ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS

DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Paying compensation under UK data protection law

The Court of Appeal lowers the bar for data protection compensation in *Farley v Paymaster*. The case now goes to the Supreme Court. By **Victoria Hordern** of Digiphile.

In what circumstances is an organisation required to pay compensation to individuals under data protection law? It's widely understood that a technical contravention of the GDPR does not automatically give rise to a right to claim damages. There must be evidence that an individual has suffered harm. What evidence is necessary to show that a GDPR contravention has taken place and

Continued on p.3

How the Online Safety Act and UK data protection laws converge on protecting children

Will compliance with one regime place organisations at risk under the other? By **Mercedes Samavi** and **Georgia Wright** of Morrison Foerster.

Understanding when and how children are at risk of exposure to harmful or illegal content is central to the UK Online Safety Act (OSA). As a marked departure from earlier (reactive) regimes, the OSA does not simply impose duties where children

Continued on p.5

Issue 143 **JANUARY 2026**

See the publisher's blog at privacylaws.com/blog2026jan

UNITED KINGDOM
report

ISSUE NO 143 JANUARY 2026

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Victoria Hordern
Digiphile
Mercedes Samavi and Georgia Wright
Morrison Foerster
Jenai Nissim and Claire Saunders
HelloDPO Law Ltd
Nel Anna Krzeslowska
PL&B Researcher
Jade Kowalski
DAC Beachcroft LLP
Hannah Heilbuth
University of Nottingham

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* United Kingdom Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2047-1479

comment

Things to look out for in 2026

In December, I was pleased to welcome some of our readers to the *PL&B Meet the Correspondents* event, generously hosted by Stephenson Harwood, where four of our brilliant regular correspondents – Katie Hewson, Stephenson Harwood; Emma Erskine-Fox, TLT; Nicola Fulford, Hogan Lovells; and Victoria Hordern, now Digiphile – spoke about topical data protection issues.

This half-day networking event was so well received that we expect to repeat it in 2026. In the meantime, I am excited to announce another regular correspondent to the pool of writers, Mercedes Samavi at Morrison and Foerster – see their article about the Online Safety Act (OSA) (p.1).

OSA's regulator, Ofcom, will be busy in 2026 – its list of key implementation deliverables under the Act starts with publishing its final guidance in February 2026 on super-complaints. This concept means that designated bodies such as consumer groups can raise systemic issues with the regulator, rather than it dealing with individual complaints.

On the legislative agenda we now have the Cyber Security and Resilience Bill which has just been through the second reading in the House of Commons (p.20). The ICO has welcomed the Bill by saying that it is an important piece of legislation that will strengthen the country's cyber resilience and ultimately better protect people's data. It plans to take a proactive, risk-based oversight approach.

On AI, the UK has chosen a sector-specific approach and empowering existing regulators to apply rules within their sectors (p.14). We may in 2026 see an AI Bill with a limited scope and a provision on regulatory sandboxes.

The next developments in AI and Copyright are expected in March with the publication of a progress statement as per the Data (Use and Access) Act 2025. The government will issue an economic impact assessment as well as a report on the use of copyright material in the development of AI systems.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

Compensation... from p.1

that harm has occurred? Is anxiety over potential data misuse sufficient and, if yes, what level of anxiety needs to be experienced to give rise to a right to compensation?

Past UK case law demonstrates that successfully claiming compensation for data protection law contraventions is not easy and that amounts awarded for compensation by the courts tend to be low. In *Farley v Paymaster (1836) Limited* [2025] EWCA Civ 1117[1] published on 22 August 2025, the Court of Appeal was asked to consider an appeal from an order striking out individual claims in a collective action which arose due to a data security breach. The High Court had already considered the facts as they applied to over 400 individuals and decided that only 14 could show an arguable case. The appellants before the Court of Appeal were an additional 432 individuals who considered they should be able to claim compensation.

What happened?

The appellants were all former or current police officers for Sussex Police. They were also all members of a pension scheme set up by the police and administered by Paymaster (trading as Equiniti). In August 2019, Paymaster sent annual benefit statements to members of the scheme. However, it transpired that more than 750 of those statements were sent to out-of-date residential addresses. Sussex Police had properly provided Paymaster with up-to-date addresses but unfortunately, when the statements were produced, a system error picked up the previous address. The statements themselves contained information about the relevant member's date of birth, national insurance number, details of their police service, salary details as well as accrued and forecast pension benefits.

Many of the statements were returned to Paymaster unopened as recipients had realised that the statements were not intended for them and had acted in good faith. A number were forwarded by the recipient to the relevant scheme member and others were retrieved by the officers themselves. However, the majority of statements were not recovered so that their fate was unknown. These facts were not in dispute. It's worth noting that these circumstances did not involve a sophisticated cyber incident and none of the data exposed was special category data. The claimants sought damages for breach of the GDPR and Data Protection Act 2018 and/or misuse of private information (the latter head of claim was later abandoned). Paymaster argued that the claims did not meet the applicable threshold of seriousness (i.e. the claim for damage or distress did not exceed a *de minimis* level) and/or was an abuse of process.

