

Quantifying damages for data breaches

[eversheds-sutherland.com/global/en/what/articles/index.page](https://www.eversheds-sutherland.com/global/en/what/articles/index.page)

15-02-2017

United Kingdom

Technology, Media and Telecoms - General

Précis

The High Court awarded damages of up to £12,500 each to six individuals as compensation for the shock and distress caused to them by the accidental publication of their personal data by the Home Office. When assessing the quantum of these damages, the Court was guided by cases involving awards for psychiatric and psychological injury, rather than cases pertaining to deliberate dissemination of confidential information for commercial gain¹.

When multiplied and considered in the context of increasingly prevalent larger scale data and system security breaches and group litigation, this case underlines that the potential damages that could be payable by organisations to effected customers and/or employees (even where there is no proven financial loss by those individuals) could be very significant.

This means that all organisations, whatever their sector, should pro-actively prepare and test their policies, practices and technical measures to prevent or minimise the impact when a breach occurs. In addition, and because the origin of a breach can obviously vary (e.g. from within, through vendors, through connected third party supply chains, etc.), organisations, their suppliers and corporate customers must all be clear contractually who should bear the risk and responsibility when breaches occur.

What?

On 15 October 2013, the Home Office, erroneously uploaded the details of nearly 1,600 people involved in the family returns process. The disclosed information included the lead family member's name, age and nationality, whether asylum had been claimed and the office which dealt with their case, from which the general area in which they lived could be inferred.

On 28 October 2013, 13 days later, the error was discovered and the page immediately taken down. Prior to the information being removed, it had been downloaded and saved by one person. The page had also been accessed on 27 occasions by 22 different non-Home Office IP addresses in the UK and by one IP address in Somalia.

On 24 November 2013, the information was uploaded to a US document sharing site where it was accessed a further 86 times before being removed on 13 December 2013.

In January 2014, the Home Office notified the affected individuals. Subsequently, six of these affected individuals proceeded to bring a claim for misuse of private information and data protection breaches. There was no evidence of any financial loss suffered by the individuals.

The Legal Framework:

Section 13(1) of the Data Protection Act 1998 (“DPA”) states that individuals who suffer “damage” as a consequence of a breach of the DPA by a data controller can claim compensation.

In *Vidal-Hall*² it was determined that claimants were not required to prove they had suffered a financial loss in order to claim compensation for a breach of the DPA. In effect, this decision clarified that section 13(1) of the DPA permits compensation to be awarded in instances where a claimant has only suffered distress as a result of the breach.

In *Gulati*³, the Court of Appeal held that an award of damages in such cases should not only compensate for distress. The court stated that damages should also compensate for the loss or diminution of a right to control private information.

The Decision

During the course of the proceedings, the Home Office admitted liability for misuse of the claimants' personal data in breach of the DPA. It was also accepted that the claimants could recover damages for distress at common law, and under section 13(1) of the DPA.

The court rejected submissions that the quantum should be assessed in-line with the guidance contained in cases involving a deliberate breach of data protection for commercial gain by media publishers, or other media operators. The court held that where claimants suffer shock, or are put in fear, as a result of a data breach, such cases are closer to those where claimants have suffered

psychiatric injury as a result of an actionable wrong (irrespective of whether the data breach was the result of a careless or deliberate act). A claimant's loss of his or her right to control of their private information was also considered when determining the quantum of each award.

Two of the claimants were awarded £12,500 each whilst the others received awards ranging from £2,500 to £6,000. Each award was quantified following an assessment of the anxiety and shock the claimant suffered as a consequence of the breach.

So What?

This case is of importance as it provides useful and relatively rare guidance in relation to damages awards in privacy and data protection claims following the *Vidal-Hall* decision.

This case indicates that where a claimant has suffered distress, damages should be calculated in a similar way to cases involving psychiatric and psychological injuries. Although the Court confirmed that claimants will be required to overcome a "*de minimis*" hurdle before they can recover damages for distress, data controllers should be aware of the potential financial implications of claims by those affected by accidental data breaches.

[1] *Gulati v MGN Ltd* [2015] EWCA Civ 1291

[2] *Google Inc v Vidal-Hall and others* [2015] EWCA Civ 311

[3] *Gulati v MGN Ltd* [2015] EWCA Civ 1291



- [James Hyde](#)
- Senior Partner
- [+44 113 200 4066](#)
- +44 113 200 4066
- [Connect with James Hyde on LinkedIn](#)

This information is for guidance purposes only and should not be regarded as a substitute for taking legal advice. Please refer to the full [terms and conditions](#) on our website.

This information is for guidance purposes only and should not be regarded as a substitute for taking legal advice. Please refer to the full [terms and conditions](#) on our website.