Mishcon de Reya
Africa House
70 Kingsway
London WC2B 6AH
DX 37954 Kingsway
T: +44 20 3321 7000
www.mishcon.com

London | Cambridge | Oxford | Hong Kong | Singapore

Our Ref:

Your Ref:

The Information Commissioner
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

BY EMAIL

Dear Information Commissioner,

PROPOSED CLAIM FOR JUDICIAL REVIEW: JAMES KILLOCK V INFORMATION COMMISSIONER

Introduction

1. We act for James Killock. This letter concerns a proposed judicial review claim against the Information Commissioner (**"the Commissioner"** or **"ICO"**). The target of the claim is the Commissioner's "Data protection framework" (**"the Framework"**), which was published on or around 9 February 2026.

2. This letter has been prepared under the Pre-Action Protocol for Judicial Review. The following section adopts the form set out in its Annex.

The Defendant

3. The Information Commissioner, Information Commissioner's Office, Wycliff House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

The Claimant

4. We act for Jim Killock. Mr Killock has been the Executive Director of the Open Rights Group ("**ORG**"), one of the UK's largest grassroots digital rights and privacy campaign organisations, since 2009. Mr Killock has serious concerns regarding the Framework. It will have serious adverse effects on both ORG – as a campaign group seeking to hold organisations to account for breaches of

their data protection obligations by way of complaints to the ICO – and on the general public, whose rights ORG seeks to safeguard.

5. Mr Killock has considerable personal experience of the issues raised by the proposed claim. In particular, he was one of the applicants in *Killock, Veale & Ors v Information Commissioner* [2022] 1 WLR 2241, which this letter addresses below.

6. The ORG has engaged consistently with the ICO in relation to its complaints handling procedures, including by proposing recommendations for improvement. For example, in November 2024, ORG published its "ICO Alternative Annual Report", which provided a perspective on the ICO's 2023-24 Annual report and data on the enforcement action it had taken. More recently, ORG responded to the ICO's consultation on data protection enforcement procedural guidance.

7. More generally, ORG has a track record of upholding data protection rights by way of legal proceedings. For example, it was previously a claimant in two sets of judicial review proceedings which successfully challenged the lawfulness of the "immigration exemption" at paragraph 4 of Schedule 2 of the Data Protection Act 2018.

8. Please direct all correspondence related to this claim to this firm.

The Defendant's reference details

9. N/A.

The details of the Claimants' legal advisers dealing with this claim

10. Legal Representatives: Jam[redacted]

11. Address of Legal Representatives: Africa House, 70 Kingsway, London, WC2B 6AH.

12. Phone Number of Legal Representatives: +44 20 3321 7000.

13. Reference: JLL/AA/74628.3

The details of the matter being challenged

14. The Framework.

The details of any Interested Parties

15. N/A.

The issues

Legal framework

The UK GDPR

16. The General Data Protection Regulation 2016/679 (**"EU GDPR"**) was made in May 2016 and came into force with effect across the EU from 25 May 2018. Since 31 December 2020, a modified version of the EU GDPR, known as the **"UK GDPR"** has been in effect. The legislative measures used to achieve these modifications are identified and summarised in *R (Open Rights Group) v Secretary of State for the Home Department* [2021] 1 WLR 3611 §§5 and 12-13.

17. The Recitals to the UK GDPR remain part of domestic law, and should be considered when interpreting its provisions: *Farley v Paymaster* [2026] E.M.L.R. 1 (***"Farley"***), §53. Those recitals include the following (emphasis added):

> "(6) 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. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.
>
> (7) Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement… … Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced. …
>
> (10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. …
>
> (11) Effective protection of personal data throughout the Union requires the 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.
>
> (129) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in

> each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons … The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. …
>
> (141) Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. …"

18. Chapter VI of the UK GDPR is headed "The Commissioner". Article 51(1) provides that *"The Commissioner is responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data"*.

19. The Commissioner's tasks are set out at Article 57(1). They include obligations to:

> "(a) monitor and enforce the application of this Regulation;
>
> …
>
> (f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period…"

20. The Commissioner's investigative powers are then set out at Article 58(1), whilst its corrective powers are set out at Article 58(2).

21. Data subjects' rights to lodge complaints with the Commissioner are provided for at Article 77, which provides in full:

> "(1) Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with the Commissioner if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

> (2) The Commissioner shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78."

