

IN THE SUPREME COURT OF THE UNITED KINGDOM
ON APPEAL FROM THE COURT OF APPEAL (CIVIL DIVISION)

[2025] EWCA Civ 1117 (King, Warby & Whipple LJJ)

BETWEEN:

MR MICHAEL FARLEY

and 431 others set out in Annex 1 to the Claim Form

Respondents

-and-

PAYMASTER 1836 LIMITED (t/a EQUINITI)

Appellant

-and-

THE INFORMATION COMMISSIONER

Intervener

WRITTEN CASE FOR THE INTERVENER
THE INFORMATION COMMISSIONER

References to the Court of Appeal judgment are in the form: Judgment, §x

References to the Data Protection Act 2018 are in the form: "DPA".

References to Regulation 2016/679/EU (the General Data Protection Regulation) are in the form: "GDPR".

References to the GDPR as amended and assimilated in domestic law, as defined in section 3(10) DPA, are in the form: "UK GDPR".

Introduction

1. The Commissioner sought and was granted permission to intervene by way of written submissions in this significant data protection appeal on the issue of whether or not a 'threshold of seriousness' applies to a claim for compensation for non-material damage, caused by a breach of data protection law, made under Article 82 of the GDPR.

2. The Commissioner's statutory role is explained below at §§47–48 of this Written Case.
3. The Commissioner was invited to intervene by the Court of Appeal, and participated by way of written and oral submissions at the hearing, including on the sole issue which remains the subject of the present appeal. Those submissions were considered by Warby LJ, in the Judgment, to be of assistance. They are summarised at §27 of the Judgment (see also, §50), and the analysis of Warby LJ on the threshold of seriousness issue is similar to that advanced by the Commissioner. [149, 155]
4. In summary, the Commissioner's position is that there is no threshold of seriousness applicable to a claim for compensation for non-material damage, or indeed material damage, under the GDPR. Any "*damage*" suffered is, in principle, recoverable. Not all emotional responses to an infringement of the GDPR will constitute recoverable non-material damage, but the need to show recoverable damage (even of a non-material kind) should not be confused with some additional hurdle of damage of a sufficiently serious kind. Low value claims can and should be addressed as they are elsewhere in the law: through case management and appropriate track allocation under the Civil Procedure Rules ("**CPR**").
5. The Commissioner's position is supported by the language and purpose of the GDPR, and also by a consistent line of case law from the Court of Justice of the European Union ("**CJEU**"), all of which post-dates IP Completion Day¹ and therefore does not bind any domestic UK court or tribunal. However, the Commissioner submits that the CJEU's case law should be followed because it is correct, and also because there are particular justifications for following CJEU judgments in the field of data protection law.

¹ 31 December 2020 at 23.00: see section 39 of the European Union (Withdrawal Agreement) Act 2020, adopted by reference by section 1A(6) EUWA. [632]

The Applicable Legal Regime

6. Since the alleged breaches in the present case occurred in 2019, the applicable legal regime is the GDPR and the DPA. The GDPR is an EU regulation which became directly effective in the Member States on 25 May 2018. The GDPR is supplemented by the DPA, which mostly came into force alongside it in May 2018.
7. The GDPR continued to form part of domestic law after exit day on 31 January 2020: see section 3(1) of the European Union (Withdrawal) Act 2018 (“EUWA”), as originally enacted. From 31 December 2020, a slightly amended version known as the UK GDPR has been in force: see the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, and the definition set out in section 3(10) DPA to cater for it. The 2019 Regulations [587] also made slight amendments to the DPA. Up until the end of 2023, the UK GDPR had the status of “*retained direct EU legislation*”, but it now has the status of “*assimilated direct legislation*” under section 3 of the EUWA. The present case [634] is concerned with the GDPR, but the Commissioner does not consider that the result would be any different if the UK GDPR applied.
8. The Claimants’ right to pursue a cause of action (based on facts occurring before IP Completion Day) under the GDPR was retained in UK law as ‘part and parcel’ of the retention of direct EU legislation under section 3 of the EUWA. This is because the EUWA is a ‘complete code’ for the application of EU law into domestic law, including for causes of action which arose before IP Completion Day: *Lipton v BA Cityflyer Ltd* [2024] UKSC 24, [2025] AC 154 at §83 [1137] *per* Lord Sales & Lady Rose.
9. Article 82(1) GDPR provides 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*”. The language of Article 82(1) of the UK GDPR is identical. Section 168(1) of the DPA [739] (as it applied at the relevant time) clarifies that, “*In Article 82 of the GDPR (right* [599]

to compensation for material or non-material damage), ‘non-material damage’ includes distress”.

10. Section 169(1) of the DPA (as it applied at the relevant time) provides for a similar right to claim compensation for contraventions of the DPA: “A person who suffers damage by reason of a contravention of a requirement of the data protection legislation, other than the GDPR, is entitled to compensation for that damage from the controller or the processor, subject to subsections (2) and (3)”. This provides the equivalent right where there has been a breach of, for example, a provision in Part 3 DPA, which regulates the processing of personal data for law enforcement purposes and implements Directive (EU) 2016/680. Part 3 was analysed by this Court in *R (Elgizouli) v Secretary of State for the Home Department* [2020] UKSC 10, [2021] AC 937, but there was no discussion of section 169. [601]
11. The Data (Use and Access) Act 2025 made a number of amendments to the UK GDPR and the DPA. However, Parliament did not legislate to amend any of the above provisions on compensation.
12. Recital (146) to the GDPR supplements Article 82 and provides that: “...The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered...”. Recitals remain a relevant aid to the interpretation of the GDPR (and the UK GDPR), in (at least) the following ways: [685]
- (1) Ordinary principles of interpretation require legislation to be read as a whole. Therefore, the language of recitals can inform the interpretation of retained/assimilated EU law: e.g. *Blanche v Easyjet Airline Company Ltd* [2019] EWCA Civ 69, [2019] Bus LR 1258. In *Oatly AB v Dairy UK Ltd* [2026]

UKSC 4, [2026] Bus LR 538, at §§30 and 32 *per* Lords Hamblen and Burrows, the language of a recital informed the meaning of the word “*designation*” in an EU regulation.

