

IN THE SUPREME COURT
ON APPEAL FROM THE COURT OF APPEAL
[2025] EWCA Civ 1117
BETWEEN:

PAYMASTER 1836 LIMITED (t/a EQUINITI)

Appellant

-and-

MR MICHAEL FARLEY
(& 431 others set out in the Annex to the Claim Form)

Respondents

-and-

(1) THE INFORMATION COMMISSIONER
(2) OPEN RIGHTS GROUP

Interveners

OPEN RIGHTS GROUP'S WRITTEN SUBMISSIONS

A. SUMMARY

1. Open Rights Group (“**ORG**”) has been granted permission to intervene in the appeal in support of the Court of Appeal’s conclusion that a seriousness threshold does not apply to claims for non-material damages under Article 82 of the GDPR.¹
2. ORG is a UK-based non-profit organisation that was founded in 2005. It has a particular focus on promoting and upholding privacy and data protection rights, including effective means of redress for infringements of those rights. It has significant experience in matters concerning the Data Protection Act 2018 (“**DPA 2018**”) and General Data Protection Regulation 2016/679 as introduced in the EU (the “**EU GDPR**”) and re-adopted expressly (with minimal amendments) by Parliament through the “**UK GDPR**”. For ease of reference, and in circumstances where the UK GDPR has not been included within the authorities bundle, these written submissions primarily refer to the “**GDPR**” throughout.

¹ See the Supreme Court’s Order of 31 July 2026.

3. The Appellant's Grounds of Appeal suggested at §20 that the Court of Appeal's [237] conclusion on the threshold of seriousness issue "*cannot have been the intention of the legislator and is only, ultimately, to the benefit of those law firms who now have every motivation to continue to seek out such claims (often based on an unintentional, technical breach)*". ORG fundamentally disagrees. It seeks in this intervention to highlight two sets of key systemic/policy issues underpinning the correct interpretation and application of the GDPR against which the appeal falls to be determined.
4. **First**, the Court of Appeal's rejection of a seriousness threshold promotes the overall aims of the GDPR of securing a "*high level of protection*" for personal data. In particular, the introduction of a seriousness threshold would undermine or, indeed, be incompatible with, that high level of protection. Adopting such a threshold could, in particular, rule out redress in a large number of cases where individual claims would be unviable due to their limited value, but the breach involved has impacted potentially thousands (and on occasion, millions) of data subjects. Cases of mass harm have become increasingly common as a result of the rapid pace of technological change. A core purpose of the GDPR is to deter controllers from non-compliance. Making it harder for data subjects to make claims would weaken the incentives of data controllers to comply with their obligations. Indeed, introducing a test of seriousness will likely lead to further protracted litigation as Defendants seek to dismiss claims on this basis, even where they have admitted liability for a breach in principle.
5. **Second**, ORG submits that the appeal has ramifications for the free flow of data between the UK and EU and the digital economy more widely, including, in particular, the issue of divergence from CJEU judgments following IP Completion Day. As the Court of Appeal correctly noted in its judgment, the GDPR has a clear international dimension. When deciding whether to follow post-IP Completion Day caselaw of the Court of Justice of the European Union ("**CJEU**"), the Courts should have regard to the implications of divergence between the interpretation and application of the UK and EU GDPRs for EU-UK data flows, in particular having regard to possible impacts on the UK's "adequacy status" pursuant to Article 45 EU GDPR. A conclusion that a seriousness threshold applies under Article 82 of the UK GDPR, where it does not apply under Article 82 of the EU GDPR, could have a material bearing on that status.

6. Both matters are highly relevant to the question of statutory interpretation before the Supreme Court. It is well-established that the Court should assess the likely consequences of adopting rival constructions, both to the parties in the case and for the law generally: see for example *R (PACCAR Inc) v Competition Appeal Tribunal* [2023] 1 WLR 2594, per Lord Sales at §§223(iv) and 241, citing with approval *Bennion, Bailey and Norbury on Statutory Interpretation*, 8th ed. (2020) at section 11.6.