22. Article 78 provides data subjects with a right to a judicial remedy against the Commissioner where, pursuant to Article 78(2), *"the Commissioner does not handle a complaint or does not inform the data subject within three* months on *the progress or outcome of the complaint lodged pursuant to Article 77"*.

CJEU caselaw

23. Although not binding, in interpreting the UK GDPR, the domestic courts will generally follow the post-Brexit jurisprudence of the CJEU. As the Court of Appeal explained in *Farley* at §67 (emphasis added):

> "That brings me to the question of whether we should choose to plot a different course from the one taken by the CJEU. That is open to the UK as a political choice and a legislative option. But a judicial decision to do so would call for sufficiently compelling legal reasons. In that context I think it right to attach some weight to the fact that the GDPR is an international legal instrument which had direct effect in this jurisdiction at the material time. Further, its domestic successor, the UK GDPR, is post-Brexit legislation in which Parliament decided to adopt the identical language, so far as material to this case. Self-evidently, divergent interpretations of the same legislative text tend to undermine legal certainty. It seems to me that, other things being equal, it makes good legal sense for the court to interpret and apply the GDPR in conformity with settled CJEU jurisprudence."

24. Mr Killock relies on two CJEU judgments in particular.

25. **First**, the complaints mechanism at Article 77 of the EU GDPR was considered by the CJEU in Case C-26/22 *UF v Land Hessen* [2024] 3 C.M.L.R. 4 (***"SCHUFA"***). At §§56-58 of its judgment, the CJEU explained that:

    (a) §56: The supervisory authority must deal with complaints *"with all due diligence"*; citing the earlier case of *Facebook Ireland and Schrems*, C-311/18, at §109.

    (b) §57: the powers at Article 58 are designed *"[i]n order to handle complaints lodged"*; and

    (c) §58: *"It follows, as the Advocate General observed in point 42 of his Opinion, that the complaints procedure, which is not similar to that of a petition, is designed as a mechanism capable of effectively safeguarding the rights and interests of data subjects."*

26. The Opinion of the Advocate General (**"AG"**) endorsed by the Court recognised several important points. At §38 the AG highlighted that (original emphasis in italics):

> "38. The Court has ruled that under that provision 'each supervisory authority *is required* on its territory *to handle complaints* which, in accordance with Article 77(1) of the GDPR, any data subject is entitled to lodge … It should be pointed out in this connection that the Court has

> underlined the supervisory authority's obligation to 'handle such a complaint *with all due diligence*' in order to ensure compliance with the provisions of the GDPR. It should also be noted that recital 141 of the GDPR states that 'the investigation following a complaint should be *carried out* … *to the extent that is appropriate in the specific case*' (my emphasis).

27. As the AG commented at §§39-40 (original emphasis in italics; added emphasis underlined):

> "39. All these factors suggest that the supervisory authority has a *binding obligation to handle complaints* lodged by data subjects with all due diligence that is appropriate in the specific case. In so far as any infringement of the GDPR is, in principle, capable of constituting an infringement of fundamental rights, it would seem to be incompatible with the system established by that regulation to allow the supervisory authority discretion as to whether or not to handle complaints. Such an approach would undermine the crucial role conferred on it by the GDPR, which is to ensure compliance with the rules on the protection of personal data, and would therefore run counter to the objectives pursued by the EU legislature. Ultimately, it should be borne in mind that complaints are an important source of information for the supervisory authority, enabling it to identify infringements.
>
> 40. This interpretation is all the more convincing because Article 57(1)(f) of the GDPR imposes on the supervisory authority a number of requirements in connection with the handling of such a complaint … Additionally, there is the obligation under Article 77(2) of the GDPR to inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78 of the GDPR. All these requirements, coming under the concept of 'good administration' which found expression in Article 41 of the Charter specifically with regard to the activities of the institutions and bodies of the European Union, are intended to strengthen the complaints procedure in order to make it a *genuine administrative remedy*.