- (2) Recitals can be used to identify the context and purpose of retained/assimilated EU law, in accordance with the ordinary requirement to interpret legislation purposively: e.g. *CG Fry and Son Ltd v Secretary of State for Housing, Communities and Local Government* [2025] UKSC 35, [2025] PTSR 1823 at §§45–51 *per* Lord Sales.

[921–
922]

The Case Law of the CJEU

13. There are now a considerable number of judgments of the CJEU which interpret Article 82 GDPR and which expressly confirm that there is no threshold of seriousness applicable to it. These judgments were all handed down after IP Completion Day. Therefore, the judgments do not constitute retained/assimilated case law for the purposes of section 6 EUWA, and the particular rules for following and departing from retained/assimilated case law in section 6(3)–(5) EUWA do not apply. Instead, section 6(1)–(2) EUWA applies. By these provisions, a court or tribunal “*is not bound by any principles laid down, or any decisions made, or on after IP completion day by the European Court*”. But a court or tribunal “*may have regard to anything done on or after IP completion day by the European Court ... so far as it is relevant to any matter before the court or tribunal*”. [639]
14. The Commissioner has identified 13 judgments of the CJEU which interpret Article 82 GDPR and which are set out in an Annex to this Written Case. The judgments consistently confirm that non-material damage is not required to reach a threshold of seriousness.
15. The first and leading authority on the threshold of seriousness issue is C-300/21 *UI v Österreichische Post AG* [2023] 1 WLR 3702, in which the CJEU confirmed both that the requirement that damage be suffered in Article 82 meant that a claim for compensation could not succeed simply by virtue of showing a [1876]

contravention (at §§32–33, 36, 42), and that the concept of “*non-material damage*” could not be subject to a threshold of seriousness (at §§45–47, 49 and 51). Rather, where a data subject has suffered negative consequences as a result of a breach of the GDPR, they must show that those negative consequences constitute non-material damage: §50.

[1906–
1908]

16. In *UI v Österreichische Post*, the CJEU came to a different conclusion to the Advocate General, who had considered that there was a threshold of seriousness.² The CJEU’s reasoning considered the language of Article 82 (at §45), the importance of recital (146) (at §46), and the purpose of the GDPR (at §47). While the CJEU was also concerned to ensure a consistent application of the GDPR across the EU (at §§48–49), this was not only, or even the principal, reason for concluding that there was no threshold of seriousness.

[1908]

17. Since *UI v Österreichische Post*, the CJEU has consistently and repeatedly applied its view that there is no minimum threshold, as set out in the Annex to this Written Case.³

18. Although there is no requirement for non-material damage to reach a threshold of seriousness, the CJEU has emphasised that not every emotional reaction to a breach of the GDPR will amount to non-material damage. For example, a data subject’s fear about possible misuse of their personal data by a third party is capable of constituting non-material damage: see Case C-687/21 *BL v MediaMarktSaturn Hagen-Iserlohn GmbH* [2024] 1 WLR 2597 at §65. However, the fear must be well-founded: §67. A purely hypothetical risk of misuse cannot give rise to compensation: §68. The CJEU confirmed this approach in Case C-200/23 *Agentsia po vpisvaniyata v OL* (EU:C:2024:827) at §§142–143 and Case C-526/24 *Brillen Rottler GmbH & Co KG v TC* (EU:C:2026:216) at §63. The

[1769]

[1770]

[1737]

[1782]

² The Appellant’s Written Case asserts, at §88, that the Advocate General’s Opinion constitutes a distinct ‘line’ of case law to which section 6(1)–(2) EUWA applies, which is of equal weight to the judgments of the CJEU. Section 6(2) certainly maintains the position that an Advocate General’s Opinion may be taken into account, but it lacks principle and common-sense to assert that an Opinion is of equal relevance and weight to the decision of a CJEU Chamber of five judges which expressly reached the opposite conclusion.

[45]

³ These judgments have now emanated from the First, Third, Fourth and Fifth Chambers.

Appellant suggests that these cases introduce a threshold of seriousness ‘via the backdoor’ (see §104 of its Written Case), but this conflates the difference [51]
between a requirement to establish non-material damage, and a requirement that non-material damage must then meet a threshold of seriousness. The former is rooted in the legislative language; the latter is not.

19. Where a data subject has suffered non-material damage, but at a low level of seriousness, the CJEU has also confirmed that there is nothing wrong with awarding a small amount of compensation, provided that that compensation fully offsets the damage: Case C-182/22 *JU v Scalable Capital* (EU:C:2024:531) at [1822] §§45–46.