B. THE EFFECTIVE PROTECTION OF DATA RIGHTS

7. The Court of Appeal’s conclusions promote the overall aims of the GDPR of securing a “*high level of protection*” for personal data. Those aims are apparent from the Recitals to the GDPR², which refer to:
- a. the need for “*a high level of the protection of personal data*” (Recital 6), a “*strong and more coherent data protection framework in the Union*” (Recital 7); [660]
 - b. the need to ensure a “*consistent and high level of protection of natural persons*”, thereby removing the obstacles to flows of personal data within the Union through the consistent application of data protection rules (Recital 10); and [660]
 - c. the need to ensure “[*e*]*ffective protection of personal data throughout the Union*” through “*strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States*” (Recital 11). [661]
8. The link between those aims and the scope of the Article 82 right to compensation is clear from Recital 146, which provides “[*t*]he concept of damage should be broadly [685] interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. ... Data subjects should receive full and effective compensation for the damage they have suffered”.

² The Recitals to the EU GDPR are retained as introductory text to the UK GDPR. Their relevance is considered below at §10.

9. Brexit has not made any difference to these overarching objectives. Article 1(1) UK [690] GDPR makes clear that the Regulation’s purpose continues to be to lay “*down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.*” Article 82(1) continues [739] to provide that: “*Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.*” Protection of personal data is an area in which Parliament has expressly maintained the core European law framework (for reasons explored in more detail in Section C below).

10. A similar situation was considered by this Court in its judgment, per Lord Sales, in C.G. Fry & Son Limited v Secretary of State for Housing, Communities and Local Government [2026] 1 All ER 615, which concerned the Conservation Habitats and Species Regulations 2017. This legislation had initially been made to give effect to the EU Habitats Directive.³ At §51 of its judgment, the Court concluded that “[t]he purpose of [922] the Habitats Regulations is to implement and follow the Habitats Directive in pursuing the same objective. Brexit has made no difference to this.” In identifying the purpose of the Habitats Directive, the Supreme Court placed weight on its Recitals (§§47-48). In the [922] present case, the Court of Appeal was also correct at §53 to recognise the importance of [155] the Recitals to the GDPR to its exercise in statutory interpretation.

11. The objectives identified above also feature heavily in the various CJEU judgments relied on by the Court of Appeal. For example, see UI v Österreichische Post AG, Case C-300/21, [2023] 1 WLR 3702 (“**UI**”) at §§46-48, the reasoning of which the Court of [1884] Appeal accepted at §71. [160]

12. ORG endorses the way in which the Court took into account the overall aims of the GDPR and adds the following four submissions.

13. **First**, the Court of Appeal’s conclusions help ensure that data rights are effectively protected and that wrongdoing is remedied. A seriousness threshold would render GDPR

³ Council Directive 92/43/EEC of 21 May 1992 on the conservation of natural habitats and of wild fauna and flora.

rights illusory in large numbers of cases where damage has been suffered but does not necessarily meet an unpredictable threshold set by the courts.

14. As the Court of Appeal noted at §101 “*the modest scale of the likely recovery cannot of itself be sufficient to justify dismissal of the claim*”, citing the observations of Lewison LJ in Sullivan v Bristol Film Studios [2012] EMLR 27, at §29. Furthermore, even small damages awards are likely to have real value to data subjects. For example, as the Competition Appeal Tribunal recognised in Consumers’ Association v Qualcomm Incorporated [2022] CAT 20 at §106, in the context of an analysis of the costs and benefits of collective proceedings, “*in the current economic climate, and given the cost of living challenges faced by many consumers*”, there may be real interest in damages awards of just £16-17 per consumer. [167] [1006]
15. However, and more fundamentally, it is important not to lose sight of the intrinsic importance of protecting the rights guaranteed by the GDPR in and of themselves. As the House of Lords has recognised in an analogous context in Campbell v MGN Ltd [2004] 2 A.C. 457 at §12, per Lord Nicholls, privacy “*lies at the heart of liberty in a modern state. A proper degree of privacy is essential for the well-being and development of an individual.*” [937]
16. Parliament has recognised the vital importance of data protection rights through:
 - a. Its decision to retain the GDPR, as the UK GDPR, following Brexit; and
 - b. More recently, section 183A of the DPA 2018, as inserted by section 106(2) of the Data (Use and Access) Act 2025. In summary, this provision protects the majority of the GDPR and DPA 2018 from being overridden by any enactments or rules of law passed or made on or after 20 August 2025.⁴ While this provision does not apply to Article 82 GDPR, ORG endorses the points made at §24 of the Information Commissioner’s intervention. [604-605] [105-107]
17. **Second**, the ability of data subjects to recover damages regardless of the seriousness of harm suffered is particularly important in the context of fast-moving technological