28. The AG proceeded at §41 to recognise that supervisory authorities were entitled to *"a margin of assessment in examining those complaints and a degree of latitude in the choice of the appropriate means to carry out its tasks"*. However, at §42 the limits of this margin were emphasised:

> "42. The detailed description of the supervisory authorities' power to adopt corrective measures shows that the EU legislature did not intend to make the complaint procedure similar to a petition procedure. On the contrary, the legislative objective seems to have been to establish a mechanism capable of *effectively safeguarding the rights and interests of individuals who lodge complaints*. It nevertheless seems clear that this latitude cannot be interpreted to mean that the supervisory authority has unlimited power, authorising it to act arbitrarily. On the contrary, the supervisory authority is obliged to exercise that latitude having regard to the limits imposed on it by EU law. For this reason too, it cannot be ruled out that the supervisory authority, as an administrative organ, will be forced to adopt a certain measure on account of the particular circumstances of the case, especially where there is a serious risk of an infringement of the fundamental rights of the data subject."

29. **Second**, Mr Killock relies on Case C-768/21 *TR v Land Hessen* (**"*Land Hessen*"**). Having repeated and endorsed the CJEU's reasoning in *SCHUFA* at §§32-35, the CJEU considered the subsequent question of whether and how a national data protection authority should remedy any breach of the EU GDPR it has found. The CJEU approached this question in light of the following points:

> "37. … it should be noted that the GDPR leaves the supervisory authority a discretion as to the manner in which it must remedy the shortcoming found, since Article 58(2) thereof confers on that authority the power to adopt various corrective measures. Thus, the Court has already held that the supervisory authority must determine which action is appropriate and necessary, and must do so taking into consideration all the circumstances of the specific case and executing its responsibility for ensuring that the GDPR is fully enforced with all due diligence (see, to that effect, judgment of 16 July 2020, Facebook Ireland and Schrems, C-311/18, EU:C:2020:559, paragraph 112).
>
> 38. That discretion is, however, limited by the need to ensure a consistent and high level of protection of personal data through strong enforcement of the rules, as is apparent from recitals 7 and 10 of the GDPR.
>
> …
>
> 40. … the system of sanctions provided for by the EU legislature allows supervisory authorities to impose the most appropriate and justified penalties depending on the circumstances of each individual case … taking into consideration, as recalled in paragraphs 37 and 38 of the present judgment, the need to ensure that the GDPR is fully enforced and to ensure a consistent and high level of protection of personal data through strong enforcement of the rules."

30. The CJEU proceeded to conclude that, although the supervisory authority is not *"under an obligation to exercise, in all cases where it finds a breach of personal data, a corrective power, in particular the power to impose an administrative fine"* (§41), it is required to do so where *"taking into account all the circumstances of the specific case, [it is] appropriate, necessary and proportionate to remedy the shortcoming found and ensure that that regulation is fully enforced"* (§42; emphasis added).

31. The Court considered that this meant that:

> "43. … it cannot be ruled out that, exceptionally and in the light of the particular circumstances of the specific case, the supervisory authority may refrain from exercising a corrective power even though a breach of personal data has been established. That could be the case, inter alia, where the breach established has not continued, for example where the controller, which had, in principle, implemented appropriate technical and organisational measures within the meaning of Article 24 of the GDPR, has, as soon as it became aware of that breach, taken appropriate and necessary measures to ensure that that breach is brought to an end and does not recur, in view of its obligations under, inter alia, Article 5(2) and Article 24 of that regulation."

32. This approach was said to be justified by the wording of the EU GDPR and its objectives (§§44-45). The CJEU then re-emphasised further elaborated on its overall conclusions at §46:

> "It follows that the exercise of a corrective power may, exceptionally and in the light of the particular circumstances of the specific case, not be required, provided that the situation in which the GDPR was infringed has already been made good and that the processing of personal data by the controller thereof in compliance with that regulation is ensured, and that such non-exercise on the part of the supervisory authority is not liable to undermine the requirement of strong enforcement of the rules, as recalled in paragraph 38 of the present judgment."

Domestic caselaw

33. Whilst the present claim is concerned with the Commissioner's approach to Article 77 UK GDPR complaints, a number of domestic cases have considered the related question of the scope of the Article 78 right to a judicial remedy. These include a number of cases in the Upper Tribunal (**"UT"**) concerning the meaning of section 166 DPA 2018, as well as the Court of Appeal's judgment in *R (Delo) v Information Commissioner* [2024] 1 W.L.R. 263; a judicial review against a decision of the Commissioner not to take any further action in response to a complaint.