20. The CJEU has applied these principles in a closely analogous case to the present also involving the sending of a letter to an incorrect address. In Case C-590/22 *AT v PS GbR* (EU:C:2024:536), a tax consultancy erroneously posted the two [1744]
data subjects’ tax return to their previous home address. The tax return contained their names, their dates of birth, their identification numbers, their bank details, their membership of a religious community, the disability of a family member, their professions and workplaces, and various expenses. The new occupant of their previous address opened the letter, realised it was not intended for him, and returned it. The CJEU confirmed that there was no requirement for the non-material damage to reach a threshold of seriousness: §26. The data subjects’ fear of misuse by third parties was capable, in itself, of [1751]
constituting non-material damage: §32. However, the data subjects still had to prove that they had actually suffered non-material damage; a mere allegation of fear would not suffice: §§33–36. [1752]

Approach to CJEU Case Law

21. The Commissioner considers that the Court of Appeal was right to follow the CJEU’s consistent view that there is no requirement for non-material damage to reach a threshold of seriousness. The CJEU’s view is correct as a matter of statutory interpretation (see §§26–39 of this Written Case). There are also two

particular justifications for interpreting the GDPR consistently with the CJEU’s approach, which support the Court of Appeal’s view (Judgment, §67) that a “*sufficiently compelling*” case would be required to depart from the CJEU’s case law in the specific context of the GDPR.⁴

[159]

22. **First**, practical problems are liable to result if the domestic courts interpret the GDPR differently to the CJEU. There is a close analogy with the domestic context in which Court has recognised that practical considerations should be relevant when the courts in England and Wales decide whether to follow decisions of the courts in Scotland or Northern Ireland: see *R (Jwanczuk) v Secretary of State for Work and Pensions* [2025] UKSC 42, [2026] AC 699 at §61 *per* Lord Reed & Lady Simler. The more clear and consistent the CJEU’s line of authority, the greater the risk of practical problems in departing from the legal certainty the CJEU has provided users of the same language in the same legislation. The Court of Appeal correctly recognised the principle that “*Self-evidently, divergent interpretations of the same legislative text tend to undermine legal certainty*”: Judgment, §67.

[159]

23. The importance of legal certainty and consistency of interpretation is especially heightened in the context of an EU measure which is not sector-specific, but applies generally. As Article 2 GDPR sets out, the legislation applies to all automated processing of personal data, subject only to the narrow exceptions in Article 2(2), as well as applying in various extra-territorial contexts defined in Article 3. The concept of processing is defined very broadly in Article 4(2) (and see the Judgment, §§35-39). Because of the breadth of the GDPR’s application, very many controllers will transfer data between countries – whether within the same business, or to clients or suppliers – and very many data subjects will have their personal data processed by controllers/processors located around the world; the free movement of data within the EU itself is

[690]

[691]

[150–152]

⁴ The Commissioner makes no submission as to whether the same sort of standard should apply in other instances of retained/assimilated EU law; that was not the context which arose for consideration by the Court of Appeal. The Commissioner’s concern is with the particular importance of consistent interpretation of the GDPR and UK GDPR, subject to Parliament making relevant amendments to the domestic legislation.

subject to no specific additional controls (see Article 1(3) and recital (9)), and [690]
transfers of personal data out of the EU to a third country are permissible
subject to the safeguards prescribed in Chapter V GDPR. All of this means that [718]
there is a particularly strong contextual importance, for both controllers and
data subjects, to be governed by the same judicial understanding of provisions
drafted and retained in the same language; the GDPR is not a context in which
the practical importance of a consistent interpretation is hypothetical or limited
to a very specific sector.

24. **Secondly**, the GDPR, the EU-UK Withdrawal Agreement, and the EUWA each
indicate that there is particular value in maintaining a stable interpretation of
the GDPR consistent with the CJEU's approach:

(1) Divergence from the EU's approach to data protection has the potential to
adversely affect cross-border data transfers from the EU to the UK. Under
Article 45(1) GDPR, a transfer of personal data from an EU Member State to [719]
the UK may take place where the Commission has decided that the UK
"ensures an adequate level of protection". The EU Commission has issued an
adequacy decision for the UK.⁵ When assessing adequacy, the Commission
must take particular account of factors including *"case-law"*, *"effective and
enforceable data subject rights"*, and *"effective administrative and judicial redress
for the data subjects whose personal data are being transferred"*: see Article
45(2)(a) GDPR. An adequacy decision is a holistic assessment of the totality
of the UK's data protection framework and it would be a matter for the
Commission to consider what weight to give any particular factor. The
present issue would be a relevant factor. Article 45 GDPR therefore
demonstrates that, in the field of data protection law generally, there are
specific legal and policy implications of diverging from the EU's approach,
particularly where to do so reduces the level of protection for, and related
rights of, data subjects. Domestic courts should therefore be particularly
cautious about departing from the CJEU's interpretation of the GDPR.

⁵ Currently: Decision C (2025) 8771 of 19 December 2025. This renewed an adequacy decision first [749]
reached in June 2021.

- (2) If the UK loses its adequacy decision from the EU, there will remain restrictions on the UK's freedom in relation to data protection law. Under Article 71 of the EU-UK Withdrawal Agreement, if no adequacy decision is in place, then EU data protection law will apply in the UK in respect of the processing of personal data of data subjects who are outside of the UK, provided that the data (a) were processed under EU law before the end of the transition period on IP Completion Day, or (b) are currently processed in the UK on the basis of the Withdrawal Agreement itself. Article 71 is itself a part of domestic law by virtue of section 7A EUWA and forms part of the legal context in which section 6 EUWA is to be applied here. The relevance of Article 71 of the Withdrawal Agreement is to maintain a permanent legislative tie between data processing in the UK and the EU's data protection legislation (and its interpretation by the CJEU). This link reinforces that divergence from the GDPR, and its interpretation, is most appropriately a matter for Parliament to assess the array of possible implications for the UK's wider obligations. [748] [647]
- (3) Data protection law now has a distinct place in the EUWA, particularly following amendments made by the Data (Use and Access) Act 2025. For most assimilated direct legislation, the EUWA creates something like a reversal of the principle of supremacy in EU law. Assimilated direct legislation must, so far as possible, be read and given effect in a way which is compatible with purely domestic enactments: section 5(A2)(a) EUWA. If a compatible interpretation is not possible, then the relevant domestic enactment has supremacy over the assimilated direct legislation: section 5(A2)(b). However, a different approach applies to certain provisions of the GDPR and the DPA, as recognised in section 5(A3) EUWA: [637]
- Legislation enacted on or after 20 August 2025, which creates a duty or power to process personal data, is presumed not to override parts of the GDPR and the DPA, unless the legislation makes express provision to the contrary: see section 183A(1)–(2) DPA. [604]

