GOWLING WLG

Article

HOW TO MANAGE THE RISKS OF MASS DATA BREACHES UNDER GDPR

Author

Helen Davenport
Director

Email Helen Davenport

+44 (0)121 393 0174

TOPICS: TECH

20 November 2017

For many organisations, the headline news from the General Data Protection Regulations (GDPR) has been the substantially more significant sanctions that will be imposed for data breaches being up to a maximum of either a fine of €20 million or 4% of annual global turnover, whichever is greater.

There has been less focus on the rights of data subjects to bring claims for damages and that claims can be brought against both data controllers and processors.

However, the cumulative value of data subjects' claims for material **and** non-material damage as a result of an infringement should not be underestimated. Where the number of data subjects affected could be in the thousands, or even millions, even individually relatively small claims for distress will amount to a substantial sum when multiplied by the numbers whose rights have been infringed.

As things currently stand, the Data Protection Act 1998 (DPA) gives individuals a right to compensation from a data controller for a breach of the DPA which results in a pecuniary loss or other material damage, but in usual circumstances only for distress where financial loss has also been suffered. This narrow terminology was challenged in the courts of England and Wales and found by the Court of Appeal to be incompatible with EU law.

The decision in *Vidal-Hall & Ors v Google Inc* [2015] opened the door to additional claims to damages for distress. The Supreme Court granted permission to appeal but the appeal has not gone ahead.

In any case, the GDPR (from its implementation in May 2018) will expressly provide for much wider data subject rights to bring claims for damages - including non-material damage for distress and hurt feelings.

What are the data subject's rights to bring private claims?

Data subjects have a right pursuant to Article 79 to claim for any infringement of the GDPR relating to the processing of their personal data.

Under Article 82(1) GDPR, the scope of liability for infringement is expanded so that any person who has suffered material **or** non-material damage as a result of an infringement of the GDPR by a data controller **or** data processor shall have a right to compensation. This right to compensation is in addition to data subjects' right to complain to the Information Commissioner's Office (ICO) under Article 77 (Article 77).

Data controllers will continue to have the most extensive liability for the damage caused by processing which infringes the GDPR, but for the first time liability is also introduced for data processors - albeit on slightly narrower grounds. They will be liable for damage caused by processing but only where it (or its sub-processor) has not complied with obligations specifically directed to processors or where they have acted outside or contrary to lawful instructions of the controller (Article 82(2)).

To ensure effective compensation, where data controllers and processers are involved in the same infringement, each can be held liable for the entire damage (Article 82(4)). Where one party ends up footing the bill for compensation, that controller or processor can then claim a contribution against the other infringer(s) for their part of the responsibility for the damage (Article 82(5)). Data subjects will be able to bring the same claim against multiple parties or against a sole data controller - a key change under GDPR. In practice the data subjects will go after the softest target which is likely to be the data controller as it has the broadest responsibilities, unless it is unlikely to be good for the money. As a result this, and the increase in the sums at stake, is likely to lead to applications by those being sued to join in the other responsible party to the proceedings or satellite claims for a contribution where liability can be passed on or shared.

The data subject's claim can be brought in the courts of the member state where the data processor or data controller has an establishment or in the data subject's home country (unless the claim is made against a public body). This choice means that at least some degree of forum shopping is likely to get the 'best' damages and ease of access to courts e.g. through class actions. Controllers and processors may therefore face multiple claims in various, unfamiliar jurisdictions outside the member state in which they are established.

Will claims become more commonplace?

The reporting obligations under Articles 33 and 34 mean that there will be more notifications of personal data breaches and, inevitably, the greater the publicity of such breaches, the more claims there are likely to be.

Data controllers will be obliged to report breaches leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data to the ICO within 72 hours (if feasible) unless the breach is unlikely to result in a risk to the rights and freedoms of the data subjects (Article 33). They will also be obliged to report data breaches to affected data subjects where the breach is **likely** to result in a **high risk** to the rights and freedoms of data subjects (Article 34) without undue delay. Data controllers will have to make difficult judgment calls rapidly in order to assess within 72 hours likely risks and also what constitutes a high risk. This will need to be assessed on a case by case basis as, for example, exposure to identity theft and fraud would risk the rights and freedoms of individuals but other cases may not be so clear cut.