⁴ Note, also, the special status given to the GDPR and DPA 2018 by sections 106(3)-(5) of the Data (Use and Access) Act 2025. [651-652]

change. As recognised at Recital 6 of the GDPR, “*Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally.*” [660]

18. In this context, small scale individual harms resulting from infringements are increasingly common. They are also, by definition, more frequent than exceptional GDPR breaches that result in the most serious forms of harm.
19. Whilst GDPR infringements giving rise to modest individual losses may not involve the most serious data and privacy concerns when viewed in isolation, the position is very different when considered in the aggregate, where, as emphasised above, there is a risk of collective harm to thousands, sometimes millions, of data subjects. As Lord Leggatt noted in Lloyd v Google at §67, “*the development of digital technologies has added to the potential for mass harm for which legal redress may be sought*” [1213]. The passage of time, ongoing pace of technological change, and ever-growing commercial incentives to process personal data have only amplified the force of this observation; for example, following the recent exponential growth in the computational power of artificial intelligence.
20. If the GDPR is to have its intended effects of (i) ensuring a high degree of protection for data subjects, and (ii) effective protection through incentivising data controllers to strive for compliance, then there cannot be a low or no cost option for data breaches and other infringements. Those breaches include those alleged in these proceedings, which the Appellant has characterised as “*unintentional*” and “*one-off*”: Court of Appeal judgment at §26. For example, shutting out a whole class of claimants, or even a substantial proportion thereof, from recovering compensation reduces the incentives to invest in the kind of technical and organisational measures required to comply with Articles 24, 25 and 32 of the GDPR. As the Advocate General recognised in UI at §46: [148-149] [1884]

“The duty to compensate operates (ideally) as an incentive to act more carefully in the future, through observance of the rules and the avoidance of further damage. In that way, by claiming compensation for himself or herself, each individual contributes to the general effectiveness of the rules.”

21. **Third**, whilst this appeal is not directly about the use of group litigation procedures, they are important to the wider statutory context. In particular, Article 82 of the GDPR sits alongside the representative action procedure at Article 80 of the GDPR, within Chapter VIII (see also section 187 of the DPA 2018).⁵
22. It is therefore clear that (i) the EU legislature, when enacting the EU GDPR, (ii) Parliament, when implementing Article 80 of the EU GDPR at section 187 of the DPA 2018; and (iii) Parliament, when deciding that Articles 80 and 82 of the GDPR should remain part of domestic law, had in mind the possibility that individual claims – particularly those causing small scale individual harms to large numbers of data subjects – might be brought by way of group litigation.
23. As this Court has recognised in the context of collective proceedings in the Competition Appeal Tribunal, group litigation mechanisms may enable “*whole classes of consumers to vindicate their rights to compensation and the large cost of the necessary litigation to be funded... The prospect that the rights of consumers can be vindicated in that way also serves to act as a disincentive to unlawful anti-competitive behaviour of a type likely to harm consumers generally*”: *Mastercard Incorporated & Ors v Merricks* [2021] 2 All ER (Comm) 669, at §2 per Lord Briggs. [1243]
24. The same essential point applies here. However, the imposition of a seriousness threshold would shut out group claims that promote access to justice and deter wrongdoers and/or would make such claims much more difficult as defendants would be incentivised to contest seriousness, even if they admit liability for the breach in principle, leading to protracted litigation rather than a speedy resolution of appropriate relief. Either of these outcomes risk undermining the effective protection of data rights. In particular, and as recognised in *Merricks*, where infringements are unlikely to attract an effective private-law remedy, controllers face significantly weakened *ex ante* incentives to comply with their legal obligations.

⁵ For a recent example of the use of this mechanism, see *Good Law Project Limited v Reform UK Party Limited* [2026] EWHC 1458 (KB), where the High Court rejected a strike out and summary judgment application regarding the application of the conditions at section 187 DPA 2018. [1012-1030]

25. **Fourth**, these points take on particular significance when one considers the interaction between Article 82 and the ability of data subjects to complain to the Information Commissioner under Article 77 GDPR. Two points bear emphasis.
- a. Whilst data subjects have the right to complain, Article 77 is not “*a straight alternative to or proxy for a direct claim against the data controller who is alleged to have infringed the rights of the data subject*”: *R (Delo) v Information Commissioner* [2024] 1 W.L.R. 263, at §79, per Warby LJ. As the Court of Appeal made clear in *Delo* (in particular §§76-77 and 80), the Commissioner does not have [1348-1349] any duty to provide a conclusive view on whether data subjects’ rights have been infringed.⁶ Indeed, the Information Commissioner often responds to individual complainants by inviting the individual to consider the personal remedies available under the GDPR and/or DPA 2018 before the Courts. As a regulator, the Information Commissioner has discretion over the deployment of his resources, and, as such, may decide not to continue an investigation and instead prioritise other types of cases and/or policy issues.
 - b. In any event, even where the Commissioner does take action, it does not have the power to enforce data subjects’ right to compensation. The only route to compensation in the UK is by way of a claim through the court system.