- Legislation enacted before 20 August 2025, which creates a duty or power to process personal data, is subject to the supremacy of parts of the GDPR: see section 183B(1)–(3) DPA. [606]
- Legislation which prohibits or restricts the disclosure of information, or authorises the withholding of information, is presumed not to restrict certain rights of data subjects under the GDPR and the DPA: see section 186 DPA. [608]

The Commissioner emphasises that these special rules do not apply specifically to Article 82 of the UK GDPR and section 168 of the DPA (since these provisions are excluded from the definition of “*the main data protection legislation*” in section 183A(4) DPA). However, the existence of a distinct approach to data protection legislation in the EUWA again supports there being a special importance to maintaining a stable approach to the interpretation of the GDPR (and now the UK GDPR) and the DPA, unless Parliament expressly decides to amend the regime. [604]

25. These specific features of the data protection regime support the Court of Appeal’s view that “*sufficiently compelling*” reasons are required to depart from the CJEU’s interpretation of the GDPR (Judgment, §67). The Court had regard to the case law of the CJEU in accordance with section 6(2) of the EUWA, and was then entitled to recognise that, in the context of the GDPR, there was particular value in following the CJEU’s approach, meaning that compelling reasons would be required to depart from it. For the avoidance of doubt, the Commissioner makes no submission on the proper approach to departing from the CJEU’s case law in other instances of retained/assimilated law. [159]

A Threshold of Seriousness in Article 82 GDPR

26. The Commissioner considers that there are four main reasons why “*damage*” under Article 82 GDPR is not required to meet a threshold of seriousness.
27. **First**, and most importantly, there is nothing in the language of Article 82(1) GDPR which is consistent with some additional threshold of seriousness being [739]

imposed over and above the need for “*damage*” to have been caused by an infringement of the GDPR. The Appellant suggests (at §101(1) of its Written Case) that the absence of an express threshold does not assist either way, but this cannot be correct. The Appellant, on its own case, is seeking to read words into Article 82 (see §1 of the Appellant’s Written Case), and is thus seeking to modify the plain meaning of Article 82. The logical and normal meaning of the term “*material or non-material damage*” means any damage of this kind suffered; if it had been intended to exclude some sub-category of such damage from the right to compensation otherwise being afforded, it was incumbent on the legislation to say so. [50] [16]

28. Imposing a threshold of seriousness would also be inconsistent with the language of recital (146), which provides that “*The concept of damage should be broadly⁶ interpreted in light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation*”, and that “*Data subjects should receive full and effective compensation for the damage they have suffered*”. Imposing a threshold of seriousness would deny “*full and effective compensation*” to data subjects who have suffered genuine non-material damage, but at a less serious level. [685]

29. Of significance is that where the GDPR does seek to impose different levels of obligation depending on the context, including seriousness, it says so expressly. For example, Article 30(5) creates an exemption from record-keeping requirements for organisations with fewer than 250 employees, “*unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10*”. There are comparable thresholds in Article 34(1) (duty to notify data subjects of a breach only where it is likely to result in [709] [710]

⁶ The Appellant suggests the word “*broadly*” was only intended to clarify that compensation is also available for non-material damage (see §31 of the Appellant’s Written Case). Such an intention is not apparent from the text of recital (146). It naturally follows from a requirement to interpret the concept of damage “*broadly*” that the courts should not impose their own non-legislative threshold of seriousness.

a high risk to rights and freedoms), and Article 35(1) (duty to carry out a data protection impact assessment only where processing is likely to result in a high risk to rights and freedoms). The Appellant makes reference to certain other thresholds within the GDPR and the DPA intended to reflect gradations of seriousness in different ways (see §35 of the Appellant’s Written Case),⁷ to reflect that not every breach of the GDPR in relation to every item of personal data will be equivalently serious. But the legislation is keenly aware that its scope is very broad and deliberately so. The existence of these thresholds only reinforces the point that, where a threshold of seriousness was intended to apply in the GDPR, the legislation has made that clear, and defined the terms in which it is to apply with care. [711] [27]

30. **Secondly**, the purpose of Article 82 is to provide an effective remedy to data subjects whenever a breach of the GDPR has caused them damage of a defined kind. This is clear from the language of Article 82 itself – including the limited defence provided in Article 82(3) and the joint liability principle in Article 82(4) – and recital (146). The core purpose of the GDPR is a protective one towards the data subject: Article 1(1) provides that “*This Regulation lays 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.*” The protection provided by the GDPR for the personal data of natural persons is itself defined as a “*fundamental right*” by Article 1(2). The imposition of a non-legislative threshold to obtain compensation would undermine that core purpose of the GDPR generally, and the specific purpose of Article 82(1) (see the CJEU’s judgment in *UI v Österreichische Post* at §47). [739] [685] [690] [1908]

31. The language and purpose of Article 82 GDPR are the most significant factors for resolving the issue in the present case, as explained more fully below at §41.