34. In *Delo*, the Court of Appeal first considered the wording of Articles 57, 77 and 78, and concluded they indicated that the Commissioner was not required to reach and pronounce a decision on the merits of every complaint lodged by data subjects: §§59-62.

35. The language used in the relevant provisions instead required an "outcome": §§63-64. This is a broader concept, and the Court of Appeal considered that the Upper Tribunal in *Killock & Veale* was right to conclude it *"embraced a decision to cease handling a specific complaint whilst using it to inform and assist a wider industry investigation"*. Notably, at §64, the Court of Appeal agreed with the conclusions of Mostyn J below ([2023] 1 W.L.R. 1327) that:

> "… the word 'outcome' is an apt description of the Commissioner's decision to conclude his consideration of Mr Delo's complaint by informing him of the Commissioner's view that the conduct complained of was 'likely' to be compliant with the UK GDPR (or, put another way, that the complaint of infringement was 'likely' to be ill-founded).

36. The Court of Appeal turned to the wider statutory context and certain CJEU authorities relied on by Mr Delo (including Case C-311/18 *Facebook Ireland and Schrems*). It concluded that the former lent some support to its linguistic interpretation, whilst the latter did not assist Mr Delo: §§65-75.[1]

37. *"Standing back"*, the Court of Appeal concluded that the functions of the Commissioner were *"not those of a regulator with exclusive competence over*

[1] The Court of Appeal does not appear to have been aware of the AG's Opinion in *SCHUFA*, which had been delivered by the time of the oral hearing. Nor could it have considered the CJEU's judgment in that case or either the AG's Opinion or CJEU

all matters of compliance, subject to judicial supervision. *Still less is the Commissioner designated as an adjudicator authority with exclusive jurisdiction"* (§§76-77); and held that the overall objectives of the legislation should not lead to an interpretation that the complaints mechanism is *"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"* (§79).

38. The Court of Appeal concluded at §80 that:

> "For the reasons I have given I would uphold the conclusion of the judge at [85] that the legislative scheme requires the Commissioner to receive and consider a complaint and then provides the Commissioner with a broad discretion as to whether to conduct a further investigation and, if so, to what extent. I would further hold, in agreement with the judge, that having done that much the Commissioner is entitled to conclude that it is unnecessary to determine whether there has been an infringement but sufficient to reach and express a view about the likelihood that this is so and to take no further action. By doing so the Commissioner discharges his duty to inform the complainant of the outcome of their complaint."

39. Therefore, whilst the Commissioner is not required to provide a conclusive view on the merits of each and every complaint, it is clear from §§64 and 80 of *Delo* that he is required to undertake enough of an investigation to reach and express a view about the likelihood that the data controller has committed an infringement.

40. More recently, in *Smith v Information Commissioner* [2025] UKUT 74 (AAC), the UT again considered the scope of section 166 DPA 2018, concluding that the more expansive approach taken in *Killock & Veale* was preferable to the narrower approach of Mostyn J in *Delo*. In reaching that conclusion, the UT at §58 noted the potential relevance of the CJEU's *Land Hessen* judgment. In circumstances where neither party had referred to it, and given what was said in *Delo* about the *Facebook Ireland* case, the UT concluded that *Land Hessen "is not capable of having any bearing on the proper interpretation and application of section 166 which Killock and Veale and Delo have held to be a matter of domestic law interpretation".* However, the UT concluded at §58 that *"what the Court of Justice says in Land Hessen may have some bearing on the approach that the High Court might take in future to judicial reviews of decisions of the Commissioner in relation to GDPR compliance".*

<u>Factual background</u>

Consultation on the Framework

41. The introduction of the EU GDPR resulted in a significant increase in complaints to the ICO: 21,019 complaints were made in 2017/18, and that number increased to 41,661 for 2018/19. [2] This significant increase is

judgment in *Land Hessen,* all of which were delivered after the Court of Appeal's judgment was handed down.

[2] Information Commissioner's Annual Report and Financial Statements 2017-18 (p.28) and Annual Report and Financial Statements 2018/19 (p.54).

consistent with both (i) the strengthening of data protection rights under the EU GPDR and (ii) the importance of the Article 77 complaints mechanism for safeguarding those rights. Since then, the number of complaints has ranged from 31,008 in 2020/21 to 42,315 for 2024/25[3] (the most recent year for which records are publicly available).

