The changing landscape of data protection in the context of civil litigation

Notwithstanding Brexit, data protection and privacy law will continue to be a key part of the litigation landscape - and increasingly the subject of large scale litigation itself.

This article was first published in Privacy Laws & Business UK Report, Issue 86 (August 2016)

The UK’s vote to leave the EU has undoubtedly created a degree of uncertainty about the future of the UK’s data protection regime. Whilst in recent years we have seen a significant movement by the EU to bolster data protection and privacy laws through legislation and decisions of the Court of Justice of the European Union (CJEU), it is now uncertain what path the UK’s data protection regime will take. Much will depend on the nature of a post-Brexit UK-EU relationship. However, what is clear is that data protection and privacy will remain important and increasingly contentious issues for businesses and their customers.

First, any post-Brexit deal that involves the UK remaining part of the European Economic Area and having access to the single market is likely to require the UK to adopt equivalent data protection and privacy rules to the EU, including the EU’s new General Data Protection Regulation (GDPR). The GDPR will in any event impact UK businesses post-Brexit which have operations in the EU.

Second, many of the important recent developments in data protection - which have tipped the balance further in favour of protecting individuals’ personal data - have been driven by the UK courts. Data protection and privacy litigation has increased steadily in the UK courts, and there has been a marked increase in the level of compensation which data controllers may be required to pay out following a breach of data protection and privacy obligations. Data protection and privacy issues have therefore been brought to the fore of civil litigation in the UK and the willingness of the UK courts to take the lead in this area seems unlikely to change following Brexit.

Data protection and civil litigation - an expanding range of claims

The Court of Appeal’s landmark ruling in Google v Vidal-Hall is one of a number of recent developments that shows data protection moving to the heart of civil litigation. Importantly, this case established that individuals whose data is not handled properly may be entitled to compensation for damage caused by “mere distress” even if they have not suffered pecuniary loss.

This marks an important change in the interpretation of s.13 of the Data Protection Act 1998 (DP Act); it was previously understood that distress alone is not a basis for recovery of damages for a breach of the DP Act, a view supported by the decision in Johnson v Medical Defence Union. However, the court in Vidal-Hall concluded that, given that the aim of the DP Act is to protect privacy, it would be odd to prevent a claim by data subjects whose privacy was breached but who had not suffered pecuniary loss.

The decision also established the misuse of private information as a tort for the purposes of service out of the jurisdiction. That should mean that it is easier for claimants who bring claims

1 See, for example, Google v Vidal-Hall [2015] EWCA Civ 311 and Gulati v MGN Ltd [2015] EWHC 1482, discussed below.


3 Johnson v Medical Defence Union [2007] EWCA Civ 262.
under this cause of action to obtain service out of the jurisdiction against foreign defendants, a very relevant issue given that many large data controllers are established in the US. It is worth noting that this cause of action is distinct from the right to privacy under Article 8 of the European Convention on Human Rights (ECHR). This ECHR right was examined in the recent case of Barbulescu v Romania. This means that there are parallel means of recourse for individuals in respect of alleged data and privacy breaches. Importantly for data controllers, the court in Barbulescu held that the monitoring of an employee’s internet use by his employer (and his subsequent dismissal) did not breach his Article 8 right as the employer had a clear policy banning employees using its equipment for personal use and had intruded on his privacy in a manner limited to the enforcement of that policy.

The rights of data subjects are not, therefore, limitless. However, the Vidal-Hall decision will have a significant impact in the field of data protection litigation and could make it much more attractive to bring claims for data protection breaches (which are typically suffered by a large number of individuals who may individually be able to recover only a small amount of damages) as class action style claims.

In that regard, the UK currently has only a limited class action regime, with restrictions on how group claims may be structured and funded. However, certain tools are available to enable claims to be brought on a large scale; for example, the courts can make Group Litigation Orders (which permit claims which give rise to common or related issues to be managed collectively) and class actions for data protection breaches could become more commonplace if the new collective action regime - which was recently introduced for breaches of competition law - is rolled out more widely. Moreover, litigation funders may well develop an appetite for funding claims for breach of data protection and privacy rules in the future. Other large scale cases are already being brought for data protection and privacy breaches; for example, over 5000 current and former employees of supermarket chain Morrisons are pursuing a claim for damages against it in the English High Court after their bank, salary and national insurance details were leaked online by a rogue employee. Moreover, we have already seen the prospect of collective litigation in Europe for alleged data protection violations - including that marshalled by privacy campaigner Max Schrems in respect of Facebook’s alleged breaches of its privacy policy.

These developments demonstrate that the UK courts are playing a key role in the development of data protection and privacy rights and their movement to the heart of litigation. Vidal-Hall in particular raises concerns for businesses which collect large amounts of personal data and are therefore particularly vulnerable to breaches of cyber-security, or to the actions of rogue employees (as demonstrated in the Morrisons claim). Even if individuals may not themselves be entitled to significant sums or want to fight these types of cases to the end, the ability of data subjects (or litigation funders) to bring claims for damages clearly poses significant legal and reputational risks for businesses large and small.

