

Driver v CPS – damages in data breach claims – an imprecise science?

The High Court has handed down judgment in the case of *Driver v Crown Prosecution Service* [2022] EWHC 2500 (KB) (“*Driver v CPS*”).

For those familiar with data breach claims, one of the more difficult questions to answer in recent years is the bottom line – what amount will a Claimant be awarded in damages?

While on an individual case-by-case basis the impact may not be significant, at scale, the amount each Claimant may seek to recover from a Defendant is of importance.

The judgment in *Drive v CPS* is of significance for this question of compensation following data breaches. In short, the Claimant was awarded £250 for their data breach claim. It is therefore useful in that it offers some contribution to the limited line of reported authority in this area.

Facts

Mr Driver is a well-known figure in local politics. In 2014, he was a suspect in a police investigation into local government corruption (“Operation Sheridan”). In March 2016 Mr Driver was informed that he was no longer a suspect. Mr Driver made press statements to that effect.

However, following being informed that he was no longer a suspect, and making those aforementioned press statements, Mr Driver became the subject of investigation again under Operation Sheridan. A file relating to eight individuals (including Mr Driver) was passed to the CPS.

For various reasons explored in the judgment, the Court noted that “*there was plenty of material in the public domain linking [Mr Driver and others] to Operation Sheridan and stating more or less in terms, that the police file [had] been sent to the CPS in August 2018*”.

On 1 May 2019, a member of the public made an enquiry to the CPS (the “Third Party”). The Third Party was described in the judgment as a political opponent of Mr Driver. In response, on 5 June 2019, a CPS official sent an email (the “Email”) that did not name Mr Driver but stated:

“A charging file has been referred from the Operation Sheridan investigation team to the CPS for consideration.”

The Third Party then communicated the contents of the Email together with his own commentary, which included naming Mr Driver, to a number of further individuals. There was no evidence, however, that anyone read the Email or acted further upon it.

Mr Driver, however, brought a claim on the basis that the Email had caused him distress.

Judgment

Mr Driver brought a claim against the CPS with the following causes of action:

- breach of the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016) (the “GDPR”) or in the alternative for breach of the Data Protection Act 2018 (the “DPA 2018”);
- misuse of private information (“MPI”);
- breach of the Human Rights Act 1998 (the “HRA 1998”). An extension of time was necessary for the human rights claim; but
- a pleaded claim in negligence was not ultimately pursued (presumably for the reasons covered in our blog post on [Warren v DSG Retail Ltd \[2021\] EWHC 2168](#) in that there is no duty of care in negligence in respect of conduct covered by the data protection legislation).

GDPR or DPA 2018 claim

The Court held that Mr Driver’s claim was not a GDPR claim, but that it instead fell within the law enforcement provisions of the DPA 2018. The making of a statement about charging constituted processing for law enforcement purposes within the meaning of section 31 of the DPA 2018 (see paragraphs 89 and 90).

What personal data?

As set out above, the Email did not in fact name Mr Driver. While a group of individuals was referred to, and not one individual, the Court held at paragraph 101 that “[p]ersonal data can relate to more than one person and does not have to relate exclusively to one data subject, particularly when the group referred to is small.” This conclusion was reached on the basis of the approach set out in a number of authorities including *Ittihadieh v 5-11 Cheyne Gardens RTM Co Ltd* [2017] EWCA Civ 121 [2018] QB 256 (see paragraphs 61-66), which is sometimes referred to as the ‘obviously about’ approach. Essentially, Mr Driver could be identified.

Was there a data breach?

Before litigation was afoot the CPS admitted that the sending of the Email constituted a data breach. At trial, CPS argued that no data breach took place. This argument was rejected on the basis that there was no necessity to update the Third Party and therefore there was no lawful processing condition that could be relied on (see paragraph 116).

Claim for MPI

Mr Driver’s claim for MPI failed. The judgment contains a helpful summary on the relevant authorities (see paragraphs 126 to 147). In short, Mr Driver had no relevant expectation of privacy in respect of the statement that revealed the fact that the CPS had received and was considering a “charging file” because those facts were already in the public domain. As stated at paragraph 156 “... *this was a very limited disclosure to people who were, I find, overwhelmingly likely already to have known what the situation was, because of earlier widespread reporting. The CPS email therefore added little or nothing to that which was already known...*”

Remedies

The Court made a declaration and an award for damages. It is the latter point which is of interest.

There are limited useful authorities on the question of what amount a Claimant may recover in a data breach claim. The judgment itself notes at paragraph 166 that Counsel had acknowledged that there are limited reported cases on

quantum in data protection cases and that assessing damages in this area is not “an exact science”.

While there has been much discussion recently on the grounds that a Claimant may pursue in the event of a data breach (see for example our case note on *Warren v DSG Retail Ltd* [2021] EWHC 2168) and the prospects of bringing a representative action (see for example our case note on *Lloyd (Respondent) v Google LLC (Appellant)* [2021] UKSC 50) there has been little commentary on the figure that a Claimant will be awarded.

Mr Justice Knowles did not find Mr Driver’s evidence of distress particularly compelling. At paragraph 168 Mr Justice Knowles held:

“I am prepared to accept that the Claimant would have experienced a very modest degree of distress upon discovering that the CPS’s email had been sent to political opponents and the media by someone who had a grievance against him in an effort (as I find) to embarrass him. But for the reasons I have given I reject his evidence that it represented some fundamental sea-change in the complexion or likely outcome of Operation Sheridan, such that it could reasonably or properly have caused him anything like the level of anguish which he claimed...”

The judgment goes on to note at paragraph 169 that “[g]iven all of the circumstances, I consider that this data breach was at the lowest end of the spectrum. Taking all matters together in the round, I award the Claimant damages of £250”.

Conclusion

While the decision provides some useful guidance on what sum a Claimant might recover in a data breach claim on the “lowest end of spectrum” it does not offer guidance on what a claimant may recover where more extensive or sensitive personal data is the subject of the dispute. The data at the heart of this dispute was limited and did not relate to more personal or indeed sensitive data that are often the subject of data breach disputes.

Furthermore, as is apparent from the comments made by Mr Justice Knowles, Mr Driver did not offer particularly compelling evidence of the distress he had suffered. While this is a point that future claimants might improve on, it is interesting to note that Mr Justice Knowles added that he was not convinced that a “sea-change in the complexion or likely outcome of Operation Sheridan” had occurred “such that it could reasonably or properly have caused [Mr Driver] anything like the level of anguish which he claimed”. Therefore, the conclusion was not just based on Mr Driver’s evidence (or lack of compelling evidence) but also the degree to which such anguish could reasonably or properly have been caused by the breach.

Another point that *Driver v CPS* does not offer much assistance on is the scenario where a data breach claim arises out of a more complicated set of circumstances, for example a cyber-attack. The questions surrounding the data breach itself in *Driver v CPS* were factually quite straight forward and the ramifications of that data breach were more straightforward than where, for example, a third party has gained access to a database and it is not clear to what degree data has been made available to further third parties or is published on the dark web.

Setting those questions aside, the judgment does provide some useful guidance that, at least in a case involving limited personal data and limited distress being suffered, £250 may be an appropriate figure or starting point. This is in contrast to an award for thousands of pounds, which claimants often allude to in correspondence or even at the pleadings stage. Indeed in *Driver v CPS*, the claim was pleaded at damages not exceeding £2,000. The case therefore offers at least some guidance on the vexed question of “how much?”

Rebecca Keating

[Read the full judgment here](#)