ASSESSING THE VALUE OF CLAIMS FOR BREACHES OF THE GDPR

A SHORT GUIDE FOR BUSINESSES

Authored by: Mariya Peykova (Barrister) - 3PB

The rise of GDPR[1] compensation claims

In recent years courts have seen an increase in the number of claims for compensation under the GDPR. Claims are often brought against business entities such as banks or other institutions that store and handle personal data. A large number of these claims are issued by litigants in person, who are unable to properly assess the substance and value of their claim. In-house legal departments must be in a position to advise on the likely value of the claim (and thus track allocation and costs implications), evaluate and make settlement offers, inform funding decisions and overall strategy, as well as make the right call about whether (or when) to seek advice and/or representation from specialist counsel. However, businesses may find these decisions difficult or impossible to make where the actual likely value of the claim is difficult to ascertain.

Compensation: Article 82 GDPR

Article 82 of the GDPR provides data subjects with a right to compensation for material or non-material damage suffered as a result of a breach of the GDPR.[2] Whilst those who seek compensation for material damage will need to prove that they have suffered pecuniary loss, it now appears to be accepted that a Claimant who seeks compensation for non-material damage does not need to establish pecuniary loss, although there is at present limited guidance on what exactly amounts to 'non-material damage'. In Lloyd v Google [2021] UKSC 50 the Supreme Court reviewed the law relevant to compensation under the old data protection regime and concluded that the term 'damage' must involve financial loss or distress, and that compensation should not be recoverable for trivial damage.

In UI v Österreichische Post AG, Case C 300/21 (4th May 2023), the CJEU determined that Article 82 of the GDPR does not provide for compensation for mere infringement of an individual's data protection rights. Instead, a data subject must demonstrate that there has been an infringement, and the data subject has suffered damage (material or non-material) caused by the infringement. The Court rejected the view that to attract compensation, a non-material damage claim must reach a certain threshold of seriousness, and held that negative consequences caused by an infringement will not attract compensation unless such negative consequences amount to 'non-material damage'.

1 References to the GDPR are to the UK GDPR. The UK GDPR is the retained EU law version of the EU GDPR, which forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of s.3 of the European Union (Withdrawal) Act 2018, as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419). It is defined in section 3(10) of the Data Protection Act 2018 (DPA 2018), and supplemented by section 205(4). With effect from 1 January 2021, there are two legal texts to consider, where relevant: the UK GDPR as well as the DPA 2018.

2 This does not apply to the processing of data by individuals in the course of purely personal or household activity, the processing of data for law enforcement purposes, and intelligence services processing. The Data Protection Act 2018 provides for this.

Whilst CJEU case law is no longer binding, it seems likely that domestic courts will follow the same line of reasoning.[3] At the time of writing this article, there is no reported case law on a pure GDPR claim for compensation. However, guidance can be derived from reported authorities in which the claims consist of two or more causes of action, such as claims for misuse of private information and breaches of the GDRP.[4] Such claims yield higher awards in compensation, although the principles applied by the court when assessing quantum would be the same whether dealing with a pure GDPR claim, or a hybrid privacy claim.

It is now becoming clear that English courts are reluctant to encourage claims for relatively minor data protection breaches, although they have not introduced a threshold of seriousness. On the present state of the law, Claimants who seek compensation for non-material damage would need to establish that the breach has caused them distress. In assessing quantum, courts will refer to the Judicial College Guidelines;[5] a useful yardstick in gauging the likely level of an award will be to 'cross-reference' with personal injury awards for psychiatric and psychological injury, as per Warby J in TLT v Secretary of State for the Home Department [2016] EWHC 2217 (QB).

The following factors are likely to be of relevance in assessing where within the notional bracket an award is likely to fall:

01 The nature and content of the private information revealed. The more private and significant the information, the greater the effect on the subject will be (or will be likely to be);

02 The scope of the publication/ disclosure. The wider the publication, the greater the likely invasion and the greater the effect on the individual.

03 The presentation of the publication/disclosure. Sensationalist treatment might have a greater effect, and amount to a more serious invasion, than a more measured publication.

04 The likely individuals who will access or be perceived as likely to access such information.

05 The Court will take a sensible approach to whether or not there is or was likely to have been real interest in the disclosure.

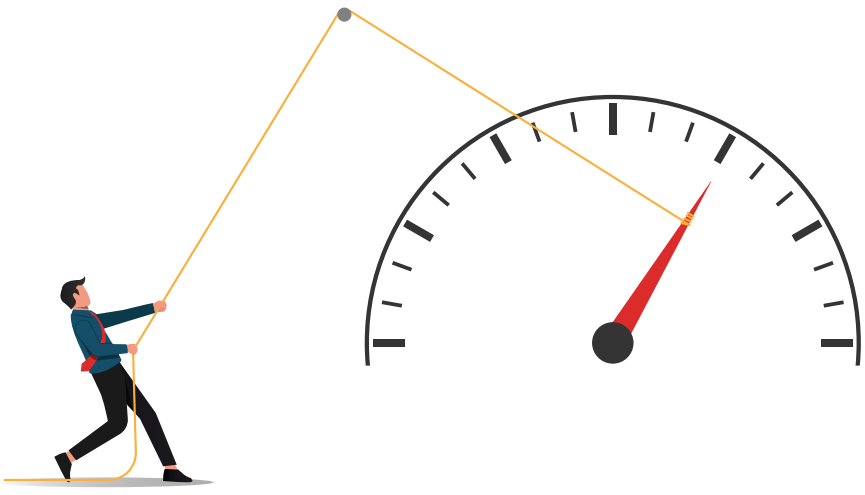
Courts have awarded compensation for distress by reference to the above principles. For example, in Halliday v Creation Consumer Finance Ltd [2013] EWCA Civ 333, £750 was awarded for a data protection breach despite the lack of medical evidence. In ST (A Child) v L Primary School [2020] EWHC 1046 (QB), the court awarded damages of £1,500 for misuse of personal information in a case where there was "limited evidence of direct impact" on the Claimant. In ST reference was made to the decision of TLT referred to above, where awards of between £2,500 and £12,500 were made to asylum seekers whose details had been erroneously made public.

Practical advice for in-house legal departments

Pure data protection claims will usually be dealt with in the County Court. The value of such claims is unlikely to exceed the threshold for allocation to the fast track or multi-track. In the absence of unreasonable behaviour, Defendants cannot recover their costs on the small claims track, and this is something to bear in mind when advising Defendants on settlement options.

Claims associated with higher compensation will usually involve additional causes of action, such as a claim for misuse of private information or a breach of confidence claim, and are highly likely to be transferred to the High Court.

Advising defendant businesses on claims for breaches of the GDPR includes considering both reputational and cost implications. Seeking legal advice from specialist counsel early on is crucial, sometimes even more so where the claim is brought by a litigant in person. Often, litigants in person will present a claim as a pure GDPR claim, but the facts in the pleadings may point to additional causes of action (in tort, for example). In these circumstances, legal advice from specialist counsel should be sought as soon as possible on the best course of action.



3 Lower value GDPR claims are already dealt with in the County Courts. See Emma Louise Johnson v Eastlight Community Homes Ltd [2021] EWHC 3069 (QB),Cleary v Marston (Holdings) Ltd [2021] EWHC 3809 (QB), and Stadler v Currys Group Ltd [2022] EWHC 160 (QB).

4 See Bekoe v Mayor and Burgesses of the London Borough of Islington [2023] EWHC 1668 (KB).

5 In Gulati v MGN Ltd [2015] EWCA Civ 1291 it was said that damages awards for misuse of private information should bear a "reasonable relationship" with awards in personal injury cases.