The New PPI?

Distress and Anxiety Claims Arising from Data Breaches

Keoghs

Contents

We have recently seen claims brought by individuals, alleging that they have suffered distress and anxiety as a result of data breaches. A number of firms are already targeting what could be a new source of claims and are actively farming potential claimants where breaches arise in relation to large, or high profile, businesses. The stakes have been raised by the Court of Appeal's decision in *Lloyd v Google*.

What is causing these claims, what are the key issues and how should data controllers and their insurers react? Christopher Stanton, partner in Keoghs Professional & Financial Risks team discusses the latest concerns regarding distress and anxiety claims arising from data breaches.

Christopher Stanton
Partner, Liverpool
T: +44 (0)151 921 7110
M: +44 (0)797 674 6671
E: cstanton@keoghs.co.uk

Background

Businesses hold huge volumes of personal data. For example, a retailer may hold personal data about customers through loyalty cards and all businesses hold confidential financial data about their staff.

The requirements upon data controllers include:

- processing personal data in a way that ensures appropriate security of that data against accidental loss or destruction (GDPR Art 5(1)(f));
- implementing appropriate technical and organisational measures and processes to ensure compliance (GDPR Art 24(1 & 2)); and
- maintaining the data subject's confidence.

If businesses breach their obligations, a data subject has the right to compensation for material or non-material damage suffered as a result of the infringement (GDPR Art 82 and s.168 DPA 2018). This includes damages for distress.

The Claims

We have seen a significant rise in claims seeking damages for distress, breach of confidence and breach of privacy as a result of (often minor) data breaches. In every case, it is asserted that the claimant has entered a Conditional Fee Agreement (CFA) with a success fee.

Liability

It has been established that data subjects can bring claims for distress caused by data breaches (*Google v Vidal-Hall*). However, is there an automatic right to compensation; or do claimants need to show that they suffered damage as a result of the breach?

In the recent Court of Appeal decision in *Lloyd v Google,* it was held that you do not need to prove pecuniary loss or distress to be compensated under data law. It basically held that the analysis in *Gulati* v *MGN Ltd* (concerning the misuse of private information dishonestly obtained via phone hacking) applies equally to data protection.

Therefore where a person loses control or autonomy over their personal data through a data breach, that person is entitled to be compensated, regardless of any financial loss or distress caused. There is still a de minimis threshold, so not every data breach will result in damages (though the threshold is sure to be tested). However, the *Lloyd* decision benefits victims because damages can be awarded for loss of control over data without proving pecuniary loss or distress.

Distress

Usually, a claim for distress must involve shock and anxiety, resulting in psychological or psychiatric damage. To date, we have not seen any claims where expert medical evidence has been utilised to support a claim for distress.

However, *Lloyd v Google* established that you do not need to prove distress to be compensated. Ironically, the rationale lies in EU law (GDPR Art 82), so that where an individual loses control or autonomy over their personal data as a result of a data breach, they are entitled to be compensated regardless of any financial loss or distress. The relevance of GDPR will continue post-Brexit because it has been incorporated into the DPA 2018.

Class Actions

The *Lloyd v Google* decision also opens the way for class actions as a result of data breaches because it makes it easier to identify people with the same interest.

Google allegedly used technology on the IPhone Safari browser to monitor users' internet activity without their consent. The Court of Appeal held that the Court's discretion should have been exercised to allow the representative action to proceed. They held that '*once it is understood that the* [4-5M] *claimants that Mr Lloyd seeks to represent will all have their* [browser generated information] – *something of value – taken by Google without their consent in the same circumstances during the same period, and are not seeking to rely on any personal circumstances affecting any individual claimant (whether distress or volume of data abstracted), the matter looks more straightforward …*'

Lloyd deals with pre-GDPR breaches. However, GDPR has tightened the rules. It has increased the obligations upon data controllers and strengthened the remedies available. The *Lloyd* judgment increases the prospects of US-style class actions because it is easier to identify a large enough group (for example BA's data breach in 2018 affecting about 500,000 customers).

Vicarious Liability

The recent Court of Appeal decision in *Various v Morrisons* has caused real concern for businesses and insurers. In that case, a rogue employee released financial records and other personal data of Morrisons' employees, in a deliberate attempt to cause harm to the company. He has been imprisoned but Morrisons have been held vicariously liable for his actions (which was his primary motive).