42. By its own admission, the ICO has struggled to respond to complaints made to it, and has therefore recently consulted on changes that will help it to respond effectively to complaints. Between 22 August 2025 and 31 October 2025, it consulted on draft changes to how it handles data protection complaints. The consultation document published on 22 August (**"Consultation Document"**) set out the background to the consultation as follows:

> "Data protection is a cornerstone of modern society, ensuring that personal information is managed with care and respect. We play a crucial role in handling people's data protection complaints, supporting the public and providing organisations with clarity on how the law applies.
>
> The UK GDPR gives everyone the right to complain to the ICO about the processing of their personal information. As people become more aware of their data protection rights, we are receiving more complaints about organisations. In 2023/24, we received 39,721 complaints. In 2024/25, this rose to 42,315 complaints. Our current forecasts indicate that in 2025/26 we will receive somewhere between 45,000 and 55,000 complaints – a significant increase over just two years.
>
> We recognise our pivotal role in helping people uphold data protection rights. As the volume of complaints continues to grow, we are strategically evolving our approach by maintaining our core responsibilities while focusing our efforts on the most impactful and significant concerns to maximise public value. At the same time, we want to empower organisations to resolve complaints effectively themselves. If they do, people benefit from faster resolution. If they don't, and the issue raises wider concerns or presents a meaningful opportunity for regulatory action, we can intervene.
>
> However, our current model of case handling is increasingly stretched by the volume of complaints. We are taking longer to address people's concerns and are finding it more difficult to consistently deliver impactful outcomes. By transforming our process, we aim to better support people who have experienced harm and focus our resources on those cases where we can have the biggest impact. Organisations will also benefit from reduced routine engagement on lower-risk cases, enabling them to focus on the most significant concerns. Our goal is not just to manage demand, but to raise standards around customer experience and regulatory effectiveness. We are also confident that the changes in the Data (Use and Access) Act, particularly

[3] Information Commissioner's Annual Reports and Financial Statements 2019/20, 2020/21, 2021/22, 2022/23, 2023/24, 2024/25. The Claimant notes that the figures provided in the Commissioner's annual report for 2024/25 are different to the figure referred to in the consultation referred to below.

> the new obligations on organisations around complaint handling, will lead to more complaints being resolved without our involvement."

43. The Consultation Document proceeded to summarise the scope of the consultation and the ICO's then-current approach to complaints handling, again repeating the point made above that this approach had resulted in a backlog of complaints.

44. The Consultation Document then explained that the Commissioner had developed a draft framework:

> "The framework sets out the criteria we would consider when deciding whether to conduct a further investigation and to what extent – for example, the impact of the data protection issue on the people affected, or whether the complaint would help us to meet our strategic priorities.
>
> Our proposed approach is designed to deliver faster and more impactful outcomes, particularly for people whose complaints raise the most serious concerns. It reflects our ambition to be a strategic regulator – one that considers every complaint, responds proportionately and uses the insight gained to identify patterns or systemic risks and drive improvements in data protection practices.
>
> The proposed framework would enable us to:
>
> • assess complaints consistently and proportionately across the tens of thousands we receive;
>
> • allocate our resources effectively, focusing on the most significant issues and providing timely outcomes; and
>
> • clarify the criteria we consider when deciding how to handle a complaint, including the extent of any investigation."

45. The Consultation Document then proceeded to summarise how the draft framework would operate.

46. Next, the Consultation Document explained that, alongside the Framework, the ICO intended to introduce a *"threshold-based approach to complaint handling and build a new process around it".* That approach was said to allow the ICO to identify:

> "• when a defined number of complaints is received about an organisation – for example, six complaints within two months; or
>
> • when the number of complaints received about an organisation increases by a defined percentage amount – for example, an increase of 50% compared to the previous month.
>
> This number or increase is called the 'threshold'. When complaints about an organisation reach this threshold, it may trigger a deeper review of that organisation's practices. This may include identifying trends or themes in the complaints or consulting other ICO teams to understand any previous engagement.

> The threshold is not fixed and we can adjust it over time to reflect emerging risks or sector-specific trends."