The issues that the Court examined were:

(1) Have the appellants set out a reasonable basis for claiming that the mistake by Paymaster involved processing of personal data that was an infringement of the GDPR?

(2) If so, have the appellants stated a basis for claiming compensation under the GDPR and Data Protection Act 2018 that is reasonable, and that has a realistic prospect of success at trial?

(3) Are the claims nonetheless an abuse of process under UK law?

Issues (1) and (3) did not take up much of the court's time. The focus was on the second issue and the grounds for claiming compensation.

Background context

Following the data security breach, Sussex Police informed the Information Commissioner's Office (ICO). The ICO considered no further action was required since the police had conducted a risk assessment that concluded that the risk to individuals was unlikely to be significant.

Sussex Police had engaged Paymaster as the administrator of the pension scheme and there were indications that both parties had understood Paymaster to be a processor when entering into that arrangement. Lord Justice Warby (LJ Warby), giving the judgment in the Court of Appeal indicated, however, that there was now a "live dispute" (14)[2] on what role Paymaster played and the court decided to consider the allegations by treating Paymaster as a controller, not a processor. Nowhere does the decision discuss the implications were Paymaster to be a processor, albeit processors also have security responsibilities and can be required to pay compensation.

In the High Court[3], the judge had struck out all but 14 of the claims by the scheme members. This was because the judge considered that any viable claim must involve a claimant being able to demonstrate that they had a real prospect of demonstrating that the benefit statement was opened and read by a third party. Following the High Court decision, the appellants recharacterised their claim. They alleged that the processing of their personal data breached statutory duty and that Paymaster had caused them to suffer anxiety, alarm, distress and embarrassment in fear that their personal data may have been passed to unknown third parties. Paymaster countered that police officers "used to contending with dangerous and upsetting situations" cannot "have been genuinely distressed over a pensions forecast sent to an old address" (26). The ICO, for its part, acting as Intervener in this case, confirmed that the activities of Paymaster did involve data processing under GDPR and that there was no *de minimis* principle to apply in this context.

GDPR infringement

A core question for the court was whether the conduct of Paymaster involved processing personal data. It may sound surprising that there was any ambiguity on this point. However, since the processing involved both an automated electronic element (addresses stored on a computer) and a manual element (the printing of hard copy documents then placed into envelopes and sent by post), it was worth clarifying. Indeed, the ICO (in its role as Intervener) argued that a "segmented or atomised approach to what went on here would be artificial and wrong in principle" (38). It was accepted that the concept of processing including any operation or set of operations is broad in scope. Indeed, LJ Warby referred to the 2024 Court of Justice of the EU (CJEU) decision of *Endemol Shine Finland Oy* C-740-22[4] to draw the observation that "where a data controller is responsible for the oral disclosure of personal data that has previously been processed by automated means, the oral disclosure forms part of the processing" (38). In other words, this cannot be deployed as a crafty way to circumvent the application of data protection law. LJ Warby considered that, though the UK courts are not bound by CJEU decisions, European rulings remain persuasive. As such, in several places LJ Warby chose to follow CJEU jurisprudence.

The appellants alleged that the actions of Paymaster involved multiple GDPR infringements, in particular breaches of data minimisation and accuracy, as well as breaches of lawfulness and fairness.

Compensation claim

This was the most complex part of the court's decision. Data protection practitioners broadly agree that it would be absurd if every GDPR infringement led to a claim for compensation. A system that entitled individuals to compensation for every GDPR infringement, however minor, would be unsustainable. Therefore, the court considered the evidence put forward by the appellants to determine whether their compensation claims under GDPR had merit. Article 82 GDPR provides the right for a person to receive compensation from a controller for material (i.e. financial loss, physical injury) or non-material damage (which includes distress) suffered as a result of an infringement. The appellants set out two generic allegations as a result of the incident: (i) the experience of anxiety, alarm, distress and embarrassment, and (ii) the aggravation of a pre-existing medical condition.

Paymaster considered it was "simply unreal" for the appellants to have a genuine belief that their data had been passed to a third party and been misused. Therefore, Paymaster cast doubt on the levels of distress referred to, essentially implying that many appellants were exaggerating. Indeed, Paymaster argued that compensation should not be recoverable for emotional responses other than distress. LJ Warby did not accept this but indicated that compensation is not available for all emotional responses to an infringement. Instead the court looked to the recitals to the GDPR (in particular recital 85) and to the way the CJEU approaches compensation for non-material harm.

In considering the European angle, LJ Warby observed that the CJEU has consistently ruled that domestic EU courts cannot require proof that the damage suffered due to a GDPR infringement reaches a minimum threshold of seriousness. Essentially, the CJEU wants to guard against Member State courts decreeing a specific bar which a person has to clear in order to claim compensation. On the other hand, Paymaster argued that the UK's Supreme Court decision in *Lloyd v Google*[5] and the Court of Appeal's decision in *Prismall v Google Ltd*[6] meant that data protection law in England includes a threshold of seriousness. But LJ Warby was not persuaded that these UK decisions led to a threshold in the UK and preferred to follow European reasoning. Significantly, one of the points made by LJ Warby was the status of the GDPR as an international legal instrument, and the CJEU's consistent aim to uphold the level of protection afforded to individuals. But that line of reasoning did not mean that any mere infringement conferred a right to compensation – damage within Article 82 must still be proven.