⁷ One of the examples given concerns when the Commissioner will issue an enforcement notice under sections 149-150 DPA. Both in that context and more generally, the Commissioner unsurprisingly seeks to focus limited resources on cases of greater seriousness and/or higher levels of impact, as a rational exercise in regulatory prioritisation (upheld in *R (Delo) v Information Commissioner* [2023] EWCA Civ 1141, [2024] 1 WLR 263). Regulatory policy and practice is not relevant to the proper construction of Article 82(1) GDPR. [594–598] [1328]

32. **Thirdly**, as the CJEU’s case law recognises, the absence of a free-standing threshold of seriousness does not equate to an absence of legal controls over claims for compensation:

- (1) A data subject must prove causation.
- (2) A data subject cannot claim compensation simply by reason of an infringement. The Supreme Court rejected such a claim under the Data Protection Act 1998 in *Lloyd v Google LLC* [2021] UKSC 50, [2022] AC 1217, [1186] and the CJEU rejected such a claim under the GDPR in *UI v Österreichische Post* at §42. [1907]
- (3) Any claim asserting non-material damage must prove that a recoverable form of non-material damage has in fact been suffered; there is no assumption that this will have occurred. A case such as *Rolfe & Ors v Veale Wasbrough Vizards LLP* [2021] EWHC 2809 (QB) is a good example of a rejection of an asserted level of non-material damage; it was in substance a finding that no recoverable damage had been suffered on the facts and there was accordingly nothing to compensate. That sort of robust engagement with such claims is entirely proper.
- (4) Not every emotional reaction to a breach of the GDPR will amount to non-material damage. For example, although a data subject’s fear about possible misuse of their personal data by a third party is capable of constituting non-material damage, the fear must be well-founded and cannot be purely hypothetical: see *BL v MediaMarktSaturn* at §§65–68. [1769–1770]
- (5) This is the relevance of the language in recital (85) on which the Appellant relies, which refers to “*any other significant economic or social disadvantage to the natural person*” in connection with what may amount to “*physical, material or non-material damage*” caused by a breach. It comes at the end of a list of such qualifying damage which includes “*loss of control*” and “*financial loss*”. Such matters, even if objectively small, are considered in recital (85) to be “*significant*”. The language of ‘serious’ is not used. [674]

33. It would be contrary to principle and the purpose of the legislative scheme for the courts to supplement these existing legal controls with an additional, undefined, threshold which must be crossed for damage to be recoverable. As the CJEU recognised in *JU v Scalable Capital* at §§44–46, it is perfectly acceptable [1822] for the courts to award small sums of compensation where damage is not particularly serious. Small sums may be of real significance to individual data subjects. Small value claims can, of course, risk using disproportionate levels of court resources but there is a well-established procedural mechanism for the management of such cases through the track allocation system under CPR Parts 26–29, with significant costs controls imposed accordingly. Claims which are started in an inappropriate venue can and should be transferred to the appropriate track, rather than be struck out by reference to a supposed threshold of seriousness: e.g. *Johnson v Eastlight Community Homes* [2021] EWHC 3069 (QB); *Sullivan (AKA Soloman) v Bristol Film Studios Ltd* [2012] EMLR 27, CA.
34. These points of principle and procedure also address the Appellant’s reliance now placed on the general principle of proportionality, by reference to which the provisions of the GDPR are to be interpreted. The Commissioner takes no issue with the existence of the principle, or its application to the interpretation of the data protection regime, both of which are well-established in the domestic case law (save that after 2023 the general principle of proportionality forms no part of domestic law by reason of section 4 of the Retained EU Law (Revocation and Reform) Act 2023, such that it cannot be an ongoing answer to the present issue). The more material issue is why the bare assertion that it breaches the principle of proportionality not to have a threshold of seriousness is advanced. There is at least one example of an argument advanced on the basis of the principle of proportionality seeking to impose a *de minimis* threshold on the application of the GDPR being rejected as finding no basis in the legislative language: *Information Commissioner v Clearview AI Inc* [2025] UKUT 319 (AAC) at §362. [1037]

35. A person who has suffered an infringement of their rights is entitled to claim compensation for the damage caused by that infringement; if the damage is small, the value of the claim will be proportionately small. The legal costs involved may be disproportionate, but addressing disproportionate costs is a fundamental purpose of track allocation under the CPR and – in mass claims of the present kind – cost budgeting and other case management tools are available to the Court. It might be thought the essence of disproportionality for a valid claim to be prevented simply because it is of relatively low value because the damage is less serious than in other, more valuable, claims. The Appellant must, but does not, confront that the logic of its argument must be that a claim under Article 82(1) for pecuniary loss will also fall to be struck out if it cannot surmount a *de minimis* threshold. The Appellant declines to specify what any such threshold might be in this context, nor address how it would operate consistently with the award of nominal damages of £1 for injury to credit and to reputation in *Halliday v Creation Consumer Finance Ltd (CCF)* [2013] EWCA Civ 333, [2013] 3 CMLR 4.
36. In light of the other legal controls on claims for compensation under Article 82 GDPR, and the well-known mechanisms available for managing small value claims proportionately, the Commissioner considers that the Appellant's concerns about overburdening the courts (see §§66–67 of its Written Case) are [38] somewhat overstated.
37. **Fourthly**, *Lloyd v Google* is not a persuasive authority in favour of imposing a threshold of seriousness. The passages relied upon by the Appellant are either concerned with the seriousness of a breach (as opposed to the seriousness of the data subject's damage), or are in fact inconsistent with Appellant's position. It is accepted that Lord Leggatt referred on a number of occasions to some kind of "*non-trivial*" threshold. At §§88, 115, 128, 137, and 138, Lord Leggatt rejected [1219, 1227, 1231, 1233] the claimant's submission that data subjects can obtain compensation for non-trivial breaches without proving any actual damage. This, however, is different to the question in the present case, which is concerned with situations where a data subject has suffered damage, but that damage is said to be trivial.

