CASE NOTES:
Farley v Paymaster in the Court of Appeal

NOTHING TO FEAR FROM FEAR ITSELF: *FARLEY V PAYMASTER* IN THE COURT OF APPEAL

On Friday 22 August 2025, the Court of Appeal handed down judgment in *Farley v Paymaster* [2025] EWCA 1117, overturning the decision of Nicklin J which had struck out almost all of the cases brought as part of a collective action under the pre-Brexit EU GDPR regime and the Data protection Act 2018.

As well as having implications for a broad swathe of data protection claims, and for those advising data controllers, the judgment is significant in the approach to post-Brexit decisions of the European courts

This case note, co-authored by Gareth Shires and Alistair Mackenzie of 2 Temple Gardens, highlights key factors in the judgment.

Gareth Shires

Alistair Mackenzie

The Facts of the Case

The Defendant administrated a pension scheme for the Sussex Police. In August 2019, the Defendant mistakenly sent over 750 Annual Benefit Statements to the wrong addresses. While, through various means, 102 such statements were eventually returned to the Defendant unopened, a significant majority of the statements were never recovered and what happened to them remains unknown.

Over 470 current or former officers brought claims under the GDPR and the DPA 2018, as well as a claim for misuse of private information, which the Defendant applied to strike out. By the time of the hearing before Nicklin J, the claims for damages for "loss of control" had been abandoned on the basis of the Supreme Court's decision in *Lloyd v Google*, and the losses claimed were (i) for anxiety, alarm, distress and embarrassment caused by the fact that personal data had or may have passed into the hands of third parties, and (ii) in respect of a small set of claimants, for exacerbation of pre-existing medical conditions.

In the first instance judgment, it was held that to have a viable claim for data protection, a claimant must show that they have a real prospect of demonstrating that their data was in fact disclosed to a third party. On that basis, all of the claims were struck out apart from 14.

By the time of the appeal, the Claimants had filed an amended claim abandoning the claim in misuse of private information and the assertion that their information had fallen into third party hands. Their claim was instead formulated on the basis that their emotional distress was caused by the fear that their data may have passed into the hands of third parties.

Infringement without Disclosure

The Court of Appeal, in a judgment of Warby LJ, held that Nicklin J had failed to properly apply the legislation.

The GDPR (now UK GDPR) imposes obligations on data processors, including compliance with the six principles identified in Article 5 (e.g. data minimisation, purpose limitation, integrity and confidentiality). Processing by a data processor is given a deliberately broad definition by Article 4 GDPR and s.3(4) DPA, which includes not only disclosure of data but also collection, recording, organising and storing.

The data breaches in the case occurred as a result of the manner in which the data had been processed. While the Claimants had alleged that their data had or may have been disclosed to third parties, the Court of Appeal held that this was not pleaded as part of their case on breach, but in support of their allegations as to damage and distress, such that there was no basis to strike out their claims.

This is an unsurprising conclusion: numerous obligations are placed on data controllers under the legislation particularly as regards to processing of data, which can be infringed in

various ways; making disclosure an additional requirement for breach would be to limit the scope of the legislation.

No "Threshold of Seriousness"

An important argument raised by the Defendant was that the data protection legislation, as it applies in the UK, is subject to a *de minimis* principle, expressed as a minimum threshold of seriousness which must be met before the damage is actionable.

Warby LJ rejected arguments often relied upon by defendants in data protection cases that this issue had already been determined as a matter of English law. Neither the Supreme Court in *Lloyd v Google* nor a trio of English first instance cases supported the argument for a threshold of seriousness.

Instead, Warby LJ held that it was appropriate to adopt the same approach as in a series of post-Brexit CJEU cases, which expressly rejected the existence of any such threshold.

An Objective Test

The guidance to be derived from those post-Brexit cases, Warby LJ held, went beyond refusing to recognise a *de minimis* threshold. Those cases also indicate that there is an objective element to any claim. While fear of the consequences of an infringement of a data subject's rights can give rise to a claim for compensation, it is a requirement that that the alleged fear is itself objectively well-founded; purely hypothetical or speculative fears will not give rise to a claim for compensation.

How this objective element will be applied is likely to be a matter of significant litigation going forward. Some guidance may be derived from Warby LJ's rejection of the submission that the fact that the claimants in *Farley* could not prove their statements were opened and read did not of itself show that their fears were ill-founded; as he noted, the test must be applied by reference to the facts as known (or unknown) at the time the fear was experienced.

Going forward, the Court of Appeal has made clear that in data protection claims it will be for each claimant to plead and to prove a reasonable basis for suffering the non-material damage (e.g. distress, fear, anxiety) in respect of which their claim is brought.

The European Aspect

One of the most important aspects of the judgment for all lawyers is Warby LJ's approach to the post-Brexit decisions of the CJEU on the "threshold of seriousness" question. While being clear that those cases were not binding on English courts, he also held that a judicial decision to plot a different course that that taken by the CJEU would call for compelling legal reasons. In doing so, he gave weight to GDPR's status as "an international legal instrument".

Farley was a case decided under EU GDPR, with the breaches having occurred prior to IP-completion day. However, the Court of Appeal made clear that on the relevant issues it regarded the UK GDPR as having identical language and it was not suggested that any of the issues would have been resolved differently under UK GDPR. This is not a surprising conclusion, as the wording of the UK GDPR is almost identical to that of the EU GDPR, although it remains to be seen whether that will remain the case.

For further details on 2TG's Data Protection and Group Litigation practices, or to contact Gareth or Alistair, please contact clerks@2tg.co.uk.