Hopkins v HMRC UK Court Ruling on Lawful Processing of Data (including Criminal Offence Data) & Disciplinary Proceedings

Date : September 17, 2020

Introduction

In the recent case of Kathryn Hopkins - v - The Commissioners for her Majesty's Revenue and Customs (HMRC) the UK High Court dismissed (on procedural grounds) legal action brought by an individual against their employer for various alleged data protection legislation breaches, finding that HMRC had acted lawfully in all but one of the claims. This brief article highlights certain issues in the case.

What's the case about?

The background is as follows:

- The claimant is a civil servant employed by HMRC;
- The claimant was arrested by the police in mid-August 2018 and in accordance with her contract of employment she disclosed the arrest to her employer. She was then suspended on full pay by HMRC pending disciplinary proceedings for possible gross misconduct with dismissal as a possible outcome. Over two years after the arrest the claimant had neither been charged with any offences nor had she been notified that the police investigation was closed. At the time of the judgment in this case HMRC had not formulated any disciplinary charges and the claimant remained suspended;
- The primary focus of the claim was the claimant's concern regarding the processing of her personal data, including criminal offence data, and the way in which the ongoing disciplinary proceedings had been handled. The claim also raised a number of other causes of action but these are not dealt with in this article which only focuses on the court's decision in relation to alleged breaches of the EU General Data Protection Regulation (GDPR) and the UK's Data Protection Act 2018 (DPA 2018);
- The claimant also brought a complaint to the UK's Information Commissioner's Office which concluded that, based on the information provided to it (which was less than what went before the court), it was likely that HMRC had complied with its data protection obligations.

What did the court rule?

In a lengthy and detailed ruling the court decided the following:

Concerning the claim for breach of contract alleging that the requirement for the claimant to provide information upon arrest was contradictory to HMRC's policies on the use of staff criminal offence data outlined in HMRC's privacy statement, the court ruled that the contractual obligation to inform HMRC was consistent with the terms of HMRC's Staff Privacy Notice: "It is made clear that criminal offence data may be processed in various circumstances, including in the exercise of HMRC's employment-related rights (such as to investigate potential misconduct and undertake disciplinary proceedings) and in the exercise of HMRC's legal obligations […]". The claimant also separately claimed that the contractual requirement to provided arrest information and information ancillary to the arrest was in breach of GDPR but this too was dismissed by the court (on the same lines concluded by the court in point (b) below);

Concerning the claim that the processing of the claimant's personal data from August 2018 onwards was unlawful under GDPR and the DPA 2018, twenty separate breach allegations were made. These were all dismissed by the court except for one. Key points are as follows;

- **Claim:** The police were the data controller of the information in question and HMRC was the data processor;
- **Court ruling:** It was "plain" that HMRC had determined the purposes and means of processing the claimant's personal data and so HMRC was therefore the data controller: "When instituting the disciplinary

proceedings, suspending the Claimant, handling her grievances and responding to her complaint to the ICO and this claim, HMRC, as the Claimant's employer, has processed her personal data on its own behalf, not on behalf of Merseyside Police.[…] The suspension and disciplinary investigation were matters for HMRC, not Merseyside Police";

- **Claim:** HMRC had no lawful basis for processing the claimant's personal data for the purposes of suspending the claimant or instituting disciplinary proceedings – HMRC breached the GDPR principles of data processing;
- **Court ruling:** HMRC could lawfully investigate conduct that was alleged to have taken place outside the workplace and the processing met the requirements of GDPR and DPA 2018 concerning processing in connection with performance of the complainant's employment contract;