The case is being appealed in November on various grounds, including whether vicarious liability is excluded from data protection legislation and, if not, whether it applies in this circumstance. However, businesses face the prospect of group actions by employees and customers arising from data breaches deliberately caused by rogue employees whose motive was to cause harm to their employer.

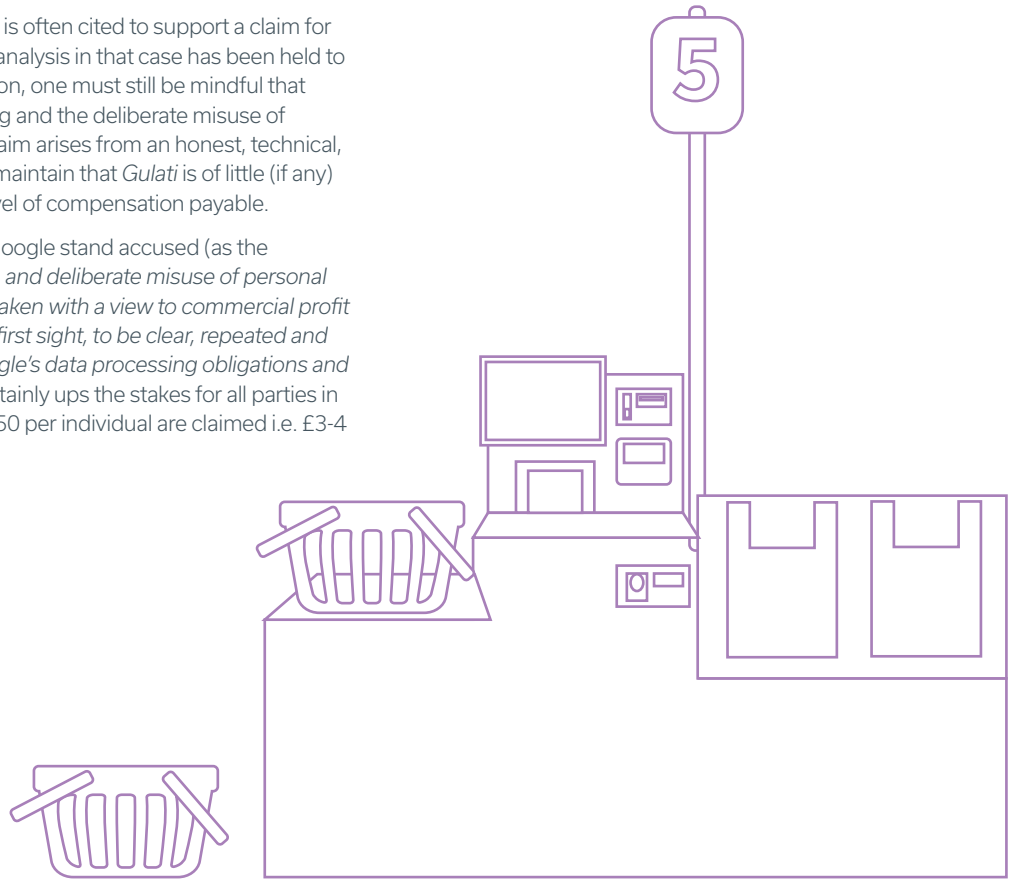
Loss

There are few reported decisions; and all pre-date the introduction of the GDPR / DPA in May 2018. However, we can be certain that the damages awarded for GDPR breaches will not be lower than those pre-dating the GDPR's introduction. These are separate from the ICO's statutory powers to fine businesses for data breaches.

In *TLT v Home Office* the High Court awarded damages ranging from £2,500 to £12,000 to six claimants for the distress caused by the accidental publication of sensitive personal data in an asylum case.

The case of *Gulati v MGN Ltd* is often cited to support a claim for breach of privacy. Whilst the analysis in that case has been held to apply equally to data protection, one must still be mindful that *Gulati* involved phone-hacking and the deliberate misuse of personal data for profit. If a claim arises from an honest, technical, data breach, businesses will maintain that *Gulati* is of little (if any) relevance in assessing the level of compensation payable.