C. THE FREE FLOW OF DATA BETWEEN THE EU AND UK

26. The Court of Appeal’s judgment has wider ramifications for the free flow of data between the UK and EU, as well as for the digital economy more widely. ORG raises these arguments both in relation to the seriousness threshold issue that the Court is asked to determine, but also the broader question of when the domestic courts might diverge from the post-Brexit caselaw of the CJEU pursuant to section 6 of the European Union (Withdrawal) Act 2018 (“**EUWA 2018**”). [639-643]

⁶ Moreover, organisations including ORG have expressed serious concerns about the Information Commissioner’s failure to act in response to complaints.

27. The starting point is the Court of Appeal’s judgment, which rightly recognised that the GDPR “*is an international legal instrument*” (§67) and that “[d]ata protection law has an international dimension” (§69). [159]
28. A key facet of this international dimension is the way in which personal data is transferred across borders. In this connection, one of the main aims of the GDPR is to facilitate “*the transfer [of personal data] to third countries and international organisations, while ensuring a high level of the protection of personal data*” (Recital 6).⁷ Moreover, Recital [660] 101 provides that “[f]lows of personal data to and from countries outside the Union and [677] international organisations are necessary for the expansion of international trade and international cooperation”.
29. These considerations apply with particular relevance to the UK following Brexit. The UK is now a “third country” for the purposes of Chapter V of the EU GDPR, which is headed “[t]ransfers of personal data to third countries or international organisations”. Article 44 summarises the “*general principle for transfers*”, and includes a requirement [718] that “*the level of protection of natural persons guaranteed by this Regulation is not undermined*” where a data transfer takes place.
30. The legal mechanism by which data flows from the EU to the UK is the (renewed) EU Commission’s adequacy decision for the UK of 19 December 2025.⁸ EU adequacy [749-778] decisions are adopted pursuant to Article 45 of the EU GDPR, Article 45(1) of which [719] provides that “[a] transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection” (emphasis added). Recital 104 further explains that “[t]he third country should offer guarantees ensuring [677-678] an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors”.

⁷ See also Recital 2 which emphasises that the GDPR more broadly contributes to “*economic [659] and social progress*”.

⁸ Decision C (2025) 8771. At the same time the main adequacy decision was renewed, the EU [749-778] also renewed its decision concerning transfers under the Law Enforcement Directive: see decision C (2025) 8782.

31. In judging the level of protection in a third country, the EU Commission must take into account, *inter alia*, “case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred”: Article 45(2)(a) of the EU GDPR (see also Recital 104). As the European Data Protection Board commented in its 2021 Opinion on the EU Commission’s draft adequacy decision for the UK, at §114, “effective administrative and judicial redress (including compensation for damages as a result of the unlawful processing of data subject’s personal data)” is one of the “key elements for the assessment of whether a data protection system provides an adequate level of protection”.⁹ [719, 677-678] [874]
32. The significant benefit of the UK holding adequacy status is that personal data may be transferred from the EU to the UK without the need for any of the more onerous safeguards listed at Article 46 of the EU GDPR. Adequacy has obvious practical benefits for the ability of data “exporters” in the EU and data “importers” in the UK, including for example, banks, hospitals, scientific researchers, retailers, lawyers, insurance companies, charities, and governmental organisations.
33. The economic significance of the UK’s adequacy status is well-recognised. For example:
 - a. The then Prime Minister announced on 3 March 2020 the UK’s intention to seek an adequacy decision under Article 45 GDPR.¹⁰ The framework documents submitted by the Government in pursuit of that objective further emphasised the importance of obtaining an adequacy decision, as follows:

“The UK has a world-class data protection regime. The UK Government is committed to ensuring the UK remains a global leader in data protection, working with the Commission and our other like-minded partners to promote strong data protection standards across the world. Protecting personal data is and will continue to be a priority for the UK. [2206]

The continued free flow of personal data is vital for the future relationship between the UK and the EU. Imports and exports of both goods and services heavily depend on the free flow of personal data between the UK and the EU. EU personal data-

⁹ Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom. See also §22. [874-895]

¹⁰ Policy paper, Explanatory framework for adequacy discussions, 13 March 2020. [2205-2245]

enabled services exports to the UK were worth approximately £42bn (€47bn) in 2018, and exports from the UK to the EU were worth £85bn (€96bn).”

