. Mr Metcalfe argued that BCRP was the data processor, acting on behalf of the Defendant. It seems to me that the much more natural reading of the situation was that the Defendant was initially the data controller, when it passed the data to BCRP, and then either they were joint data controllers, or BCRP became a data controller on its own. I note that the ISA 2018 describes the Defendant and BCRP as joint data controllers, and that appears to me to be correct.

89. However, I am not sure that this debate really matters. The Defendant is undoubtedly the data controller at the point that it passes the information about the individual to BCRP and as such the duties in s.32(2) apply to the Defendant.

90. As I have set out above the Defendant therefore has duties to implement the appropriate technical and organisational measures under Part 3 to ensure that the processing of the personal data complies with the requirements of Part 3 (s.56); to implement the data protection principles in an effective manner and the necessary safeguards (s.57(1); and that the measures under s.57(3) must ensure that "*personal data is not made accessible to an indefinite number of people…"* and finally that the

Defendant must ensure a level of security appropriate to the risks arising from the processing of personal data (s.66(1)). Mr Metcalfe argues that these duties have to be interpreted in the light of recital 50 of the Law Enforcement Directive, and in particular that the data controller must implement "*specific safeguards in respect of the treatment of personal data of vulnerable natural persons, such as children".*

91. He also argues, that all those duties have to be interpreted in line with the individual's article 8 right to privacy firmly in mind, and in particular the need to protect the article 8 rights of children. Ultimately, I have to reach a judgment as to whether the safeguards in place through the ISA 2018 are sufficient to meet the terms of the 2018 Act, and in particular to do so where sensitive personal data is being shared, and the interests of children are in issue.

92. The following issues arise in deciding whether the safeguards are sufficient to meet the statutory requirements, and to protect M's rights- (a) the nature of the data that can be shared under the agreement; (b) the provisions as to who it can be shared with and control over any onward sharing; (c) the requirements for the training and vetting of recipients of the data; and (d) the degree to which the specific interests of children are factored into the proportionality exercise. In deciding whether the sharing of information is proportionate I also have to take into account the reason or justification for the sharing. I will go through each of the factors I have identified in turn, and then reach a holistic view as to whether the safeguards are sufficient to meet the terms of the 2018 Act.

93. The first stage I have identified (a), is the nature of the information shared. Mr Gold says that under ISA 2018 the only information which can be shared is the name, date of birth; photographic image; address and offences against BCRP members. He takes this from Box J of the Legitimate Interest Assessment. This restriction on the data being shared is somewhat unsatisfactory. It is not set out in the ISA itself, nor in Appendix 4 of the ISA, which deals with the policy for processing the data of children. If the intention is, as Mr Gold says it is, no to longer share bail conditions, then it is surprising that this is not made express in appendix 4. The lack of clarity is exacerbated by the fact that Appendix 3, which covers how and what information will be shared and constraints thereon, says that bail conditions will be shared without any reference to the LIA. Mr Gold's argument is that in respect of children this has to be read subject to the LIA, but this is not at all clear from the documentation.

94. Mr Metcalfe argued that the safeguards must be set out in one document and therefore reliance on the appendices, let alone the LIA, was not permissible. I do not think this can be correct. Any references to one document, including a contract, must contemplate that such a document may have appendices or other documents incorporated by reference. However, seeking to apply the law in a realistic and effective manner and not an illusory one, if reliance is placed on a series of documents then they must be clearly referred to and accessible at the same time as the principal document. Otherwise any safeguard being relied upon which is set out in those documents will not work. In this case the fact that the limitation on the data is buried in a document to which there is only an opaque reference, and which is actually drafted to deal with a different legal situation (that of the GDPR), does not suggest that that safeguard alone in respect of the type of data to be shared is likely to be very effective, if at all.

95. However, taking the restrictions in the LIA at face value (i.e. excluding the bail conditions), the only sensitive personal data which can be shared is the photograph. According to the ISA, when images are taken the Defendant informs an individual that their image may be used, disclosed or retained. It is also relevant, though not in any sense determinative, that certainly in the case of M, her photo was already widely disseminated through BCRP's members' CCTV footage.

96. In my view the safeguards in respect of what data is shared are not alone sufficient to meet the requirements of the 2018 Act. However, that does not lead to the conclusion that the ISA 2018 breaches the 2018 Act, because it is necessary to consider all the various safeguards in a holistic manner.

97. The next stage (b) is with whom the data can be shared. 239 members of BCRP are currently entitled to have data shared with them. All decisions as to what data is shared are made by a senior officer of the Defendant. Once data is shared with members then safeguards are in place as to whom within those members has access to the data. Members have to sign the Data Integrity Agreement and confirm that they have read the relevant documents. The BCRP manager and relevant staff must be vetted to NPV2 level.

