GDPR Collective Civil Claims Present Potential for Reputational Risk and 'Ruinous' Damages

Skadden

02 / 07 / 19

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

David Kavanagh QC
Partner / London
44.20.7519.7288
david.kavanagh@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

Nicholas Adams
Associate / London
44.20.7519.7286
nicholas.adams@skadden.com

Four Times Square
New York, NY 10036
212.735.3000

40 Bank St., Canary Wharf
London, E14 5DS, UK
44.20.7519.7000

While much attention has been paid to the maximum level of administrative fines under the General Data Protection Regulation (GDPR) — up to 4 percent of total worldwide annual turnover — the regulation also provides for another source of potential liability: it grants any individual the right to compensation for damage caused by a data controller's or processor's breach of the GDPR's requirements. Key features of that civil claims regime provide for alarming reading, even if the precise parameters remain unsettled. Compensation is recoverable whether or not the relevant loss was financial in nature (though the quanta properly attributable to nonfinancial losses, such as reputational damage or distress, remain uncertain). Even in the context of business-to-business operations, where a data processor may not actually have interacted with a named plaintiff, the GDPR provides for joint liability among culpable respondents (though contribution from the other respondents can still be sought). Further, a data controller or processor will be culpable for the event that caused a data breach unless it can demonstrate that it was not "in any way" responsible for it.

As the more stringent approach heralded by the GDPR has begun to be applied over the last year, serious data leaks or hacks have impacted major corporations ranging from Ticketmaster to Marriott. It is therefore clear that the brake on compensation claims will not be the occurrence of such events. Rather, to the extent that there has been a limiting factor, it has been the size of the loss suffered by each individual. In order to overcome that challenge, privacy rights organisations in Austria have for some time been aggressively pursuing collective actions. Here in England and Wales, there are two avenues by which groups of potential plaintiffs might pursue collective recoveries. First, the GDPR enables affected individuals to mandate certain not-for-profit entities to pursue compensation on their behalf. Those individuals also would also have to satisfy the high CPR Part 19 procedural hurdle of demonstrating that they had the same interest in the relevant claim and would each benefit from the relief sought. Second, the GDPR gives EU member states the flexibility to provide mechanisms in their national laws by which individuals might bring claims collectively. At present no "opt-out" mechanism has been implemented in England and Wales, although a review of whether to do so is expected by 2020. In the meantime, plaintiffs may still seek a group litigation order from the High Court if they are able to demonstrate that their claims give rise to common or related issues of fact or law.

In either the first or the second scenario, the central challenge for groups of plaintiffs will be the logistical and administrative obstacles attendant on bringing significant opt-in actions in England and Wales. However, events over the last year have made it clear that potential plaintiffs and their legal counsel are actively exploring how best to pursue such claims despite those obstacles. Several U.S. law firms specialising in collective damages actions have recently opened offices in England and Wales and begun to market in this area. The appetite of litigation funders in this jurisdiction for class actions continues to grow exponentially. Most recently, British Airways has been threatened with a class action lawsuit by individuals whose data may have been compromised after a data hack resulted in the loss of payment card data associated with 380,000 transactions. The plaintiffs assert an entitlement to recover from the airline damages for "inconvenience, distress and misuse of their private information" of up to £1,250 each, leaving a total quantum running well into the hundreds of millions of pounds. Entitlements currently asserted against respondents in other contexts claim several billion pounds.

GDPR Collective Civil Claims Present Potential for Reputational Risk and 'Ruinous' Damages

It remains at present hard for plaintiffs, their lawyers (who may be operating on conditional fee bases) and litigation funders properly to assess actual returns in this area. They will, however, have been encouraged by the figures being mooted and by the view, recently expressed by the English Court of Appeal, that there is potential for "a large number of claims [for] ruinous amounts" in this area. The scale of those potential financial incentives is why many such professionals now await a strong test case justifying the time-consuming and expensive exercise of constructing a group of litigants. The workload of the Information Commissioner's Office (the U.K. data protection authority) means that post-GDPR enforcement notices are only now beginning to be issued, but rapid developments in this area should be expected following the issuance of a GDPR enforcement notice demonstrating a uniform but serious impact (such as identity or other fraud) across an extensive but readily identifiable class of individuals. In the meantime, clients should take this opportunity to ensure that they fully understand and have appropriately managed their risk profile in this area. Practical steps might include checking that:

- key personnel fully understand the financial and reputational risks posed by compensation claims under the GDPR;
- internal policies and privacy notices comply with the GDPR;
- data security measures have not been superseded;
- staff are adequately trained in identifying data protection issues;
- data governance (including escalation procedures) remains fit for purpose and protects privilege;
- appropriate systems exist for notifying any breach to individuals (which will also alert them to the need to take any steps to minimise their losses); and
- existing insurance coverage would cover compensation paid under the GDPR.