

# UK Data Protection Infringement Damages Claim Distress Threshold Not Met

**Date :** October 27, 2021

## Introduction

Claims for compensation for alleged data protection infringements seem to continue unabated including seeking damages where it is claimed distress has been caused as a result. The recent UK court case of Rolfe -v- Veale has however sent out a strong signal with the threshold of alleged distress that has to be crossed in such cases. It could mean that less nuisance or trivial claims are brought. This article sets out highlights of the case.

## What's this all about?

This case concerned a single email (with attachments) about school fees. Due to a one letter difference in the email address of one of the individuals bringing the claim the email went to a person with an identical surname and the same first initial. The (incorrect) recipient responded on the day they received the email indicating that they thought that the email was not intended for them. The law firm who sent the email replied promptly asking the recipient to delete the email (from both their inbox and deleted items folder). The following day the recipient confirmed they had done that.

A claim was then brought to the UK High Court for, amongst other things, damages, including for an alleged data protection legislation infringement that had allegedly caused distress. This was met with an application for so-called "summary judgment" (a means to dispose of a case promptly without a full trial) on the basis that distress was implausible in the circumstances.

Generally-speaking, in principle damages can be obtained for breaches of data protection legislation including for distress caused, and, in principle, loss of control of personal data can constitute damage. But, there needs to be damage, and a claim can't succeed where any possible loss or distress is not made out or is trivial. In a given scenario the question that can arise is to what the threshold is met e.g. for distress.

Here, the law firm argued that those bringing the claim could not have suffered damage or distress above the threshold. Their arguments included the following:

- As regards the nature of the private information in question: no intimate information was involved, the only personal data being names and home address; the only financial details involved were the invoice for school fees and the statement of account of school fees for the previous five years paid by those who brought the claim (neither their bank details nor details of the state of their finances were involved); and, the only location data involved was the school address and the home address of those bringing the claim; and,
- As regards the circumstances of disclosure: this was to one individual only, accidentally as a result of a typographical error; the individual notified the error the same day and the next day, when asked to delete the email and confirm that this had been done, the individual did so two and a half hours later; and, the email was encrypted.

Those bringing the claim argued that the distress threshold had been crossed, including on the basis that:

- They had lost sleep worrying about the possible consequences of the data breach which "had made them feel ill". Much of the alleged distress stemmed here from the "fear of the unknown" in terms of who the (incorrect) recipient might have been, given that the profession of one of those bringing the claim was an IT specialist.

## What was the ruling?

The ruling was as follows:

- This was a case of: (a) “minimally significant information, nothing especially personal such as bank details or medical matters, a very rapid set of steps to ask the incorrect recipient to delete it (which she confirmed) and no evidence of further transmission or any consequent misuse (and it would be hard to imagine what significant misuse could result, given the minimally private nature of the data)”; and, (b) “a frankly inherently implausible suggestion that the minimal breach caused significant distress and worry or even made them 'feel ill'. In my judgment no person of ordinary fortitude would reasonably suffer the distress claimed arising in these circumstances in the 21st Century, in a case where a single breach was quickly remedied”;
- The threshold could not therefore be crossed and, according to the ruling, “it is not appropriate for a party to claim, (especially in the in the High Court) for breaches of this sort which are, frankly, trivial”; and,
- Those who'd brought the claim would have to pay the costs of the case, and provide an interim payment of £11,000 (around US\$ 15,000).

## What are the takeaways?

Although this case was decided by a “Master” (a judge of limited jurisdiction, albeit in the higher courts) it still makes it clear that data protection infringement compensation claim cases involving trivial incidents where no real distress has been caused are unlikely to succeed.

Despite this however, we'd expect that some individuals and their lawyers will not be deterred and will continue to bring these cases. We're often seeing the same claimants and law firms crop up time and time again with relatively small claims for data protection and cookies matters and some are becoming increasingly more inventive in the claims they are making. Organizations should therefore be prepared and consider managing these cases with care. In England & Wales, the rules governing these cases can be complex. Often allegations are also included on other legal grounds such as misuse of confidential information, breach of confidence, and negligence. But, by taking the time to understand the process, an organization can get hands-on with a claim brought against it at a very early stage and be equipped to deal with it effectively.

Some of the practical steps an organisation might want to consider include:

1. Carefully checking email recipients and making sure there is training on this. In some cases software can help. Consider whether email messages should be encrypted too.
2. Having a proper response procedure in place to respond to events. This will usually include putting in place immediate measures to reduce the likelihood or harm and prevent a repeat. We have built up a list of actions an organisation can take to remediate and mitigate after a breach which we usually work through with a client after an event to reduce the harm quickly.
3. Make sure that you deal with any claim promptly and properly. If you're insured you'll want to make contact with your insurers straight away. Even nuisance claims can be harmful especially when the business model for some seems to be to extract a small amount of money and then publicise it to hit the organisation with repeat claims. Good lawyers who know their way around developments in the law in this area will be essential.

## Resources

Cordery's GDPR Navigator subscription service is an expansive set of resources and a community of peers helping companies deal with GDPR and related issues. GDPR Navigator includes short films, straightforward guidance, checklists and regular conference calls to help you comply. More details are at [www.bit.ly/gdprnav](http://www.bit.ly/gdprnav).

We've written about data protection compensation issues before including here

<https://www.corderycompliance.com/data-protection-breaches-and-compensation-litigation-issues-for-consideration/> and here <https://www.corderycompliance.com/scope-restrictions-data-breach-comp-claims/> and here <https://www.corderycompliance.com/aven-v-orbis-compensation-awards/>.

The court's judgment can be found here <https://www.bailii.org/ew/cases/EWHC/QB/2021/2809.html>.

We report about data protection issues here <https://www.corderycompliance.com/category/data-protection-privacy/>.

We report about compliance issues here <https://www.corderycompliance.com/news/>.

For more information please contact André Bywater or Jonathan Armstrong who are lawyers with Cordery in London where their focus is on compliance issues.

[Jonathan Armstrong](#), Cordery, Lexis House, 30  
Farringdon Street, London, EC4A 4HH  
Office: +44 (0)207 075 1784  
[Jonathan.armstrong@corderycompliance.com](mailto:Jonathan.armstrong@corderycompliance.com)



[André Bywater](#), Cordery, Lexis House, 30  
Street, London, EC4A 4HH  
Office: +44 (0)207 075 1785  
[Andre.bywater@corderycompliance.com](mailto:Andre.bywater@corderycompliance.com)

Farringdon

