Data protection claims - UK

By

Marc Dautlich

Bristows LLP
100 Victoria Embankment
London
EC4Y 0DH

Since the introduction of the GDPR in the European Union in 2018 (from which the UK has subsequently withdrawn, while maintaining its own version of the GDPR, known as the UK GDPR, in substantially the same form), data protection litigation has been a focus area for claimant law firms in the UK. Data controllers have consequently been required to fend off all manner of claims pleaded in data protection, arising from security incidents but also arising more broadly under the numerous other rights conferred on individuals (known as data subjects) under the UK GDPR.

At one end of the spectrum, there has been a surge in claimants seeking compensation in the hundreds or low thousands for minor breaches of the legislation. At the other end, representative/group actions have sought billions from the largest firms in the tech industry. That said, welcome relief for data controllers at both ends of the spectrum began to emerge in the early 2020s with a clear narrowing of the litigation risk, as a result of a number of judgments which saw the UK courts come to the aid of defendants. This is, however, by no means the end of the story; claimants, funders and other stakeholders in this area are too invested to give up on such claims. Instead, they are increasingly resorting to novel ways to pursue these claims.

As a result of the court decisions referred to, it is now less financially viable for claimants in UK proceedings to bring low-level data protection claims. For example, the UK courts have decided that, generally, low-value claims do not belong in the High Court but rather in the County Court, probably the Small Claims Track (**SCT**). In the SCT, the ability to recover costs is very limited. As a result, such claims are generally no longer as financially viable, and have been decreasing greatly in number. In addition, the scope for bootstrapping claims for the common law tort of misuse of private information (**MOPI**) to data protection claims under the UK GDPR, in order to recover ATE insurance premiums – which are not recoverable for data protection-only claims – seems to have been narrowed. This is because MOPI claims require 'misuse' in some form by the defendant. Where, however, by way of example, the defendant has been the subject of a cyber-attack, 'misuse' of private information by the defendant is generally not in scope and a MOPI claim will accordingly fail.

In short, for the reasons above, there has been a marked drop-off in the number of low-value data protection claims issued in the High Court. Developments in data breach claims at the other end of the spectrum have also favoured data controllers. In *Lloyd v Google*, the UK's Supreme Court rejected the notion that compensation could be awarded for the mere "loss of control" of personal data. The term "loss of control" used in the statute gave claimants hope that they could claim compensation for all manner of scenarios where a 'loss of control' of data by a controller could be said to have occurred. The *Lloyd v Google* decision, based on the pre-GDPR legislation, means that the represented class could not be said to have "the same interest", so making representative actions very challenging. The Supreme Court did suggest that a two-stage approach could work (liability first, with quantum sought on an individual basis second). This approach, however, seems to be uneconomical for funders, judging by the lack of such claims being brought. Many group/representative actions that had been paused pending the *Lloyd* decision have since been abandoned.

Collective actions in the UK based on data protection are currently very much on the ropes. They are expensive, cumbersome to run at scale and face major procedural and/or administrative obstacles, whether brought as representative actions or group litigation orders. That said, it is doubtful that the threat to controllers has been seen off for good. There have been renewed calls for the Government to introduce legislation to put collective actions in this area on a firmer footing (even though the Government decided not to do so last time it looked at the issue, in 2021).
There will also inevitably be more large scale and serious data breaches in future. Since the UK data protection regulator, the Information Commissioner's Office, has no powers to award compensation to affected individuals following a data breach, expect claimants, their lawyers and funders to find novel ways to bring claims for such compensation. The prize for these stakeholders is too great for them to give up for the time being.