38. At §153 of *Lloyd v Google*, Lord Leggatt indicated that, “If (contrary to the conclusion I have reached) those facts disclose “damage” within the meaning of section 13 at all, I think it impossible to characterise such damage as more than trivial”. It is not in dispute that this view is *obiter* and based on the claimant’s own concession (recorded at §153) that there was a threshold of seriousness under the Data Protection Act 1998. It is instructive to consider why the claimant made that concession. A core aspect of the claimant’s case in *Lloyd* was that he could claim compensation for a mere loss of control (in the sense of a bare infringement) under the Data Protection Act 1998, because loss of control damages are available under the tort of misuse of private information (“MPI”), and the tort shares a “common source” with data protection legislation in the form of Article 8 ECHR. Since MPI has a threshold of seriousness, the claimant conceded that the Data Protection Act 1998 would have a similar threshold. However, the Supreme Court rejected the ‘common source’ argument at §113, §124, and §128, emphasising the material differences between data protection legislation and MPI at §§130–135. Thus, *Lloyd v Google* ultimately undermines the Appellant’s case, which relies on a similar ‘common source’ argument to submit that the threshold of seriousness in MPI should be read across into the GDPR. [1237] [1226, 1229, 1231] [1231]

39. In summary, there is no threshold of seriousness applicable to claims for compensation under Article 82 GDPR. The CJEU’s analysis on this issue is correct, and the Appellant’s arguments to the contrary are not in fact supported by *Lloyd v Google*. It does not follow from the absence of a threshold of seriousness that there are no other legal controls on compensation under Article 82 GDPR. Where a claim is of small monetary value, it can be managed proportionately by the courts under the established track procedures in the CPR.

Thresholds of Seriousness in Other Causes of Action

40. It is recognised that various thresholds of seriousness apply to other causes of action which are sometimes brought alongside claims under the GDPR.

However, comparisons with other causes of action are of limited value in this context.

41. **First**, the primary focus should be on the language and purpose of Article 82 GDPR, rather than on comparisons with other causes of action such as MPI. In *Lloyd v Google*, the Court's first reason for rejecting the possibility of loss of control damages under the Data Protection Act 1998 was simply that this was not a permissible interpretation of the language of the legislation: see §§113–118. Similarly, in *Vidal-Hall v Google Inc* [2015] EWCA Civ 311, [2016] QB 1003 at §81, the Court of Appeal focused on the plain meaning of the word “*damage*” in the relevant Directive, and declined to read across aspects of Article 8 ECHR. [1226–1228] [1540]
42. **Secondly**, not all causes of action in the field of data protection, privacy, and reputational torts have a threshold of seriousness. In the tort of malicious falsehood, there is no requirement to prove “*serious harm*” (in contrast to defamation), and a claimant can sometimes obtain nominal damages where they are unable to prove any actual pecuniary loss: see *George v Cannell* [2024] UKSC 19, [2025] AC 871. If a claimant can bring a successful claim in malicious falsehood without proving any loss at all, then the claimant cannot need to prove that they have suffered loss that meets a threshold of seriousness.
43. **Thirdly**, where a cause of action does involve a threshold of seriousness, it does not necessarily operate in the same way as the threshold proposed by the Appellant. To bring a successful claim for MPI, a claimant must have a reasonable expectation of privacy. To establish this, the information itself must meet a threshold of seriousness: see *Ambrosiadou v Coward* [2011] EWCA Civ 409, [2011] EMLR 21 at §§27–30 and *Primsall v Google UK Ltd* [2024] EWCA Civ 1516, [2025] KB 663 at §§39–42. If this concept were read into the GDPR, it would affect the definition of personal data in Article 4(1) GDPR rather than the ability to claim compensation under Article 82(1). There is also authority that, in a claim for MPI, the misuse by the defendant must meet a threshold of seriousness: see *Palmer v Farmer* [2023] EWHC 976 (KB), [2024] EMLR 1 at §56 and §§59–61. If this concept were read into the GDPR, it would mean that a [1317]

breach of the GDPR must meet a threshold of seriousness, but not necessarily that the level of damage must meet a minimum threshold.

44. In the law of defamation, it took legislative reform to develop a threshold of seriousness which is comparable to that proposed by the Appellant. At common law, a statement is only defamatory if it has a “*tendency or likelihood*” to cause adverse consequences for the claimant which reach a threshold of seriousness: see *Thornton v Telegraph Media Group Ltd* [2010] EWHC 1414 (QB), [2011] 1 WLR 1985 at §52. Thus, the focus at common law is on the tendency or likelihood to cause harm of a certain threshold, rather than the actual level of harm suffered by the claimant. Parliament then enacted section 1 of the Defamation Act 2013, which provides that “*A statement is not defamatory unless its publication has caused or is likely to cause serious harm to the reputation of the claimant*”. Section 1 “*not only raises the threshold of seriousness above that envisaged in Jameel and Thornton, but requires its application to be determined by actual facts about its impact and not just to the meaning of the words*”: see *Lauchaux v Independent Print Ltd* [2019] UKSC 27, [2020] AC 612 at §12 *per* Lord Sumption. [1076]
- The threshold of seriousness proposed by the Appellant in the present case focuses on the actual facts about the impact of a breach of the GDPR on the claimant. Such an exercise was only achieved in the law of defamation through legislative reform.
45. **Fourthly**, there are principled reasons for applying a threshold of seriousness to other causes of action, which do not carry over to the data protection context. For example, MPI usually involves a balancing exercise between competing rights (invariably privacy under Article 8 ECHR against freedom of expression under Article 10 ECHR). In that context, it is understandable why privacy rights need to meet a threshold of seriousness before they can permissibly interfere with the freedom of expression. In defamation law, Tugendhat J identified two reasons for why there is a threshold of seriousness. The first was that this was the best interpretation of previous authorities on the meaning of “*defamatory*”. The second was that this was required by Article 10 ECHR and the principle of proportionality: see *Thornton v Telegraph Media Group Ltd* at §90.

Neither of these justifications applies with the same force to the GDPR. Rights under the GDPR will occasionally need to be balanced against other fundamental rights, and recital (4) of the GDPR does make reference to the principle of proportionality, but it does not follow that there should be a blanket threshold of seriousness that applies to all compensation claims under Article 82 GDPR, including those that do not involve any countervailing fundamental rights.