98. Any onward sharing (i.e. to members' staff) is the joint responsibility of the Defendant and BCRP as joint data controllers. For the Defendant's decision to share with BCRP to be lawful they have to be satisfied that BCRP has in place sufficient safeguards about onward transmission. In my view there are sufficient safeguards at this stage. The Code of Conduct only allows staff to access to data on a need to know basis. This, I accept is a somewhat crude safeguard because of the very wide element of judgement involved.

99. However, this leads directly to stage (c) and the training and vetting requirements for those who receive the data. All security staff have to hold licences from the SIA, and thus be DBS (Disclosure and Barring Service) checked. The reality of the data sharing is that the people who are most likely to be using the data, particularly the photo, are security guards employed by BCRP members, and it is therefore of considerable importance that there is a process of licensing and DBS checking them. If there were a case of inappropriate onward transmission of the data, or the individual using it in an inappropriate or unlawful manner, then that would be directly relevant to whether their SIA licence was revoked, or not renewed.

100. The data itself is placed on a secure intranet, which is encrypted and password protected. Of course I accept that these safeguards are not "water-tight", but considering them together with the nature of the personal data (including sensitive personal data) that is to be shared, I think they are proportionate. For the data sharing to achieve its purpose, i.e. for BCRP members to be able to use the information to prevent or limit unlawful or anti-social behaviour around their premises, employees have to have relatively easy access to the information. Therefore there must be a balance between the legitimate interest of public protection, and the dissemination of the data.

101. The next relevant stage (d) is the consideration of the specific interests of children and young persons. There are at least two reasons why particular consideration has to be given to the interests of children in the decision as to whether to share data. As a

matter of law the interests of children have a particular weight in any article 8 balance, ZH (Tanzania) v Secretary of State for the Home Department [2011] 2 AC 166. The evidence of M's mother makes clear the impact that sharing data can have on M's ability to get employment and to live a normal life for a teenager. There is also a very specific risk that sharing of data may expose M (and other children) to increased risk, for example of sexual exploitation. Even without any inappropriate data sharing on specific sexual exploitation concerns, if she is widely known to be subject to bail conditions and to have a certain profile, this could lead to increased risk. It is therefore of the utmost importance that the impact on children and young people is properly and fully considered.

102. Appendix 4 of the ISA is sensitive to the particular needs of children, and the relevant factors in terms of their interests, under a legitimate interest assessment. The balancing exercise set out within Appendix 4 is however focused on the decision as to whether or not to exclude, rather than the decision as to what sharing of data is appropriate once a decision to exclude has been made. In this regard the document could certainly do with more careful redrafting. However, it does set out the relevant factors, and it does albeit opaquely, send the reader to the Legitimate Interest Assessment document.

103. Mr Metcalfe placed considerable reliance on recital 50 of the LED and the reference to specific safeguards in respect of, inter alia, children. However, that is a recital rather than an article of the Directive and therefore is only an aid to interpretation, rather than a legal requirement. I certainly consider that there has to be a process by which the interests of children and young persons are specifically considered, but I do not think either the Directive or the 2018 Act requires specific separately listed safeguards for children.

104. Taking these matters together I have reached the conclusion that the ISA 2018, together with the appendices and the LIA, do provide sufficient safeguards and effective measures, including technological measures, to meet the relevant requirements of the DPA 2018. That is not to say that those safeguards could not be improved, particularly by clearer reference to the LIA, and some reframing of that document. However, I do not think those problems are sufficient to make the ISA itself unlawful. In reaching this conclusion I take into account the purposes of the ISA, which are public protection and the prevention of crime, and therefore the need for sharing with a fairly wide group, i.e. employees of BCRP. I also take into account the interests of children and young people, but take the view that so long as the nature of the data shared remains as in the LIA, and the safeguards exist as to onwards transmission, the sharing is proportionate.

105. The position in relation to the ISA 2017 is now academic in the sense that that Agreement has been superceded. I can therefore be very brief in respect of it. The legal position on compliance with the statutory tests is less clear cut because the safeguards are less clearly set out. Probably the most troubling element is that the bail conditions could be shared under that Agreement, whereas they cannot under the ISA 2018. Although I have found above that this was not a breach of the 1933 CYPA, that does not answer the data protection issue. There seems to have been limited consideration of the potential impact on children of sharing bail conditions with BCRP, and indeed unclear processes by which the specific interests of children were considered. However, the principal safeguards that I have referred to above were in

place under the ISA 2017, in particular the controls over what was shared, in what format, and over onward transmission. I therefore find that the ISA 2017 did not breach either the 1998 Act or the 2018 Act.

