UK data protection litigation — a burgeoning market that needs rebalancing

Ashley Hurst, Partner, and Jamie Halpin, Senior Associate, with Osborne Clarke, explore the boom in data protection litigation in the UK

Since the GDPR came into force in 2018, there has been a dramatic upsurge in data protection litigation in the UK. What could be the cause of this change? Do data subjects really now care more about their personal data than they used to? Or is it because claimant lawyers now have a much better understanding of a previously niche area (and the money they can make from it)? Or could the rise be due to regulators throwing their weight around more?

The answer is probably a combination of all of these factors. What is clear is that data protection litigation is here to stay. The long-standing EU law principle of proportionality appears to be taking a back seat as litigation funders and entrepreneurial law firms seek to capitalise on contraventions of the GDPR by controllers and processors.

In this article, we take a look at some of the trends, cases and dynamics that are shaping this complex market.

Data protection group actions

Group Litigation Orders:
Following the implementation of the GDPR, there has been a dramatic rise in the number of data protection claims being issued in the UK High Court. Whilst many of these cases are low value and more suitable for the small claims track in the County Court, some of them are being consolidated by group litigation orders ('GLOs'). The cases relate to a variety of alleged breaches of the GDPR, including lack of transparency, processing without consent, and perhaps most commonly in post-data breach cases, failure to take 'appropriate technical and organisational measures' to protect personal data.

In one threatened group litigation case, hundreds of footballers publicly announced their intention to take legal action against a variety of gaming, betting and data-processing companies that allegedly used their personal data without their consent (or without providing them with compensation). Their claim potentially includes a claim for alleged loss of earnings stretching back six years. The claim, dubbed 'Project Red Card', is led by the Global Sports Data and Technology Group, an entity that clearly intends on profiting from data privacy litigation, describing data as "the new oil of the world" in its website." If these footballers and their representatives decide to bring a claim, they will need to consider whether to bring one or more test cases which can be managed together, or bring multiple claims and seek a formal GLO.

A GLO may be granted where the claimants are able to demonstrate that they have 'common or related issues of fact or law'. The procedure is intended to allow the Court to manage the claims in an efficient and orderly manner, often by managing claims in several waves.

Unlike Project Red Card where financial losses are likely to be claimed, in the vast majority of group data protection claims, the claimed damages per person tend to be very low (limited to non-pecuniary damages) and the likely damages awarded even lower. What makes these cases interesting to claimant law firms and litigation funders is not the size of the damages per case, but the number of claimants and the legal costs that can be recovered in successful claims. Many of these firms learned their trade in personal injury litigation where, prior to recovery of success fees and ATE (after the event) premiums being abolished, personal injury lawyers could rack up considerable costs before the defendant's insurers could consider settlement.

If a claimant law firm manages to pull together 10,000 clients with a strong claim on the merits, and each is awarded £1,000 in compensation, the damages pot is £10m — enough to wipe out many small businesses. Adding on the legal costs, of which 60-80% are usually recoverable on success in High Court litigation, and the numbers start to get very substantial indeed. The legal costs will dwarf that amount if the claims are allowed to proceed in the High Court where successful claimants can typically recover 60-80% of their costs if successful.

On this model, even if only one claim is litigated as a test case and the rest then settle, the claimant law firm is

likely to claim well in excess of £1,000 per client in legal fees. If a firm can run these cases with limited overheads and low cost paralegals, backed by an ATE insurer in case they lose, it is not hard to see why so many former personal injury firms are turning to this model.

Representative actions: An even more alarming form of group action now being faced by controllers is the 'representative action', where a single individual brings a claim as a representative of all the other individuals who might be able to bring a claim.

In order to bring a representative action, the representative will need to demonstrate that he/she and the represented parties all have (1) a common interest; (2) a common grievance; and (3) a remedy which would benefit all of those in the represented class.

The much hyped *Lloyd v Google* [2019] EWCA Civ 1599 case (currently awaiting judgment from the Supreme Court on whether it can proceed) is a representative claim. Rather than seeking damages for distress — something that is very subjective and will vary from claimant to claimant — Mr Lloyd's claim is for damages in respect of the 'loss of control' of the claimants' data. This concept is recognised in the GDPR and also in the phone-hacking litigation brought against Mirror Group Newspapers. However, it has developed a life of its own in the data protection context thanks to some creative claimant lawyers, who have argued that the simple fact of losing control over one's data is worthy of compensation, provided the so-called 'minimum threshold' is met.

The Court of Appeal surprisingly agreed, much to the excitement of the claimant data litigation market, who immediately started eyeing up multi-million pound claims against multi-national companies, most of which are proceeding very slowly until the outcome of the *Lloyd* case is known. The Supreme Court heard the arguments in the case on 28th and 29th April 2021. If the appeal is rejected, we are likely to see an increase in US-style class actions against multi-national companies and the kind of eye-watering financial exposure that will be uninsurable. If the appeal succeeds, we may well see a rejection of 'loss of control damages' as the basis for a representative action in data protection claims, which will mean some claimant law firms and litigation funders will need to re-think their business models in relation to data protection litigation.

> ***"The importance of the Warren case cannot be underestimated, as it makes it highly unlikely that claimant firms will be able to recover ATE (after the event) premiums from the defendant if they win."***

The controller fight-back: Notwithstanding the uncertainty over the *Lloyd* case, controllers are starting to fight back against the gravy train for this new breed of claimant data protection lawyers.

Claims of this nature tend to be brought by law firms on a 'no win, no fee' basis and with the benefit of insurance to cover any adverse costs order that may be awarded. One of the key features of these claims is that claimants tend to bring claims for 'misuse of private information', breach of confidence, and negligence alongside their claims for alleged breach of data protection legislation. They do so in order to increase their prospects of recovering their ATE insurance premiums if they win (ATE premiums can be recovered in misuse of private information claims, but not data protection claims), and because breach of confidence claims must be issued in the High Court.

However, in the recent case of *Warren v DSG Retail Limited* [2021] EWHC 2168, the High Court struck out several low value claims which had been issued against DSG Retail Limited (Dixons Carphone) following a publicised cyber-attack on the retailer in 2017-18. In doing so, the Court held that there was no claim for breach of confidence, misuse of private information, or negligence in circumstances where the controller had been the victim of a cyber-attack and had not committed a positive act in relation to the compromised personal data (which was little more than basic contact information). The judge also transferred the case to the County Court, where costs recovery is typically much more limited.

The importance of the *Warren* case cannot be underestimated, as it makes it highly unlikely that claimant firms will be able to recover ATE premiums from the defendant if they win this type of case. Such premiums can be very substantial, especially as the risk increases close to trial. If the claimant law firms are forced to pay those premiums themselves, the economic viability of bringing group data litigation claims will be severely challenged.

Assessing damages for distress

As the data litigation market matures in the UK, the question of the appropriate level of damages where the minimum threshold is met will become more settled. At present, the uncertainty in quantifying claims means that claims which should either be struck out or settled early are progressing.

Prior to the GDPR coming into force, the high profile case of *Vidal-Hall v Google* [2015] EWCA Civ 311 established that damages were available for distress in data protection claims and this has been cemented into the GDPR (and UK GDPR). However, the reality is that the question of distress is very subjective. While some individuals are protective of their data and spend time opting out of emails and cookies and applying stringent privacy settings, others adopt a laissez-faire approach and are relaxed about their data being shared and posted liberally on social media without ad-

(Continued on page 10)

(Continued from page 9)

justing their privacy settings. Unsurprisingly, many of the individuals that bring data protection claims usually claim to be very protective of their privacy. Some of them also appear to be extremely susceptible to distress, sleepless nights, and sometimes illness as soon as their email address goes missing in a data breach.

Gaining clarity as to how to assess damages will be important to allow genuine cases to settle early. As explained above, legal costs of litigation usually far exceed the difference between what the claimant is claiming and what the defendant is prepared to pay.

In an important data protection claim in the UK, *Aven and others v Orbis Business Intelligence Ltd* [2020] EWHC 1812 (QB), the claimants were awarded £18,000 in damages after it was found that their sensitive data were processed unlawfully. Having determined that the claimants had suffered distress and reputation damage, the Court decided that damages should only be modest on the basis that the claimants were of a 'robust character'. Damages could have been higher had the claimant been of vulnerable disposition (damages for distress are not capped under the Data Protection Act 2018).

However, the *Aven* case is not typical — it was more like a libel case in that damages were principally awarded for reputational harm in relation to a false allegation concerning delivering illicit cash to President Putin. By contrast, in the cases that usually follow cyber-attacks, there is often no convincing evidence that the personal data in question have been misused to the detriment of the claimants, such that it can often be argued that the minimum threshold for damages has not been met.

The minimum threshold for data protection claims is now a well-established principle, as was accepted by the Supreme Court at the hearing in *Lloyd.* But where exactly it sits is still a matter of considerable debate. Does, for example, a certain amount of distress suffered by an individual on discovering that he/she has been the victim of yet another data breach and now needs to change his/her password as a precaution exceed that threshold?

There is a line in the Court of Appeal judgment in *Lloyd* indicating that damages should not be paid in relation to "one off data breaches that are quickly remedied". This appeared to put some relevance on the extent of culpability of the controller rather than simply the damage suffered by the data subject. However, the law is far from clear on this point.

In time, we may well see a tariff being developed much like in the personal injury market (e.g. £1,000 for loss of password data, £2,000 for full credit card details, etc.). However, such a system would need to retain some flexibility and, crucially, be clear on where the minimum threshold sits for when compensation is payable at all.

Impact of adverse regulatory decisions

Another major dynamic in data protection litigation is the position adopted by regulators. An adverse finding by a Supervisory Authority can make defending follow-on damages claims much more difficult, at least on the question of whether the GDPR has been breached.

After a steady start and despite a period of leniency during the pandemic, the UK Information Commissioner's Office ('ICO') is starting to flex its muscles. On 16th October 2020, the ICO fined British Airways £20m (reduced from an initial intention to fine £183m). While this is still the largest fine that the ICO has ever levied, it announced that "the economic impact of Covid-19 had been taken into account".

In the same period, the ICO also released penalty notices in relation to Marriott International (£18.4m) and Ticketmaster (£1.25m). In all three instances, the ICO found that the occurrence of a cyber-attack or personal data breach did not necessarily mean that there has been a failure on the part of the company. However, in each case, multiple failures were found, and it is clear from the lengthy decisions that multi-national companies are going to be held to very high standards of data security. Litigation against British Airways has subsequently settled — perhaps an indication of the difficulty in contesting liability once the ICO has thrown the book at the company.

Ironically, whilst adverse decisions by regulators make follow-on litigation much easier for claimant law firms, it also means that they are less likely to be contested in full and require expert evidence on technical issues. If liability is accepted, the claims could be pushed to the small claims track of the County Court for a simple assessment of damages in each case. Given the inability to recover costs in the small claims track, such cases might not be so attractive to the claimant law firms looking to make millions from litigating low value claims.

Data Subject Access Requests in the context of litigation

Finally, it's worth mentioning the explosion in Data Subject Access Requests ('DSARs'), as this is where many data protection cases start. Whilst many DSARs are made in a genuine attempt to understand more about data processing, the system is open to abuse. Many DSARs are submitted either as a fishing expedition for documents that may assist litigation (such as an employment grievance claim) or to gain leverage in a dispute given the administrative burden created by such requests and the potential sensitivities over certain disclosure.

There is some protection built into the UK GDPR and Data Protection Act 2018 to ward off the possibility of abusive DSAR requests. Searches for responsive personal data need only be 'reasonable and proportionate' and controllers can refuse requests that are 'manifestly unfounded or excessive' (Part 3, section 53), an issue that the ICO has provided guidance on. However, these provisions are often difficult to apply in practice if the DSAR's are framed cleverly by claimant lawyers.

The decision of the High Court in *Dawson-Damer v. Taylor Wessing*

LLP [2020] EWCA Civ 352 confirmed that a data subject's motive in submitting a subject access request is irrelevant and that evidence must be provided by a controller in order to rely upon the 'disproportionate effort' limitation in relation to the controller's obligation to search for personal data. This has since been adopted by the ICO in its guidance, which confirms that the UK GDPR 'places a high expectation on you to provide information in response to a SAR' and states that 'you should make reasonable efforts to find and retrieve the requested information.' Organisations therefore need to develop smart and efficient procedures as well as understanding when Supervisory Authorities will likely intervene.

Conclusion

To sum up, the data protection market is going through a turbulent time. There are many uncertainties, most of which do not tend to favour controllers and are being capitalised on by claimant law firms developing a new volume-based business model.

However, the realities are dawning on regulators and the courts and it is only a matter of time before the scales are rebalanced and a sense of proportionality is restored.

Ashley Hurst is speaking on 'Data Protection Litigation — a Greater Threat than Actions from Regulators' at the 20th Annual Data Protection Compliance Conference, taking place in-person and virtually on 7th and 8th October 2021. See www.pdpconferences.com for further details

Ashley Hurst and Jamie Halpin
Osborne Clarke
ashley.hurst@osborneclarke.com
Jamie.halpin@osborneclarke.com