46. In summary, comparisons with other causes of action do not justify a departure from the language and purpose of Article 82 GDPR and the consistent case law of the CJEU, which both indicate that there is no threshold of seriousness.

The Role of the Information Commissioner

47. The Commissioner is appointed by His Majesty by Letters Patent under the DPA (as was the case under the predecessor legislation). The Commissioner's office is maintained by section 114 DPA, with various detailed provisions in Schedule 12. By section 115, the Commissioner was the supervisory authority in the United Kingdom for the purposes of the GDPR, as it applied at the relevant time. Following withdrawal from the European Union, and the assimilation of the GDPR into domestic law as the UK GDPR (see section 3(10) DPA), this supervisory authority function ceased. The Commissioner remains the national regulatory authority for data protection law, and has similar functions under various other information-related pieces of domestic and European-derived legislation.
48. The Commissioner has a wide range of functions under the UK GDPR and the DPA to monitor and enforce the provisions of the legislation, which are not materially altered from the formulation of those functions under the terms of the GDPR. These functions are set out in particular in Parts 5–6 DPA, and Chapter VI UK GDPR. Where the Commissioner takes enforcement action, the affected controller has a right of appeal to the First-tier Tribunal: sections 162–163 DPA. The Commissioner's enforcement functions do not extend to

requiring any award of compensation or other monetary payment be made by a controller to a data subject. A data subject is not required to seek the involvement of the Commissioner and may bring a claim for breach of their rights under the UK GDPR in the ordinary courts: see Article 79 UK GPDR / GDPR and section 167 DPA.

Conclusion

49. The Court is respectfully invited to dismiss the appeal for the following amongst other reasons:

- (1) The CJEU has consistently held that non-material damage under Article 82 GDPR is not required to reach a threshold of seriousness to justify the award of compensation. The CJEU's interpretation should be followed because it is correct, and in any event because there is particular value in following the CJEU's judgments in the field of data protection.
- (2) Both the language and purpose of Article 82 indicate that there is no threshold of seriousness. Instead, there are other legal controls over claims for compensation, as the CJEU's case law also recognises.
- (3) Comparisons with the various thresholds of seriousness that can apply to other causes of action are of limited assistance in this particular legislative context, and do not justify a departure from the plain meaning of Article 82.

CHRISTOPHER KNIGHT KC
OLIVER FRIEND-SMITH

11KBW

26 August 2026

**Annex to the Information Commissioner’s Written Case:
CJEU authorities on the interpretation of Article 82 GDPR**

Case	Date	Facts	Interpretation of Article 82 GDPR	Advocate General’s Opinion
Case C-300/21 <i>UI v Österreichische Post AG</i> [2023] 1 WLR 3702	4/5/23	An Austrian company applied an algorithm to infer the data subject’s affinity to an Austrian political party.	If a person suffers negative consequences as a result of a breach of the GDPR, they must demonstrate that those consequences constitute non-material damage. However, non-material damage is not required to reach a certain degree of seriousness: §§43–51.	In contrast to the CJEU, AG Campos Sánchez-Bordona had considered that non-material damage must meet a certain threshold of seriousness, beyond mere upset: §§95–117.
Case C-340/21 <i>VB v Natsionalna agentsia za prihodite</i> [2024] 1 WLR 2559	14/12/23	After a cyber attack on the Bulgarian National Revenue Agency, the data subject’s personal data was published on the internet. She feared her personal data might be misused.	Non-material damage is not required to reach a certain degree of seriousness: §78. The data subject’s fear of possible misuse of their personal data is capable of constituting non-material damage, but the fear must be well-founded in the specific circumstances: §§79–86.	AG Pitruzzella (in an Opinion pre-dating the CJEU’s judgment in <i>UI v Österreichische Post</i>) considered that non-material damage must meet a certain threshold of seriousness, beyond mere upset: §§78–83.
Case C-456/22 <i>VX v Gemeinde Ummendorf</i> (EU:C:2023:988)	14/12/23	A German municipality published the data subjects’ names and home addresses on its website.	Non-material damage is not required to reach a certain degree of seriousness: §§15–23. However, the data subjects must prove that they have actually suffered such damage, however minimal: §22.	There was no AG Opinion.
Case C-667/21 <i>ZQ v Medizinischer Dienst der Krankenversicherung Nordrhein</i> (EU:C:2023:1022)	21/12/23	The data subject’s employer prepared an expert report on his capacity to work. The data subjects was concerned about the potential for his colleagues to have access to the report, and the security measures for archiving the report.	Article 82 GDPR has a compensatory rather than a dissuasive or punitive function. Therefore, the seriousness of a breach of the GDPR does not affect the quantum of compensation: §§85–87.	AG Campos Sánchez-Bordona considered that the seriousness of a breach of the GDPR does not affect the quantum of compensation: §§113–118.