47. The Consultation Document concluded by explaining that *"[w]e are proposing to introduce this new approach to ensure that our complaint handling is more timely, proportionate and focused on the areas where we can have the greatest impact. To measure the success of this model we will assess both operational performance and the wider outcomes it delivers for people, organisations and the ICO."*

48. The Consultation Document was accompanied by a draft Impact Assessment and "*proposed data protection harms scale*". Mr Killock understands that both documents have been updated following the consultation. The scale of harms is addressed in more detail below.

49. After the ICO considered consultation responses it published a **"Consultation Response"** (its date of publication is currently unclear to Mr Killock).

50. The Consultation Response explains that 81 responses were received, and that the ICO had made a number of changes in response to those responses. The Consultation Document also highlighted a number of points made by consultees. Mr Killock emphasises four matters for the purposes of this letter.

51. **First**, the Consultation Document records that *"Respondents raised concerns about the perceived lack of enforcement mechanisms and clear consequences for non-compliance. Multiple respondents criticised our overall approach to enforcement. Others, particularly individuals, thought we should prioritise enforcement against organisations that don't comply with the UK GDPR."* However, the ICO considered that these concerns fell outside the scope of the consultation.

52. **Second**, as the Consultation Document records:

> "Some respondents thought that the new approach would mean we wouldn't [sic] fulfil our legal duties or investigate complaints adequately. Respondents were concerned that the framework would narrow what we investigate, which could be perceived as a reduction in complaint handling. Respondents suggested we ensure that we handle complaints in line with what they consider to be our duty under data protection law to investigate all complaints and inform complainants of the progress and outcome within a reasonable period.
>
> A few respondents referred to the Government's obligation under recital 120 of the UK GDPR, arguing that we should have more resources to handle complaints. Several respondents felt that we should redirect some staff to focus on complaints.
>
> …
>
> Others felt that complaint handling would become a triage exercise rather than a guarantee that information rights will be upheld. A few respondents were concerned that our approach would lead to many complaints not being investigated and instead being recorded 'for information purposes'. Some respondents highlighted their concerns about people they described as

'vulnerable', especially children, as they felt such people would be disadvantaged or even automatically excluded.

53. The Consultation Document responded to these concerns as follows:

> "Although we're receiving an increasing number of complaints, we're committed to ensuring we handle them in line with our legal obligations. We will investigate all complaints to the extent appropriate and inform complainants of the outcome. We will decide whether we need to make more detailed enquiries based on substantive matters, such as whether the data protection issue has caused a high level of harm or whether a more detailed investigation would be in the public interest. One of our goals is to support organisations to comply with their data protection obligations as part of our complaint handling work.
>
> Our approach will be proportionate and flexible, and we recognise that we must deploy resources effectively. This means that, while we will assess all complaints against our published criteria, we may prioritise those involving the highest levels of harm or those where we need to intervene most.
>
> The more serious the harm, the more likely it is that we will give a complaint substantive attention, but we can't guarantee we will investigate every case in detail. Where resources are constrained, such as during periods of high volume, we may need to place even some high-harm cases in queues or triage them further. This approach is consistent with recital 141 of the UK GDPR, which makes clear that we have broad discretion to decide whether to conduct a further investigation and, if so, to what extent. We will avoid blanket policies that exclude entire categories of complaints and will remain transparent about the factors we consider when allocating resources.
>
> While consultation responses referred to recital 120 of the UK GPDR and suggested that we should have more resources to investigate complaints, issues such as funding are outside the scope of the consultation. We remain committed, however, to maximising the use of our resources to meet our obligations under the UK GDPR."

54. **Third**, the Consultation Document recorded the following risks highlighted by respondents, but did not provide any response to them:

> "Respondents identified various risks, including:
>
> • missing serious complaints;
>
> • failing people who've experienced harm;
>
> • misclassifying or processing complaints incorrectly, including due to insufficient guidance;
>
> • preventing people from making complaints, especially those who need support or people respondents referred to as 'vulnerable'; and
>
> • being unable to carry out our responsibilities to monitor and enforce data protection law."

55. **Fourth**, the Consultation Document recorded that:

(a) 12 respondents (i.e. around 15% of all respondents) had argued that *"[f]ailure to investigate complaints may lead to a proliferation of non-compliance, harm or both, negatively impacting wider society"*; and that *"[o]rganisations may take advantage of reduced enforcement of data protection to deprioritise data protection compliance. Where we fail to act early to address an identified harm, this harm may become more serious and costly to us, organisations or wider society."* Again, the ICO did not provide any response to these concerns.