- **Claim:** HMRC breached the GDPR principles of data processing in the various ways that it shared the claimant's personal data, e.g. within HMRC with HR and the press office;
- **Court ruling:** The processing of personal data for the purposes of the disciplinary investigation were not unlawful and so the data-sharing claims had no realistic chances of succeeding. See for example: "The nature of the offences for which the Claimant was arrested was such that there was a clear business reason to brief HMRC's press office in order to ensure that if the allegations against the Claimant entered the public domain the press office would be ready to respond, if necessary. The need for HMRC's press office to be briefed was heightened by the press interest in a separate claim that the Claimant brought against a different government department. The Claimant's concern regarding the sharing of her personal data with HMRC's press office appears to reflect a view that this was tantamount to disclosing it to the press, whereas that is plainly not the case";

- **Claim:** HMRC failed to securely process the claimant's personal data when it sent a particular letter to her notifying her of HMRC's investigation;
- **Court ruling:** There was no basis to claim that the use of Recorded Delivery service to send the letter failed to provide an appropriate level of security, in breach of GDPR security requirements: "The letter […] to the Claimant, notifying her of the investigation, was sent by Recorded Delivery, which had the effect that its delivery was tracked, and it needed to be signed for on delivery. It was sent to the Claimant's last recorded address and, before it was sent, the Claimant's line manager contacted her to explain how the correspondence would be sent. The Claimant was not present to sign for it when delivery was first attempted so the letter was held at the Post Office for her to collect, which she did about a week later. […] In accordance with the disciplinary procedure and policies, HMRC had to send the letter notifying the Claimant of the matters which it was investigating. […] Nor is there any alleged loss given that sending the letter by Recorded Delivery did not, in fact, result in any accidental loss or inadvertent disclosure of the Claimant's personal data";

- **Claim:** Some data processing information had not been provided by HMRC in response to various requests by the claimant;
- **Court ruling:** Information does not need to be provided where a data subject already has the information, in accordance with GDPR;

- **Claim:** A letter to HMRC from the claimant requesting the claimant's suspension and the disciplinary investigation "to be halted" invoked rights under GDPR (the right to restriction of processing & the right to

object to processing [on certain grounds]) which had not been complied with by HMRC;
- **Court ruling:** The letter was neither a GDPR notice of objection nor a GDPR request to restrict processing as the claimant had not stated that she was making requests under the GDPR rights articles in question nor had she specified any of the grounds as a basis on which those rights could be relied on. In any event, HMRC was processing the claimant's personal data for the purposes of the disciplinary investigation on a GDPR legal basis which was not relevant for the purposes of a GDPR objection request;

- **Claim:** HMRC had failed to respond to a Subject Access Request in the required time period;
- **Court ruling:** This claim was upheld.

What are the takeaways?

HMRC would appear to have put into practice data protection compliance that in part at least fended off this litigation. Having in place good employee privacy notices, policies and processes, and identifying the proper lawful bases for data processing clearly pays off, including where aggrieved employees are litigious and bring "everything but the kitchen-sink" type of claims (or as the judge more judicially put it, allegations that have no "cause of action" or are "unparticularised"). This case therefore serves as a reminder to organisations to consider ensuring that their data protection compliance house is in order, for example by undertaking an internal audit.

Data protection breach claims seeking compensation are becoming more and more common – we have written about these claims in general here https://www.corderycompliance.com/data-protection-breaches-and-compensation-litigation-issues-for-consideration/.

Cordery's GDPR Navigator includes resources to help deal with data protection compliance. GDPR Navigator includes:

- guidance on handling requests from data subjects and;
- template and;
- procedures.

For information about our Breach Navigator tool please see: https://www.corderycompliance.com/solutions/breach-navigator/

We report about data protection issues here: http://www.corderycompliance.com/category/data-protection-privacy/.

For more about GDPR please also see our GDPR FAQs which can be found here: http://www.corderycompliance.com/eu-data-protection-regulation-faqs-3/ and our Data Protection Glossary which can be found here: http://www.corderycompliance.com/?s=glossary.

The court's judgement can be found here: https://www.bailii.org/ew/cases/EWHC/QB/2020/2355.html

For more information please contact André Bywater or Jonathan Armstrong who are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringd Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com