Case	Date	Facts	Interpretation of Article 82 GDPR	Advocate General's Opinion
Case C-687/21 <i>BL v MediaMarktSaturn Hagen-Iserlohn GmbH</i> [2024] 1 WLR 2597	25/1/24	The data subject purchased an electrical appliance from a shop. An employee mistakenly gave a document (which included the data subject's name, address, income, and bank details) to another customer. The document was returned within half an hour, and there was no evidence that the other customer had read the document.	Non-material damage is not required to reach a certain degree of seriousness: §59. However, a data subject must still show that negative consequences resulting from a breach actually constitute non-material damage: §60. A data subject's fear of possible misuse of their personal data is capable of constituting non-material damage: §65. However, this fear must be well-founded (§67) rather than purely hypothetical (§68). If a third party did not become aware of the personal data, there can be no non-material damage arising from a purely hypothetical fear that the third party misused the data: §69.	There was no AG Opinion.
Case C-741/21 <i>GP v juris GmbH</i> (EU:C:2024:288)	11/4/24	A company sent two advertising leaflets to the data subject, despite his having revoked consent to the processing of his personal data for the purpose of marketing.	Non-material damage is not required to reach a certain degree of seriousness, but the data subject must nevertheless demonstrate that a breach caused such non-material damage: §36. The data subject's loss of control over his personal data is capable of leading to compensation, provided that he can show that he actually suffered non-material damage, however slight: §§41–42.	There was no AG Opinion.
Case C-182/22 <i>JU v Scalable Capital GmbH</i> (EU:C:2023:820)	20/6/24	Unknown third parties gained access to the data subjects' personal data on a trading platform. However, there was no evidence of any actual misuse or identity theft.	Non-material damage is not required to reach a de minimis threshold: §44. However, where the damage is not serious, national courts can award a small amount of compensation, provided that this compensates in full for the damage suffered: §§45–46. The mere accessing of the personal data by third parties could still give rise to compensation where the data subject has suffered non-material damage as a result: §§53–58.	AG Collins considered that non-material damage need not attain a certain degree of seriousness, or a de minimis threshold. However, there must be clear and precise evidence that the data subject suffered non-material damage. Potential or hypothetical damage, or mere disquiet relating to the theft of one's personal data, is insufficient: §24. The mere accessing of personal data by third parties could still give rise to non-material damage: §§26–31.

Case	Date	Facts	Interpretation of Article 82 GDPR	Advocate General's Opinion
Case C-590/22 <i>AT v PS GbR</i> (EU:C:2024:536)	20/6/24	A tax consultancy erroneously posted the data subjects' tax return to their previous home address. The new occupant opened the letter, realised that its contents were not addressed to him, and returned it.	Non-material damage is not required to reach a certain degree of seriousness: §26. The data subjects' fear as to possible misuse of their personal data by third parties is capable, in itself, of constituting non-material damage: §32. However, the fear constituting non-material damage must still be proven. A mere allegation of fear cannot give rise to compensation: §§33–36.	There was no AG Opinion.
Case C-200/23 <i>Agentsia po vpišovaniyata v OL</i> (EU:C:2024:827)	4/10/24	The Registration Agency of Bulgaria refused to erase the data subject's personal data, which was available on a public register.	Non-material damage is not required to reach a certain degree of seriousness, or a de minimis threshold: §§147 and 149. If a breach of the GDPR causes negative consequences, the data subject is required to demonstrate that those consequences constitute non-material damage: §142. A fear that personal data will be misused in the future must be well-founded in the specific circumstances: §143. A loss of control over personal data is capable of causing non-material damage, but the data subject must prove that they have actually suffered such damage: §150.	AG Medina's Opinion was concerned with other questions.
Case C-21/23 <i>ND v DR</i> (EU:C:2024:846)	4/10/24	One pharmacist claimed that another pharmacist was failing to obtain customers' consent for the processing of their personal data.	Chapter 8 GDPR (including Article 82) does not preclude national legislation which enables a person to claim that a competitor's breach of the GDPR constitutes an unfair commercial practice: §73.	AG Szpunar considered that the GDPR does not preclude national legislation which enables a person to claim that a competitor's breach of the GDPR constitutes an unfair commercial practice: §§106–107.
Case C-507/23 <i>A v Patērētāju tiesību aizsardzības centrs</i> (EU:C:2024:854)	4/10/24	At Latvian consumer protection centre distributed an online video which featured a character imitating the data subject, who was a Latvian automotive journalist.	Article 82(1) GDPR does not prohibit the making of an apology from being standalone or supplementary compensation for non-material damage, provided that the apology complies with equivalence and effectiveness, and that it compensates in full the non-material damage that has actually been suffered: §§36–37.	There was no AG Opinion.

Case	Date	Facts	Interpretation of Article 82 GDPR	Advocate General's Opinion
Case C-655/23 <i>IP v Quirin Privatbank AG</i> [2026] 1 CMLR 22	4/9/25	The data subject applied for a job with the controller. An employee of the controller mistakenly sent a message (which was intended for the data subject) to someone else, who knew the data subject and worked in the same sector. The message stated that his salary expectations could not be met, and offered him a lower salary.	Non-material damage is not required to reach a certain degree of seriousness, or a de minimis threshold: §58. A loss of control over personal data may be sufficient to cause non-material damage, provided that the data subject proves that they have actually suffered such damage, however minimal: §60. Fear that personal data will be misused in the future is capable, in itself, of constituting non-material damage, provided that that fear, with its negative consequences, is duly proven: §61. Feelings such as annoyance, displeasure, dissatisfaction, worry, and fear are also capable of constituting non-material damage: §57 and §62.	AG Campos Sánchez-Bordona's Opinion was concerned with other questions.
Case C-526/24 <i>Brillen Rottler GmbH & Co KG v TC</i> (EU:C:2026:216)	19/3/26	The data subject subscribed to a company's newsletter. Thirteen days later, he made a DSAR. The company considered that the DSAR was abusive: the data subject had systematically made DSARs to other controllers and then sought compensation.	Non-material damage is not required to reach a certain degree of seriousness, or a de minimis threshold: §62. A mere allegation of fear/uncertainty caused by a loss of control over personal data cannot give rise to compensation; the fear/uncertainty must be well founded in the specific circumstances: §§63–64. A data subject cannot be compensated for non-material damage where the damage was caused by the data subject's own decision to submit the data to the controller in order to create artificially the conditions for compensation: §66.	AG Szpunar was not asked to address this question, but commented that a loss of control over personal data may constitute non-material damage, provided that the data subject can show that they have actually suffered such damage. There is no de minimis threshold: §89. AG Szpunar also noted that, where damage is established but it is not serious, a national court can compensate for it by awarding minimal compensation, provided that this compensates the damage in full: §90.