(b) At least one respondent referred to relevant analysis in the field of behavioural economics, which *"shows that certainty of enforcement, not severity, determines compliance. By announcing low-risk complaints won't be investigated, there may be an increase in violations."*

56. The ICO's response to these concerns was that:

> "We don't accept the view that the new approach will lead to widespread non-compliance or harm. As described in the impact assessment, we believe that by triaging cases, we will be able to allocate resources more effectively and efficiently, focusing on the most significant issues and providing more timely outcomes. This prioritisation will strengthen regulatory certainty and incentivise organisations to comply with the law, reducing financial and reputational risk. Furthermore, we believe that dealing with high-risk cases more efficiently will lead to a reduction in data protection harms and the societal costs associated with non-compliance."

57. The ICO published an updated Impact Assessment at the same time as the Consultation Response.

The Framework

58. The Framework was published on or around 9 February 2026. It states at the outset that (emphasis added):

> "We assess each complaint individually and decide the extent of our involvement using the criteria set out below. Triaging complaints and handling them based on their individual circumstances allows us to:
>
> • focus on the most serious data protection issues;
>
> • provide timely outcomes; and
>
> • support organisations to comply with their data protection obligations.
>
> This means we record some complaints for information purposes only, without further investigation. …
>
> When considering a complaint, we review the details provided to determine the appropriate extent of our involvement. This can range from a light-touch review to carrying out more detailed enquiries, depending on the

circumstances and in accordance with our published criteria. This is different from deciding to open an investigation, where we send a case opening letter to an organisation to notify them."

59. The Framework goes on to explain that:

> "We examine each complaint carefully and use the criteria below to decide whether we can provide an outcome at this stage or need to look into it in more detail.
>
> Due to the range of complaints we receive, this requires a degree of judgement, so we use the following criteria to help us remain as consistent as possible."

60. The criteria for triaging complaints is then set out. The first factor given is *"Has the data protection issue caused, or is it likely to cause, anyone a high level of harm?"* (The ICO's approach to harm in complaints is summarised below.)

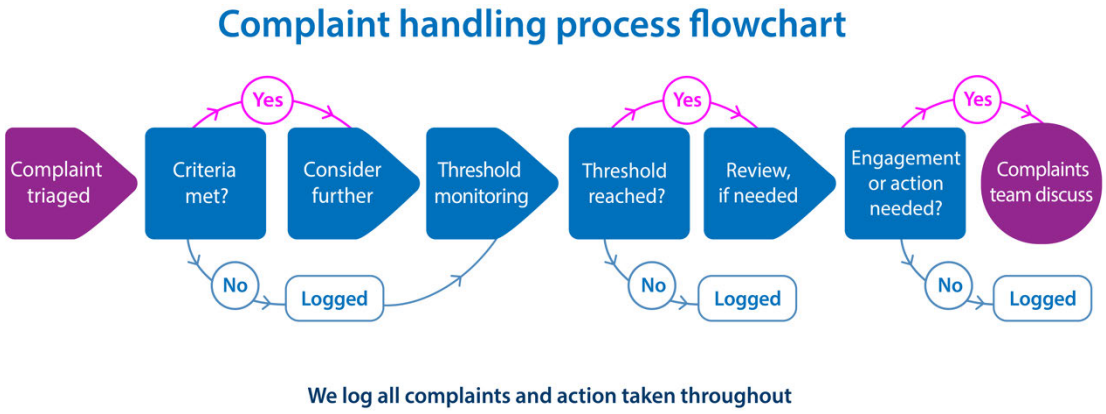
61. The Framework then states that:

> "If, based on the criteria above and our judgement, we need to investigate further before providing an outcome, we allocate the complaint to a case officer. The case officer:
>
> • weighs up the facts of what's happened, fairly and impartially;
>
> • asks the complainant and the organisation for further information, if they think they need it; and
>
> • provides an outcome."

62. The Framework makes clear that (emphasis added):

> "We may conclude, based on the above criteria and our judgement, that we don't need to obtain further information or contact the organisation. We may instead decide to record the complaint for information purposes."