Conclusions on Issue Two

106. This Ground does not turn on an assessment of whether the ISA has sufficient safeguards to meet the legal requirements, but rather whether the specific incidents of data sharing between the Defendant and BCRP, in respect of M, were in breach of the DPA 1998 or the DPA 2018 (depending on the date of the specific sharing) and as such unlawful.

107. For the reasons that I have explained above it is not possible to be wholly confident as to what data has been shared with BCRP and at what date. There are five incidents of assault/affray, the last one of which took place on 7 June 2018 and therefore fell under the 2018 Act, details of which were shared. The Defendant also accepts it shared the Claimant's name, date of birth, photograph and bail conditions on four occasions. The Defendant accepted the photograph was biometric data and therefore sensitive personal data. There is a dispute as to whether information about M's vulnerability to child sexual exploitation was shared and a further dispute over whether sharing of bail conditions was lawful.

108. There are therefore four categories of information that were shared; (a) information about the various incidents; (b) the photo and other personal data; (c) information about vulnerability; and (d) the bail conditions.

109. The Defendant argues that the purpose of the sharing of the information is for the prevention of crime and the protection of vulnerable persons. They further argue that the Claimant could have had no expectation of privacy when she engaged in criminal or anti-social behaviour. I find the latter argument difficult to understand because the requirements under the DPA (both 1998 and 2018) are not removed by the fact an individual was guilty of a criminal offence, or antisocial behaviour.

110. In reaching a conclusion on issue two I have to consider what safeguards were in place to ensure that the data protection law was complied with, and then I have to consider whether the sharing that took place was lawful. I am concerned on the generic level that, as I have said above under Issue One, there does not appear to have been any clear process under the ISA 2017 by which the particular interests of children were taken into account. This may well explain why the Defendant changed its position on bail conditions, which I will refer to below, and why information on vulnerability seems to have been shared without any (or any evidence of) consideration of the potential impacts on the child.

111. In respect of the sharing of information about the various incidents I do not think this was unlawful. Firstly, it was not sensitive personal data. Secondly, the incidents were known to BCRP members in any event. Thirdly, the sharing of this information was plainly for a public protection purpose and was justified for that purpose.

112. I reach a similar conclusion in respect to the sharing of the photo, and other personal information. Although the photo is sensitive personal data, being biometric information, the reality of the situation is that the M's photo was on the BCRP

database in any event. There was a legitimate interest in the security guards employed by BCRP members having access to a clear photograph, and there were safeguards, similar to those in the ISA 2018, in respect of there being any onward transmission of the photograph.

113. In my view the position is different in respect of the information that was shared relating to M's vulnerability to sexual exploitation. The Defendant had strongly disputed that it had shared data stating that the Claimant was a person who is sexually vulnerable and/or at risk of sexual exploitation. However, this denial was difficult to accept in the light of two emails which have been disclosed. The first dated 3 October 2017 was in the context of a publicity for a missing person and refers to "intel for CSE risks" in respect of M. The second was dated 29 January 2018, was headed "Operation C" and refers to M, saying that a security guard had "raised issues around her vulnerability". It is not clear to me what had previously been disclosed about M's risk of child sexual exploitation and the parameters of Operation C, but the clear implication of the email is that those receiving it knew that Operation C was concerned with young people who were said to be vulnerable.

114. It is possible that the 29 January email is merely 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. However, putting the two emails together it is plain that the Defendant did give BCRP information about M being vulnerable and at risk of sexual exploitation. It is easy to see why this was of considerable concern particularly to the Local Authority, given that there is a very obvious risk that by sharing this information the police were exposing M to greater risk.

115. It appears that the two emails (and any other disclosures as to vulnerability) were in breach of the ISA 2017, i.e. they should not been shared under that agreement. It was only at the hearing that the Defendant accepted that such information had been shared. Further, as I have said this information was likely to put the Claimant at greater risk, and any benefit in such sharing might be limited. The Defendant may argue that they were seeking to protect M, but there is no evidence that the Defendant properly weighed up the impact on the Claimant of sharing this information, or whether there were sufficient safeguards to ensure against onward transmission. In particular there is no evidence that the Defendant addressed its mind to the particular importance of not sharing information of this nature about a child.

116. I therefore find that there was a breach of M's rights under the DPA 1998 by the sharing of information about her vulnerability and risk of sexual exploitation.

117. In respect of the sharing of the bail conditions. Having considered the caselaw referred to above, it is my view that the sharing with BCRP did not amount to sharing with "the public". The sharing is limited to BCRP members, in their capacity as members. All the employees who receive the information are doing so entirely in their employment (or contractual) capacity and subject to safeguards which limit its use to that within that capacity. In other words, they are not receiving it as members of the public, but as employees of BCRP and for the purposes of BCRP.

118. For these reasons I dismiss Issue One, and I find for the Claimant on only one part of Issue Two, namely the sharing of information that revealed her vulnerability to child sexual exploitation.