- b. As the Government explained in June 2021 when the EU Commission’s adequacy decision was first adopted, the *“free flow of personal data supports trade, innovation and investment, assists with law enforcement agencies tackling crime, and supports the delivery of critical public services sharing personal data as well as facilitating health and scientific research.”*¹¹ [2189]
 - c. In the same vein, a November 2020 report by the New Economics Foundation and UCL European Institute conservatively estimated that the costs on UK companies of the failure to secure adequacy were at that time between £1 billion and £1.6 billion.¹² [2172]
34. The importance of obtaining an adequacy decision lay behind the careful and limited amendments made by Parliament to the UK GDPR following Brexit. Indeed, in seeking a positive decision on adequacy in spring 2020, the framework documents submitted by the UK Government emphasised that the UK GDPR follows the structure of the EU GDPR and retains the right to compensation.¹³ This was a relevant factor in the EU’s Decision in June 2021.¹⁴ Recital (108) made express reference to the fact that: *“... under Article 82 of the UK GDPR and Section 168 of the DPA 2018, any person who has suffered material or non-material damage as a result of an infringement of the UK GDPR has the right to receive compensation from the controller or processor for the damage suffered. The rules on the compensation and liability in Article 82(1) – (5) of the UK GDPR are identical with the corresponding rules in Regulation (EU) 2016/679. Under* [800]

¹¹ See a press release of 28 June 2021, titled “EU adopts ‘adequacy’ decisions allowing data to continue flowing freely to the UK”. [2188-2190]

¹² New Economics Foundation and UCL European Institute, “The Cost of Data Inadequacy: The Economic Impacts of the UK Failing to Secure an EU Data Adequacy Decision”, November 2020. As explained at p.28 *“[i]n reality, the overall costs to business in the event of no adequacy decision are likely to be much higher”* than this estimate. Note also p.33 onwards, concerning wider economic impacts (e.g. reduction in EU-UK trade or investment within the UK) that were not part of the estimate. [2172] [2177-2180]

¹³ Explanatory Framework for Adequacy Discussions Section C: The UK’s Legislative Framework. See also Explanatory Framework for Adequacy Discussions Section A: Cover Note, p.4; and Explanatory Framework for Adequacy Discussions Section G: The Role of the ICO and Redress, pp.26-28. [2211-2216] [2205-2210] [2217-2245]

¹⁴ Commission Implementing Regulation (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom. [779-846]

Section 168 of the DPA 2018, non-material damage includes also distress...” as one element in support of the Commission’s overall conclusion on adequacy (Recital (5)).

35. ORG does not suggest that, if the appeal is allowed, the EU is likely to revoke the UK’s adequacy status, which involves a holistic assessment of the UK’s data protection landscape. However, the imposition of a seriousness threshold could have a material bearing on that status. If this Court were to interpret Article 82 of the GDPR as imposing a seriousness threshold, this would directly undermine the effectiveness and enforceability of the rights of data subjects whose data is being transferred from the EU to the UK and result in a significant divergence with the position in the EU. It is therefore precisely the kind of jurisprudential development contemplated by Article 45(2)(a) of the EU GDPR. Indeed, §§120-126 of the EU’s renewed adequacy decision for the UK specifically envisages that the EU Commission will monitor relevant developments, including “*case law developments*” (§120). [719] [776-777]
36. More generally, ORG submits that, when domestic courts consider departing from CJEU caselaw handed down after IP Completion Day pursuant to their discretion at section 6 of EUWA 2018, they should take into account the possibility that a divergent approach that results in a materially lower level of protection for data subjects than found under the EU GDPR might risk undermining the EU’s assessment that the UK offers “*essentially equivalent*” levels of protection, and the wider social and economic benefits that flow from the UK’s adequacy status.

D. CONCLUSION

37. The Court is invited to dismiss the appeal and uphold the Court of Appeal’s interpretation of Article 82 of the GDPR.

JULIANNE KERR MORRISON & WILL PERRY

Monckton Chambers

26 August 2026

Referenced and updated on 9 September 2026