LJ Warby cited the ruling in the CJEU's decision from 2024 in *VB v Natsionalna agentsia za prihodite* C-340/21[7] as accepting that fear experienced by an individual that their personal data will be misused (so long as the court considers such fear is well-founded) can constitute non-material damage. LJ Warby concluded that "in principle a claimant can recover compensation for fear of the consequences of an infringement if the alleged fear is objectively well-founded but not if the fear is (for instance) purely hypothetical or speculative" (75). The issue therefore is whether the fear is well-founded and LJ Warby considered this needed to be assessed using an objective standard or test of reasonableness. So, for instance, what difference did it make to appellants who were aware that their benefit statement had never been opened and read by a third party? Paymaster argued that for those individuals, their fears were not well-founded. However, LJ Warby did not accept this. Significantly, the reasonableness test must be applied, in his view, with reference to the facts and matters known to the appellant at the time they experienced the stated fear. So, a person can hold well-founded fears about future harm even if no such harm ever happens.

Nevertheless, in this instance, an appellant must still prove a reasonable basis for fearing: (i) that their benefit statement had been or would be opened and read by a third party, and (ii) that this would result in identity theft or one of the other consequences feared. The next aspect for discussion was how likely someone would open correspondence that was not addressed to them, the chances of the information in the statement being misused, and the fact that, in the years after the event, no evidence had emerged of misuse. LJ Warby was clear that appellants were still required to state a specific and reasonable basis for fearing that, in their particular case, the envelope would be opened and the statement read, and state the particular circumstances why they had a reasonable basis for fearing that the information might be misused. However, LJ Warby declined to review each schedule presented by the appellants to determine whether each individual met these requirements, and therefore remitted this exercise back to the High Court.

A subset of the appellants argued that the incident had aggravated an existing medical condition. LJ Warby considered that the exacerbation referred to could potentially be classified as material damage since these were forms of psychiatric harm that are recognised as personal injuries. However, existence of this group who alleged that the incident aggravated their existing medical condition did not sway his prior reasoning. He argued "these claims will stand or fall according to the court's conclusions on the objective reasonableness of the stated fears" (92). On the other end of the scale, LJ Warby allowed that claims for compensation based on annoyance or irritation caused by fear of third party misuse can be permitted, provided the fear is well-founded. But fleeting or transient subjective reactions of annoyance may not qualify as non-material damage in his view.

Abuse of process

LJ Warby also considered whether the appellants' claim was an abuse of process based on jurisprudence from *Jameel v Dow Jones Inc* [2005] EWCA Civ 75[8]. This established that proceedings may be abusive where they are objectively pointless and wasteful. While LJ Warby acknowledged that any compensation paid to appellants in the Paymaster case would likely be small, he stated that "the modest scale of the likely recovery cannot of itself be sufficient to justify dismissal of the claim" (101). In fact the real reason that Paymaster was likely to be arguing abuse of process was, in LJ Warby's view, the scale of the costs that the appellants had run up with their legal team. However, LJ Warby dismissed the notion that the appellants were abusing the process.

What are the implications?

The Court of Appeal won't be the final word. Permission to appeal their decision was lodged with the UK Supreme Court in November. There are significant implications bound up with what the court decides. Indicating that there is no threshold of seriousness could lead to a flurry of activity from lawyers and claims companies alike albeit the *Lloyd v Google* decision will still circumscribe representative actions. Likewise, not having to prove actual damage but only that you had a well-founded fear broadens the circumstances for making a claim. This development could prompt more individuals to seek compensation following data security breaches, and companies to more readily pay compensation to avoid litigation. Individuals might also lay claim to well-founded fears where they have been tracked online or their personal data has been used for training an AI model. We will need to wait to see the final outcome in *Farley v Paymaster*. However, with this recent decision, the pendulum has partly swung back towards individuals.

AUTHOR

Victoria Hordern is Privacy, Data and AI Partner, Digiphile.
Email: vicky.hordern@digiphile.law

REFERENCES

1 www.bailii.org/ew/cases/EWCA/Civ/2025/1117.html
2 The numbers in brackets in this and subsequent quotations refer to the paragraphs in the court's judgment.
3 www.bailii.org/ew/cases/EWHC/KB/2024/383.html
4 curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-740/22
5 www.supremecourt.uk/cases/uksc-2019-0213#judgment-details
6 www.judiciary.uk/wp-content/uploads/2024/12/Prismall-v-Google-UK-Ltd-Approved-judgment-11.12.24.pdf
7 curia.europa.eu/juris/documents.jsf?num=C-340/21
8 www.bailii.org/ew/cases/EWCA/Civ/2005/75.html