Information sharing agreement requirements under Part 3 of the Data Protection Act 2018 (R (on the application of M by her litigation friend, the Official Solicitor) v Chief Constable of Sussex Police)

29/04/2019

Information Law analysis: Matthew Holdcroft, barrister at Serjeants' Inn Chambers, considers the practical impact of the decision in R (on the application of M by her litigation friend, the Official Solicitor) v Chief Constable of Sussex Police which is the first substantive judgment in relation to information sharing under Part 3 (Law enforcement processing) of the Data Protection Act 2018 (DPA 2018) and also considered preceding laws under DPA 1998.

R (on the application of M by her litigation friend, the Official Solicitor) v Chief Constable of Sussex Police [2019] EWHC 975 (Admin)

What are the practical implications of this case?

Lieven J's judgment in *R (on the application of M by her litigation friend, the Official Solicitor) v Chief Constable of Sussex Police* is significant as it provides a broad outline as to the way in which the courts will interpret information sharing agreements (ISAs) under the regime governing law enforcement processing. DPA 2018, part 3 implemented the Data Protection Law Enforcement Directive 2016/680/EU (DPLED) into UK law.

Where a controller in circumstances similar to those in this case enters into an ISA with another body, care must be taken in relation to the preparation and operation of that agreement—in particular the controller must be aware that they are likely to be treated as joint controllers of the information disclosed and ensure they put in place ISAs that comply with their obligations under data protection laws.

LexisNexis practical point: However, it is not enough for controllers to put in place a compliant ISA—they must also ensure they implement the necessary processes to ensure those agreements and the underlying data protection obligations are complied with. In this case the ISAs were found to comply with data protection laws but the defendant was found in breach of data protection law because of a disclosure which occurred in breach of an ISA. While this case did not involve consideration of data sharing under the general data protection regime established by the General Data Protection Regulation (EU) 2016/679 (GDPR) this general point is a useful reminder for compliance with both regimes.

In cases such as this, as a minimum the ISA must, for example:

- set out with clarity the type/nature of information that may be shared under the ISA
- strictly circumscribe the circumstances in which sharing may take place, ie the legitimate interest in sharing should be easily discernible
- identify, so far as possible, the persons who will have access to the information, eg by role, and the professional requirements that those individuals should possess (eg a vetting level or confirmation of a valid Disclosure and Barring Service check or the completion of specific training)
- specify a process whereby the persons who may access the information must confirm that they have read, understood and agreed to the terms of the ISA (this should be recorded and capable of being evidenced)
- set out the minimum-security storage requirements
- restrict, so far as is possible, the onward disclosure of the shared information and the internal use to which the information is put

- be clear as to the circumstances in which onward disclosure may be permitted which must be as restrictive as possible
- ensure that only minimal information is shared allowing for the legitimate interest underpinning the ISA to be met and no more
- be self-contained and easily navigable—if reliance is placed on a series of documents they must be clearly identified and accessible
- ensure that particular consideration will be given to the interests of the vulnerable, eg children

Consideration should be given to indemnities in any such ISA.

What was the background?

The claimant challenged the defendant Chief Constable's decision to share information with a private body, the Business Crime Reduction Partnership (BCRP), which is composed of over 500 members, including a large number of local businesses comprising retailers both local and national and a number of private security firms, pubs, bars and nightclubs. The principal aim of the partnership is the efficient management of its members' exclusion scheme (the scheme), prohibiting persons from entering its members' commercial premises. The contractual nature of the scheme meant that its members should not be regarded as 'members of the public'. The BCRP shares information that relates to excluded individuals amongst its members via a secure intranet and mobile app.

The claimant argued that:

- the ISAs failed to provide sufficient safeguards as required by applicable data protection law to prevent the unlawful processing of the claimant's sensitive personal data
- there had been an unlawful and disproportionate disclosure of the claimant's sensitive personal data

The claimant is a vulnerable 16-year-old girl. She has convictions and a history of going missing and engaging in anti-social behaviour—the defendant had recorded over 50 incidents relating to her since October 2017. She was made the subject of an exclusion order under the scheme in November 2017.

Due to when the relevant events had occurred, the case encompassed claims under both the DPA 2018 and the preceding DPA 1998. The court was also called to consider both a preceding ISA (ISA 2017) and an updated ISA that had been introduced in December 2018 to address DPA 2018, Part 3 (ISA 2018).

One of the disclosures complained of was that in October 2017 (when the DPA 1998 applied), the defendant emailed the BCRP to report that the claimant was missing, stating that 'it was concerning due to the company she is now keeping XXX, [the claimant] whom both have intel for [child sexual exploitation] risks.' The BCRP replied to the email, stating that it would, 'distribute to members via our website.'

What did the court decide?

Lieven J concluded that the ISA 2018, together with its numerous appendices and supporting documents, did provide sufficient safeguards and effective measures, including technological measures, to meet the relevant requirements of DPA 2018. A similar conclusion was reached regarding the ISA 2017. However, she also found that the disclosure that the claimant may have been at risk of sexual exploitation was unlawful—the question of remedy remains outstanding.

Importantly, Lieven J held that it was for the defendant to prove that the ISA 2018 complied with DPA 2018 rather than the claimant having to prove that it did not. She further stated that DPLED was only relevant to the case insofar as it aided the interpretation of DPA 2018, Part 3 (since no suggestion was made that DPLED had been incorrectly transposed).

The judge rejected most claims that certain specific incidents of data sharing were in breach of DPA 1998 or DPA 2018 (as applicable). However, she found that the disclosure in 2017 that the claimant may have been at risk of sexual exploitation was unlawful under DPA 1998—the question of remedy remains outstanding.

She added that there should be a clear process under the ISA that takes into account the particular interests of the vulnerable.

Interviewed by Kate Beaumont.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor.