GDR NEWS

Riding the tidal wave

02 November 2020

*Data privacy class actions in Europe are here to stay. Bird & Bird partner **Bryony Hurst** explores the rise in class actions, the EU member states that are likely to become popular litigation forums, key cases that have already been filed across Europe, and how organisations can stay as dry as possible when the data protection class action tidal wave hits.*

Two years ago, I wrote an **article** which addressed the predictions that companies subject to the GDPR would suffer a deluge of class actions as soon as the legislation came into force in May 2018. At the time of writing the article, what had

become clear is that, for many reasons, the tidal wave of litigation had not yet hit and, at most, we were at the early warning stage. Now that the GDPR has had time to bed in, what is the position two years on?

Claimants are jumping in feet first

We still may not be drowning in cases, but there's definitely a need to start swimming. As I noted previously, a culture of data privacy awareness has grown out of the introduction of the continent-wide GDPR framework. Data subjects have more and clearer rights to data protection, and data controllers are required to provide greater transparency into what data they handle and how. The GDPR also provided that judicial remedies would be available to all those who had suffered harm as a result of a breach of its provisions. Consequently, claimants have become more clued up about their rights, and more confident in asserting them in national courts. The evolution of class action claimant law firms and litigation funders interested in data privacy cases has further encouraged this. Individual and collective actions have increased around Europe as a result.

However, despite the best of intentions, GDPR has not delivered an utterly clear path for claimants to pursue relief in court. Key aspects of the remedies provisions (found in Chapter 8 of the GDPR) are still left to be implemented at the discretion of each EU member state. In particular, each country can decide for itself which entities can bring representative actions on behalf of data subjects, and whether those entities can apply for compensation or just declaratory relief. Article 82 of the GDPR is also not overly prescriptive as to what type of harm should be compensable, stating only that compensation should be available to anyone who has suffered "material or non-material damage" – and different member states' judiciaries have taken their own stab at defining this. There is still, then, a certain amount of working out to be done before Europe can boast that it has a truly effective and consistent collective remedies regime for data protection infringements.

These GDPR-specific hurdles should be considered alongside Europe's somewhat potted history and attitude to collective redress mechanisms more generally. The European authorities have intermittently flirted with the idea of legislating for an EU-wide representative actions regime. The European Commission considered the issue in 2013 but stopped short of passing any laws, issuing instead a non-binding

“recommendation” on common principles for injunctive and compensatory collective redress mechanisms. Certain countries, such as France and the Netherlands, did introduce new means of collective redress in quite a broad range of areas; others such as Spain and the UK did so but limited their mechanisms to certain breaches of law only; and still others made no changes, concluding either that their current regimes were sufficient, or that there was no need for collective redress mechanisms. Not entirely surprisingly, when the issue was reviewed by the European Commission in 2018, the availability of collective redress across Europe was found to be inconsistent.

The GDPR has broad territorial scope: data controllers do not have to have an establishment in Europe to be caught by its provisions, and in certain circumstances, data subjects do not even have to reside in Europe to be entitled to protection. Data subjects can choose to sue a data controller in the member state where the controller has its main establishment, or in the member state where the data subjects resides. This gives individual claimants at least two options, and gives representative organisations of collective actions a wide choice of forum to hear the dispute – if data subjects in multiple EU countries are affected by the alleged infringement, a representative entity has an array of jurisdictions to select from.

This creates a real headache for potential defendants to class actions in Europe: claims could pop up anywhere and predicting where is not an easy task. By analysing each member state’s particular collective redress regime, however, and observing current class action trends, it is possible to make some educated guesses as to the likely most popular forums:

The Netherlands

This is a growth class action market of note. Class actions brought by a “representative entity” for declaratory relief relating to the same or similar events have long been permitted in the Netherlands. As of 1 January 2020, though, actions for compensation are now also available – subject to certain conditions relating to the funding, structure and transparency of the representative entity (which, if not fulfilled, could provide an opportunity to strike out the claim).

First published on the *Global Data Review* website, November 2020

The new law specifically provides for such actions to be brought in relation to GDPR violations and interestingly deems that representative actions will operate as an opt-out claim for residents of the Netherlands (and opt-in for non-residents, unless the court is asked to order otherwise – which one could foresee a defendant might seek to do, in an attempt to avoid copycat litigation in multiple member states).

A collective settlement law already exists which provides a neat and swift resolution to mass damages claims if settled which, again, operates on an opt-out basis.

This is the closest European regime we have seen to US-style class actions, and is already proving attractive to groups of claimants, particularly civil rights/not-for-profit organisations whose main motive is to seek declaratory relief to clarify the law in a particular area of data protection law, but who can more easily obtain investment for their actions if they are also able to take advantage of the damages mechanism to attract litigation funders.

UK

Thanks to a case that has been making its way through the UK court system over the past couple of years, the UK is currently teetering on the edge of accepting opt-out mass damages claims without any formal legislative mandate. The UK has not yet opted to introduce the rights in Article 80 of the GDPR for not-for-profit bodies to start proceedings in court on behalf of data subjects without their consent.

The case, *Lloyd v Google*, has been brought using a representative action mechanism in the UK Civil Procedure Rules. The standing test for representative actions' has historically been interpreted narrowly, and the mechanism has not been the collective action of choice for groups of litigants to date. Representatives can bring claims on behalf of other persons who have "the same interest" in the claim.

In *Lloyd v Google*, which concerns allegations of a lack of transparency around Google's 'Safari Workaround', the High Court determined that the "same interest" threshold had not been met because a) claimants would have suffered different types of damage and b) it was not possible to identify every member of the class.

First published on the *Global Data Review* website, November 2020

The case has since been heard by the Court of Appeal, which disagreed and upheld the action. The primary reason for this appears to be the creative way in which Lloyd structured the claim: he disavowed any claim for damages to compensate specific pecuniary or other losses, and claiming only a relatively low, uniform amount for each claimant in respect of the damage they all had in common, which he asserted was a loss of control over their personal data. This appeared to impress the Court of Appeal; if the appeal judgment is upheld by the Supreme Court, it may provide a novel way for claimant groups and representatives to engineer an opt-out damages claim using the representative action mechanism.

This could act as a real boon for collective actions in the UK which previously have been funnelled down an alternative route known as Group Litigation Orders (GLOs). GLOs are not true class actions, but are simply a procedural mechanism by which courts can more efficiently manage and hear a large number of claims concurrently. They are difficult to commence (requiring a large administrative effort to sign claimants up to a court register), to handle (often involving multiple claimant law firms all vying for influence over the case) and entail high costs risks for claimants, unless litigation funding and insurance is obtained.

Italy

In April 2019, Italy passed a new law which significantly amended its collective action regime. It extended the availability of class actions (for compensation as well as declaratory relief) from just consumers to any group of individuals who have "homogenous rights" (ie rights generated by the same fact or event). It also created a right for not-for-profit associations and consumer organisations to bring claims on behalf of individuals, and extended the causes of action from a limited number of specific torts to virtually any and all breach of tort law.

The system is opt-in, but claimants have two bites of the cherry in this regard: they can sign up to the action after it has been declared admissible by the court, or after judgment on liability has been entered.

The new regime is rather unfriendly for defendants in respect of costs. A loser-pays principle has been introduced, and the defendant also has to cover the costs of technical and quantum experts appointed in the proceedings to assist the court with aspects of the case and calculation of damages. An additional "reward" fee is paid

by the defendant to the claimants' lawyer – this is likely to act as an additional incentive for class action lawyers in Italy to identify easy-win cases (for example, egregious data breaches).

France

France introduced legislation in 2016 which provided for an opt-in class action regime in certain areas of law, including data protection. To qualify, the group members must have been in "a similar situation" and suffered material or moral harm as a result.

Groups of litigants can bring such action, but the law also allows "authorised associations" to bring representative actions on behalf of individuals. The French Data Protection Act defines which entities fall within this class.

France also decided, in implementing Article 82 of the GDPR, to permit authorised associations to seek compensation on behalf of data subjects for any infringement that occurred after 24 May 2018, not just declaratory relief.

One problem representative associations face in France is a prohibition on advertising the collective action anywhere other than newspapers. The litigation funding market is also less developed in France than in certain other member states, which can be an additional hurdle to getting an action off the ground.

Spain

Spain has a collective action regime (which permits claims for compensation) available to protect "consumer rights", but it does not explicitly cover data protection actions, and Spain's data protection legislation does not provide for collective actions.

That said, a case is currently making its way through the Madrid Commercial Court which is likely to test the boundaries both of Article 80 of the GDPR and the definition of "consumer rights" and establish, much in the same way as *Lloyd v Google* in the UK, whether representative actions can in fact proceed in the courts despite the absence of a legislative mandate. The case has been brought by a

consumer organisation (OCU) against Facebook in relation to data protection breaches arising out of, among other things, the Cambridge Analytica scandal. If OCU succeeds with its action, it is foreseeable that Spain may become another hotspot for collective action in the data protection sphere. The Spanish data protection authority is very active in its investigations and enforcement and has issued some relatively large fines in recent times. That said, it has not pursued Big Tech to the near exclusion of all other organisations in the way certain other data protection authorities have, and the Spanish courts have to date issued only low damages awards for data protection infringement. For claimant law firms going after the obvious targets (Big Tech) and looking for a strong return on investment, this jurisdiction may require further testing before it becomes a firm favourite.

Who's taken a dip so far?

You can be sure that the economics of class actions dictates that claimants and their lawyers will follow the money. If an organisation commits a breach of data protection law that impacts lots of people in a serious way, claims will be brought against that organisation even where forum-shopping is not an option. For example, following British Airways' data breach in 2018, one claimant law firm published its first advertisements for data subjects to join its class action against the company within a couple of weeks of the breach being announced. If they have a choice, they will of course seek to commence claims in the friendliest forums – but if they have to, or if the maths means it makes sense, they will also get creative to tackle the trickier jurisdictions. A good example of this is the actions recently brought in the Netherlands (and shortly to be brought also in the UK) by The Privacy Collective, a civil rights group, against Oracle and Salesforce in relation to their use of cookies to collect data for use in real-time bidding. The Privacy Collective has been very open about choosing the Netherlands due to the collective action regime available there, and has also spoken about its hopes of taking advantage of the Court of Appeal's decision in *Lloyd v Google* to pursue remedies in the UK.

The *Lloyd v Google* case itself is another example of claimants taking on a jurisdiction which historically has presented hurdles to collective actions, and to circumvent a legislative lacuna to establish a new route to mass remedies. A note of caution for excitable claimant lawyers in this regard: whilst the novel structure of the *Lloyd v Google* claim does appear to present an opportunity to craft a collective action that passes the representative action standing test, this will not be a one-

size-fits-all solution to data protection group claims. As a more recent case (*Jalla & others v Shell*, not a data privacy case) which referred to the Court of Appeal decision in *Lloyd v Google* has demonstrated, where questions of individual causation still exist, altering your action to claim only a uniform amount of damage à la *Lloyd v Google* will not convince the court that your action should be squeezed into the mechanism. In the UK we are currently witnessing a rise in group claims following on from data security incidents, typically alleging that passwords and data belonging to individuals has been stolen as a result of a lapse in an organisation's IT systems; in cases such as these, one could envisage a large question mark over whether damage suffered by any given individual was caused by this particular security lapse, or one of the many other data breaches that occurs daily, and which could also have allowed the individual's data to be stolen, proving an obstacle to a *Lloyd*-style effort. The Court of Appeal, in its obiter comments, also appeared to support the continuance of some sort of de minimis threshold for data protection group claims, indicating that "an accidental, one-off data breach that was quickly remedied" would not give rise to a claim for loss of control over personal data alone. This is the lone encouraging aspect of the decision and one that potential defendants are hoping the Supreme Court will confirm (and expand usefully on).

Another good indicator of tomorrow's class actions is today's regulatory investigations. Class action lawyers and litigation funders can window shop potential claims by watching and waiting to see where data protection authorities are focusing their energy and, more importantly, who they decide to penalise most stringently. One current trend is the attack on adtech – an industry under a great deal of regulatory scrutiny that has already been criticised by many data protection authorities as being in breach of the GDPR in various significant respects. For consumer associations looking to expedite change and hammer home to large organisations the need to alter their practices, filing mass damages claims alongside regulatory complaints is proving a popular tactic. For example, several civil rights groups in France are focused on changing what they see as unacceptable data practices by Big Tech. Two of note currently are the Internet Society France's claim against Facebook in respect of 7 different data privacy-related complaints (which, it was announced last month, has failed to settle and so will head to court shortly), and UFC-Que Choisir's action against Google which focuses on Google's targeted advertising data practices, which commenced last summer and in respect of which a decision on admissibility is pending.

First published on the *Global Data Review* website, November 2020

Another national court system likely to be kept busy by privacy activists (well, one in particular) in times to come is that of Austria, the home of the not-for-profit Noyb, founded by Max Schrems, the perennial thorn in Facebook's side. Noyb was founded in 2018 to, in its own words, "bring long-term strategic enforcement cases".

It is clear that, in instances where it reaches what it considers to be a regulatory dead end (or delay) in Ireland (where Facebook has its main establishment for GDPR purposes), it will file claims in the Austrian courts to drive matters forward. Austria is another potentially interesting forum for data protection mass actions, being one of only a few Member States to have specifically implemented a right for representative bodies to bring damages claims on behalf of data subjects, pursuant to Article 80(1) of the GDPR.

It is worth noting that the class action mindset is catching – it is no longer just consumers and their representatives taking on organisations who they view as profiting at the expense of their privacy. In the UK, at least, data subjects are looking at how else their data is being used for commercial gain and testing if there is any value to claiming an abuse of their rights. New types of group litigants are emerging as a result; for example, one well-publicised potential suit, known as Project Red Card, involves over 400 footballers threatening action against gambling operators and data supply companies for use of their performance and tracking data without their consent. Successful or not, it's not hard to imagine similar cases being brought by athletes in other sports, and in other countries – or analogous actions in other industries.

Put your life jacket on

As an organisation processing the data of European citizens, what can you do to avoid drowning when this tidal wave eventually hits?

Wherever actions are brought, you can expect some commonality in tactics used by claimants and forewarned is forearmed. Where available, claimants will definitely seek to use findings and evidence from published data protection authority decisions, so keep that in mind if you become ensnarled in any regulatory investigation – documents clearly summarising the systems and processes you had in place to minimise harm to data subjects, for example, make for a nice paper trail for a defendant to group actions later down the line. Another common tactic is the

use of subject access requests by claimants to fish for information and evidence to bolster any action being put together by their lawyers. Any failure to comply with a subject access request is also sometimes used to beef up a list of other breaches levied against a defendant. For both these reasons, approach subject access requests carefully and ensure they are handled properly.

As claimants start to adopt US-style offensive tactics, another certainty is that defendants will do the same in terms of their defence. Expect to see key battlegrounds emerging around class certification and defendant applications equivalent to a US motion to dismiss, as defendants become clued up on challenges likely to cause a collective action to stall early on. Another line of defence likely to cause problems to groups is questioning the suitability and organisation of representative bodies bringing claims on behalf of consumers; different EU member states have their own requirements as to such bodies' constitutions, structure and funding which one could expect defendants to rake over and use as objections to the progress of any action.

As a final note, the European authorities have, since their 2018 review, decided that EU-wide legislation is required to harmonise collective consumer actions and a draft directive was recently sent to the European Parliament for approval. If brought into force, it will ensure that a means of collective redress for consumers for a wide range of legal breaches will be available in each member state – and will significantly assist groups with members in more than one member state (a harmonised cross-border action approach is included in the draft text).

On one hand, this legislation is good news for defendants. It may eradicate, or at least reduce, the need for forum shopping for cross-border representative actions. On the other hand, however, the much talked about tidal wave could finally hit. Whilst the draft introduces the "loser pays" principle across Europe and still prohibits punitive damages, this widespread availability of collective action mechanisms and remedies would still bring Europe a good few steps closer to the US-style mass claims culture. In 2018, then-European Commissioner for Justice, Consumers and Gender Equality Věra Jourová said: "Representative actions in the European way will bring more fairness to consumers, not more business for law firms." We will all have to watch this space to see if she was right.

This article was previously published in four different parts.

First published on the *Global Data Review* website, November 2020

First published on the *Global Data Review* website, November 2020