However, in the *Lloyd* case, Google stand accused (as the Court put it) of the '*wholesale and deliberate misuse of personal data without consent, undertaken with a view to commercial profit …* [involving] *what appear, at first sight, to be clear, repeated and widespread breaches of Google's data processing obligations and violations …*' That analysis certainly ups the stakes for all parties in the litigation. Damages of £750 per individual are claimed i.e. £3-4 Billion in total.



Insured Risks?

A data breach would not normally be covered under an EL/PL policy, though many businesses now have cyber extensions or separate policies which cover data breaches.

However, claims for distress involving personal injury may well be covered under a typical PL policy. Many policies have an extension covering policyholders for damages for distress caused by data breaches. Insurers, brokers and policyholders need to review their policy wordings very carefully, to ensure that they understand the nature of the cover provided, and any limitations (such as aggregation).

Costs

In our experience, claimants' solicitors typically refer to a CFA and success fee being payable in the letter of claim. That gives rise to a number of issues.

Historically, distress is a psychological and psychiatric injury. Costs are not recoverable in small claims for damages for personal injury. In fast track cases, fixed costs apply and no success fee or CFA premium are recoverable from the paying party in personal injury claims. However, *Lloyd* provides an automatic remedy for distress caused by a data breach.

Claimants' solicitors will be arguing that GDPR is inherently complex, should be conducted on the multi-track and should not be classed as personal injury litigation, in order to recover their success fees and insurance premiums. If the claims were classed as personal injury matters then any success fee or premium would need to come out of the damages.

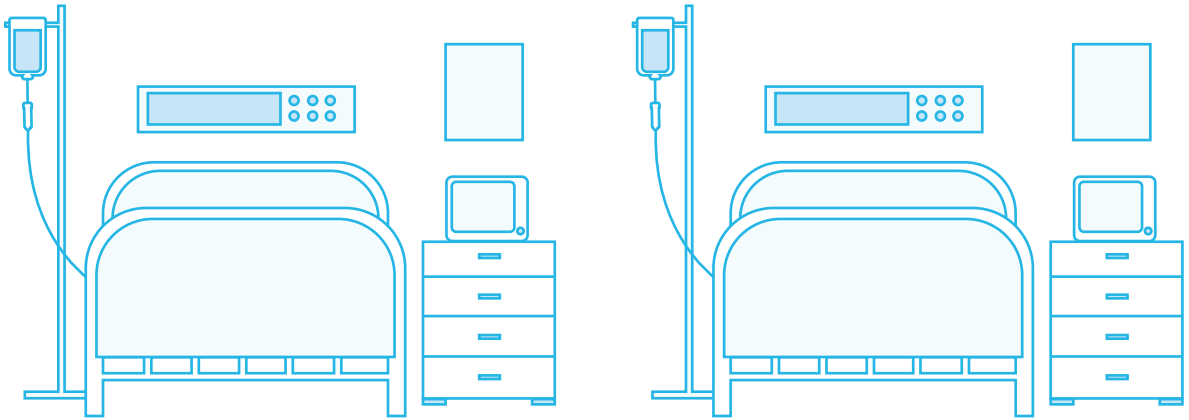
We anticipate that the question of the paying party's liability for costs, and the nature of those costs, will need to be resolved by the Court in the future.

Floodgates?

Morrisons has about 110,000 employees and face a potentially significant bill if their appeal fails. If each employee was awarded just £500 that equates to about £55M.

The *Lloyd* decision was simply determining whether the Court should have exercised its discretion to allow the representative action to proceed. The answer was a resounding 'yes'. Given the Court of Appeal's comments on the nature of the claims and the volume of data subjects affected, the implications for all parties could be enormous. The claim against Google seeks £3-4 Billion.

Taking it one stage further, what might happen if personal data held by the NHS or a national supermarket was hacked and released? The NHS holds sensitive personal data on everyone in the country and has 1.2M employees. If customers' personal data held by a supermarket was released, there could be millions of potential claimants. The repercussions could be enormous for businesses and their insurers because very few businesses (or insurers) have pockets as deep as Google or Facebook.



Conclusion

We assume that Google will seek permission to appeal. However, as a result of the *Lloyd* decision, individuals will assert that they have an automatic right to compensation for distress as a result of a data breach. We expect to see a significant rise in group actions and individual claims against businesses and other data controllers arising from data breaches. Other issues include the extent of vicarious liability for data breaches; and the recoverability of costs.
The courts will be kept very busy - watch this space for developments.