4 Following Vidal-Hall, the tort of misuse of private information is now a basis for satisfying the jurisdictional gateway for permission to serve a claim out of the jurisdiction under CPR 6.37 and paragraph 3.1(9) of Practice Direction 6B.

5 Barbulescu v Romania 61496/08 [2016] ECHR 61.

6 There had been uncertainty as to the status of the Court of Appeal’s decision in Vidal-Hall pending an appeal to the Supreme Court. However, that appeal has now been withdrawn. As a result, the Court of Appeal’s decision is good law.

7 There has been another announcement of a “class action” claim against online gambling company GVC following its transfer of data as part of a prospective tie up with another large betting company (though it is not currently known how this action will be structured or in which court it will be brought).
Step change in consequences of data protection breaches

As well as the increasing scope of data protection litigation, businesses need to be aware of the increasingly significant consequences of breaches of data protection or privacy rights, both in the form of damages awards in private actions and fines in the public enforcement arena. Two points stand out.

First, the recent decision in Gulati v MGN Ltd marks a step change in the courts’ approach to damages in data protection and privacy litigation. In this case – which related to the infringement of privacy rights of individuals through the hacking of phones – Mann J made damages awards far in excess of those in previously reported privacy cases, awarding between £85,000 and £260,250 to each claimant. The courts have previously been far more restrained in damages awards for breaches of privacy, including in Mosley v NGN, where a comparatively small award of £60,000 was made. Even if these awards mark the ‘extreme’ end of damages awards, taken with the scope for collective claims, the potential liability of data controllers could be greatly increased if this more robust approach by the courts continues.

Moreover, the severity of the competition-style fines regime introduced by the GDPR is likely to focus the minds of parties to litigation and their legal advisers on data protection issues in a way not previously seen. Fines of up to the greater of €20 million or 4% of annual worldwide turnover may be imposed for breaches of obligations under the GDPR. The potential for much larger fines will also increase reputational risk for businesses which are found to have breached their data protection obligations. Whilst any data protection reform that the UK implements following its exit from the EU may not necessarily adopt these fining provisions, it is clear that the UK’s data protection enforcement body, the Information Commissioner’s Office (ICO), is taking a more robust approach to enforcement in respect of data protection breaches. Further, the GDPR will, due to its broad territorial scope, still directly impact UK (or other non-European) establishments which monitor the behaviour of, or offer goods and services to, citizens in the EU.

Further challenges on the horizon: the impact of the GDPR on civil litigation

The UK’s decision to leave the EU has resulted in uncertainty as regards the impact of the GDPR on UK businesses. However, a statement released by the ICO on 24 June 2016 confirmed that, although the GDPR would not apply directly to the UK if it is not part of the EU, in reality the UK is likely to implement similar standards to those under the GDPR. Not only is this in keeping with the recent direction of travel by the ICO in terms of the UK’s own data protection regime but, in order to transfer data from the EU to a non-member state, the GDPR requires that the non-member state have “adequate” protections in place. The ICO has therefore stated that it is in the UK’s interests - if it wishes to encourage trade (and exchange information) with the remaining Member States - to adopt legislation similar to the GDPR.

Further, in the event that the UK has not left the EU by May 2018, the GDPR will become law in the UK. The upshot of this is that the status quo will be maintained in the short term, and in the longer term - once the UK formally leaves the EU - the UK is likely to implement data protection reforms which closely mirror the standards under the GDPR. Businesses dealing with the EU or with EU-based customers should therefore continue taking steps to ensure compliance with the GDPR.

Given this, the implementation of the GDPR or an equivalent framework will result in a number of changes for litigators and businesses involved in litigation in the UK. Two of the biggest challenges are likely to relate to: (i) the reliance on the consent of data subjects to disclose personal data, and (ii) the cross-border transfer of personal data.

---

8 Gulati v MGN Ltd [2015] EWHC 1482.
Reliance on a data subject’s consent for processing

A key principle of the GDPR is that a data subject’s consent to processing of their personal data must be freely given, specific, informed and unambiguous, and, in respect of sensitive personal data, consent must be explicit. As a result, the threshold for showing that the data subject’s consent to data processing has been obtained is going to be higher. This means that data controllers and their lawyers need to ensure they have received the required consent before seeking to review or disclose - in the course of litigation proceedings - documents containing personal data. Data controllers will, for example, have to consider whether any consent to data processing given by employees in their employment contracts is sufficient for the purposes of the litigation, or whether it is necessary to rely on another ground to justify the processing (or disclosure) of personal data.