Data controllers may also have their hands forced to notify data subjects as the ICO can mandate that the data controller notifies affected data subjects even if the data controller concludes there is no "high risk" to the data subject.

In addition, individuals are becoming more knowledgeable about data privacy and the value of their data and no longer need to suffer a financial loss in order to bring a claim for damages. Inevitably, claimant law firms and claims consultants will exploit commercial opportunities arising from well publicised mass data breaches and unions, pressure and consumer groups could all be instrumental in orchestrating claims. The ability to obtain Group Litigation Orders under the Civil

Procedure Rules makes litigating mass data breaches which, individually may be of low value, commercially lucrative especially when combined with a no win no fee agreement for aggrieved data subjects. The GDPR also envisages that third party not-for-profit public interest bodies will be able to bring claims on data subjects' behalf (Article 80(1)).

What will be the value of such claims?

Special damages, i.e. financial loss, is recoverable (Article 82(1)) subject to the general principles of foreseeability and remoteness. Each case will be fact and evidence specific so it is impossible to give a value as to how much each claim may be worth.

In relation to damages for distress, again, the courts will adopt an evidence based approach to assessing distress which may prove particularly challenging in group actions. Damages awards are likely to remain relatively low but the cumulative effect of a mass data breach where there may be thousands (and conceivably millions) of individuals affected could have very serious consequences. Some recent court decisions give an illustration of the potential levels of damages that may be awarded:

- In *TLT & Others v Home Office (2016)* (currently on appeal), awards of between £2,500 - £12,500 for distress suffered were made per claimant following accidental disclosure of asylum seekers' personal data. There were approximately 1600 people in the family returns process who were affected. Even at the lower level of award, this equates to damages of £4 million if all claimants had claimed and succeeded.
- In *Brown v Metropolitan Police Service (1) and Greater Manchester Police (2) (2016)* an award of £9,000 was made following a serving police officer's personal data being wrongfully obtained by her employer to support a disciplinary enquiry.

So how can you manage the risks associated with mass data breaches?

Defences are limited. Article 82(3) provides that 'a data controller or processor shall be exempt from liability… if it proves that it is not in any way responsible for the event giving rise to the damage'.

This exemption appears narrower than the exemption that can currently be claimed under the DPA by a controller who can prove 'that he is not responsible for the event giving rise to the damage'. This perhaps subtle change reflects the policy of protecting data subjects' rights.

A combination of the following will be needed in order to manage the inevitable risks:

- first and foremost, review existing activities involving the processing of personal data and make sure that there are appropriate technical and organisational measures in place to ensure effective data security. Identify any gaps in current compliance against GDPR and devise and implement any necessary remedial action. Regularly test, assess and evaluate how effective those measures are and update them where necessary.
- a robust data breach detection and incident response policy, as well as staff training are essential. This is especially so in the context of data controllers needing to make quick decisions about the potential impact of the incident on data subjects and whether to notify, and processors being obliged to notify the controller without undue delay after becoming aware of a personal data breach.

- develop a notification procedure, based on an assessment of the personal data you hold and how breaches might be categorised - are they likely to result in a high risk? And at what point and how should they be notified?
- contractual risk transfer. Liability between data controllers and data processors will be apportioned according to: the parties' respective contractual rights and obligations - make sure these are clearly set out; general contractual limits and exclusions of liability; specific caps on liability in respect of data breaches; and the common law duties of care - i.e. negligence. Review and if necessary re-negotiate existing contracts to ensure they are GDPR compliant and that the commercial terms reflect the increased risk - and cost - of non-compliance.
- insurance. This is a new and evolving market with few insurers offering specific cyber risks policies. Will insurance products evolve to address these risks and if so, will they be affordable? For example, TalkTalk received a record fine of £400k under the current regime but potentially that could have been £73 million under GDPR. Would a policy cover that, or a fine of up to 4% of annual global turnover, and if so what would the premium look like? Indeed, is such a fine insurable at law?

Our recent research of 999 large SMEs in the UK, France and Germany showed that less than a quarter of UK businesses are aware of General Data Protection Regulation (GDPR) fines. The research revealed that 'regulatory issues' is one of the key digital risks for these businesses. Take a look at our Digital Risk Calculator to find out your business' digital risk score and identify your top five digital risks.