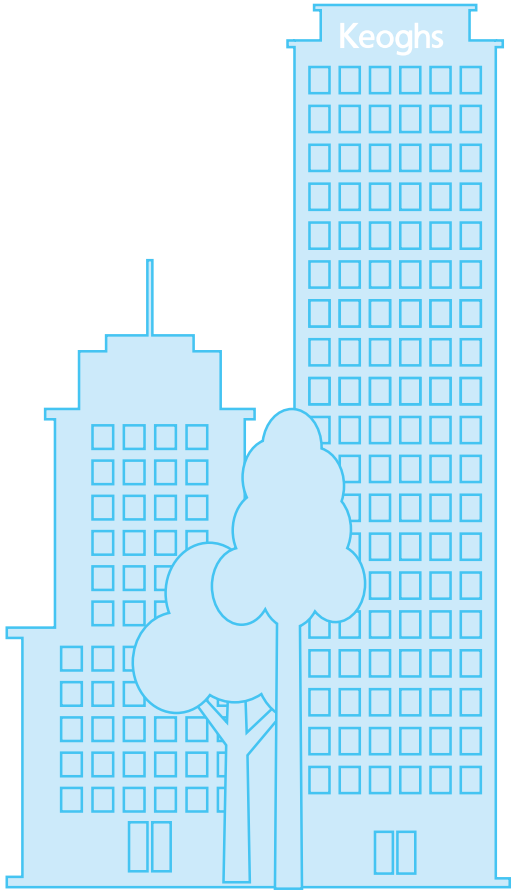
The key for businesses remains to secure and protect any personal data they hold; and to have robust systems in place to prevent any breaches, whether deliberate or accidental.

For insurers, brokers and policyholders you will need to carefully check your insurance cover to ensure that you understand the risks which are being covered and that they are fit for purpose. Important issues include aggregation and deductibles.

If you have any questions arising from this article or would like to discuss the issues generally, please contact Christopher Stanton.

Glossary

- DPA 2018 – Data Protection Act 2018
- GDPR – The General Data Protection Regulations (EU) 2016/679
- ICO – Information Commissioner's Office
- Lloyd v Google Plc [2019] EWCA Civ 1599
- Vidal-Hall v Google Inc [2015] EWCA Civ 311
- Gulati v MGN Limited [2015] EWCA Civ 1291



About Keoghs

Keoghs is a top 50 law firm based in ten locations across the UK, solely focussed on insurance.

With a thorough understanding of insurance claims processes, we offer a cost-effective, flexible and high quality service for handling the a-z of insurance; from personal injury claims including motor, casualty and complex injury to non-injury claims such as policy advice, recoveries and insurance disputes.

Boasting vast experience across a broad and eclectic mix of industry sectors, local authorities and businesses, we handle claims ranging from low value to complex on both a delegated and non-delegated basis.

Our award winning teams include acknowledged experts who have been involved in some of the most significant developments in their respective fields. This enables us to bring a rare depth of understanding and expertise to every aspect we handle.

We work in partnership with our clients, helping them to anticipate, navigate and adapt to industry change, maximising opportunities whilst minimising risks. We are forward-thinking and pioneer new solutions.

That's the Keoghs difference.

For further information on all of our services please visit our website,

keoghs.co.uk

Keoghs has provided defendant legal and claims related services to the insurance industry since

1968

We handle general insurance claims of all types, from the lowest value disputes through to the largest catastrophic losses.

1,700

Keoghs has over 1,700 employees

10

locations in Belfast, Bolton, Bristol, Coventry, Glasgow, Newcastle, Liverpool, London, Manchester, and Southampton. Keoghs provides a national service across England, Northern Ireland, Scotland and Wales to clients based in all areas

Head Office:

2 The Parklands
Bolton
BL6 4SE
T: 01204 677 000

E: info@keoghs.co.uk
@keoghslaw
W: keoghs.co.uk
F: 01204 677 111

Belfast | Bolton | Bristol | Coventry | Glasgow | Newcastle | Liverpool | London | Manchester | Southampton

Disclaimer and Copyright Notice

2096/1019/V1/AJ