Transferring personal data abroad

A transfer of personal data to a foreign authority or court is a common issue faced in litigation and investigations and one which has been complicated by a number of recent developments:

a. First, in Schrems,10 the CJEU held that the Safe Harbour regime (which allowed the free flow of personal data from EEA data controllers to US organisations which had joined the scheme) was invalid. In February 2016, the European Commission announced a political agreement with the US Department of Commerce on a revised Safe Harbour scheme, introduced as the “US-EU Privacy Shield”. However, the European data regulator group, the Article 29 Working Party, has criticised the Privacy Shield for its lack of protection for EU citizens’ data from US government surveillance. If the European Commission does not make modifications to the proposed Privacy Shield before its formal adoption, we could see the Privacy Shield’s terms challenged in the courts.

b. Secondly, as a result of Schrems, in May 2016, the Irish Data Protection Commissioner (IDPC) applied to the Irish High Court for declaratory relief and a reference to the CJEU to clarify whether data transfers to the US under Standard Contractual Clauses (SCCs) are compatible with data protection legislation. Data controllers and data protection practitioners will await the outcome of the IDPC’s action to see whether the court will prevent reliance on SCCs to transfer data to non-EEA countries which lack adequate safeguards.

c. Finally, Article 48 of the GDPR prohibits the transfer or disclosure of documents containing personal data in response to a request by a court or administrative authority of a non-EEA state unless there is an international agreement between that state and the EU or the relevant Member State. The effect of Article 48 will be that businesses will face a more difficult balancing act between, on the one hand, cooperating to the greatest extent possible with foreign investigating authorities or courts which order disclosure but, on the other hand, complying with the broad obligations under the GDPR.

10 Schrems v Facebook (C-362/14).
For the time being, there therefore continues to be uncertainty surrounding international data transfers. It is possible that international data transfers (in both a litigation and non-litigation context), may themselves become the subject of litigation (and certainly significant tactical consideration) as parties and data protection authorities attempt to navigate an increasingly complex patchwork of data protection law.

The use of data protection as a weapon in litigation

Recent practice also indicates a shift from the previous view that data protection represented a procedural problem to a realisation that it can also provide an effective tactical tool to be deployed during litigation.

A key example of this is the use of subject access requests (SARs). These allow a data subject to access information that an organisation holds about them, and have been used as a means of obtaining limited pre-action disclosure. Although an SAR will require only personal data to be handed over - and may therefore be much narrower in scope than an order for disclosure - it is a useful tool for a litigant or potential litigant and has some clear advantages, including:

a. the cost saving compared to an application to court for pre-action disclosure - generally the data controller may not charge more than £10 for facilitating an SAR;

b. allowing a claimant to assess the strength of its case before commencing a claim; and

c. providing a mechanism for obtaining documents where the CPR requirements for early disclosure cannot be satisfied.

Debate continues as to whether SARs may be used for purposes other than pure defence of individual data protection rights. For example, the ICO has investigated the way SARs have been used to obtain medical records of individuals seeking insurance. In a litigation context, earlier cases suggested that the courts would not entertain the use of SARs to “obtain discovery of documents that may assist...in litigation”. However, there is now a growing body of authority which appears to accept the use of SARs as part of a litigation strategy, including the Court of Appeal’s obiter statement in Dunn v Durham County Council that an SAR may be made “before during or without regard to legal proceedings”. This position has received recent support in Guriev v Community Safety Development. There, the court held that the purpose for which an SAR has been submitted is not generally a matter for enquiry by the court and that seeking access to information which might become disclosable in litigation is not an abuse of process (and so the data controller should comply with the SAR).

However, there may still be scope for resisting such SARs. In Dawson-Damer v Taylor Wessing, which concerned an attempt by three claimants to obtain information from the defendants’ lawyers, the court held (inter alia) that:

a. SARs exist to enable data subjects to check whether data processing unlawfully infringes privacy rights and to take steps to protect those rights - not to enable discovery of documents that may assist in litigation of complaints against third parties, which would be an abuse of process; and

b. it was not reasonable to require Taylor Wessing to carry out any search to determine if particular documents were privileged or not as this exercise would be complex and very costly.

The case is currently under appeal to the Court of Appeal so we can expect further development or clarification of these issues in the near future.

---

14 Dawson-Damer and others v Taylor Wessing and others [2015] EWHC 2366 (Ch).
Finally, the DP Act has proved to be a valuable legal tool in other contexts; for example, it has provided a useful means of recourse for a company in circumstances in which an employee left and took a client list with him. The employee was reported to the ICO and was convicted for a breach of s. 55 DP Act, which makes it a criminal offence to knowingly or recklessly, without the consent of the data controller, obtain or disclose personal data, or procure the disclosure of personal data to another. This could prove a useful mechanism for other wronged data controllers and again shows that the DP Act can be an aid as well as a burden for data controllers.

Conclusion

Given recent legal developments and the increased awareness of individuals of their data protection and privacy rights, there is a real need for businesses to consider the adequacy of their handing of individuals’ data and the risk assessments they undertake in this regard. There are considerable business upsides to doing so, both in terms of minimising the costs and risks of litigation, and also generating the reputational (and commercial) benefits of being seen as a business which respects its customers’ data rights.

Further publications on the GDPR and other data protection and privacy issues are available on our website. For further information, please contact Richard, Camilla or your usual Slaughter and May advisor.