63. A diagrammatic summary of the ICO's approach is provided in the Framework:



64. Further details of "*the threshold*" are then given: *"If the number of complaints goes above a certain amount (the threshold) within a certain time period"*. It appears from the Framework that, where a complaint is not investigated further – i.e. because it does not meet the criteria for further consideration – it will generally be logged for information purposes *save* where the threshold is met. If the threshold is met, then the ICO *"may analyse the available information we have about the organisation to determine whether to intervene"*.

Harm in complaints

65. The ICO has published a webpage titled "*Harm in complaints*". It explains that:

> "When we look at a complaint about how an organisation has handled people's personal information, we consider the level of harm. Our case officers do this by using the information people provide in their complaint to understand the impact it has had on them. We use our judgement to assess whether the data protection harm has a low, moderate or high-level impact. We've designed a scale of harm to help us be as consistent as possible while giving us flexibility to handle the very varied scenarios we see in complaints.
>
> We understand that the same data protection issue can affect people in very different ways. For some, it may cause real distress or anxiety, and that can be hard to measure. We also understand that personal circumstances, such as the need for extra support or living with an illness, can make the impact feel much greater.
>
> When we assess something as low or moderate harm, we still recognise that it may have been upsetting or frustrating enough for someone to make a complaint. Most people only take the time to complain when they feel strongly about what happened, and we don't want to minimise that.
>
> Our approach assesses the relative scale of harm across all complaints so we can focus our limited resources where we can make the biggest difference. This doesn't mean your experience doesn't matter; it does."

66. The various levels of harm are set out as follows (emphasis added):

> **"<u>Low level of harm</u>**
>
> For a low level of harm, we consider the impact that someone experiences because the organisation did not follow data protection law is lower, relative to the range of harms we see in complaints. For example, being annoyed, frustrated, worried, inconvenienced or mildly distressed. This is usually when:
>
> • something happens once;
>
> • the effect lasts a short time; or
>
> • there are no other adverse effects or ongoing wider impact."
>
> **Example**
>
> An employee makes a subject access request to their employer asking for information held about them. The organisation responds two days after the

calendar month timeframe. The person complains that the response is late and a specific document is missing. The organisation apologises and provides the missing document.

Why is this low harm?

• The impact is limited to someone being mildly annoyed.

• The organisation apologises and puts things right.

• The impact is short-lived.

What might change this?

If the missing document is critical to the employee (eg for an employment tribunal), the organisation would usually signpost the employee to the appropriate court process for obtaining the information.

If the delay causes additional adverse effects, we could consider this to be moderate or high harm. For example, if it prevents the employee from acting on some important information in sufficient time, or if the missing document causes the employee to miss a deadline for claiming compensation. Other examples could include instances where the impact is more serious but only happens once or lasts a short time.

…

Moderate level of harm

For a moderate level of harm, we consider the impact that someone experiences because the organisation did not follow data protection law is greater, relative to the range of harms we see, than a low level of harm and usually lasts longer.

We may also consider the harm to be moderate if the impact on the person affected is serious but only lasts a short time and is unlikely to continue or happen again.

…

Example

An organisation keeps a record that incorrectly states an employee has a criminal conviction. During a routine job vetting process, the organisation discloses this information to a potential employer. They discover the error and correct it within a month, but the employee experiences anxiety about their reputation, significant stress, and worries about the impact on their career.

Why is this moderate harm?

• The impact goes beyond someone being mildly annoyed or inconvenienced.

• Disclosing incorrect criminal offence data causes someone to be noticeably distressed and concerned about their reputation.

• The harm is not permanent.

What might change this?

If the organisation hasn't corrected the incorrect information promptly, or it has led to the employee losing their job or being unable to get another one, we could consider the harm to be high.

…

High level of harm

For a high level of harm, we consider the impact someone experiences because the organisation did not follow data protection law is the most serious, relative to the range of harms we see, and is substantial and ongoing.

…

Example

A school sends an email to all parents but mistakenly attaches the wrong document. The attachment contains sensitive information about a child, including medical details. The child's family is extremely distressed and concerned about the breach of privacy and potential gossip or discrimination.

Why is this high harm?

• The impact is significant and lasting.

• Disclosing sensitive medical information could lead to higher levels of distress or anxiety.

• The effect cannot be reversed, and the family faces ongoing worry about their child's privacy and well-being.

What might change this?

If the information is less sensitive, or if the email has only been sent to a small, relevant group and quickly contained, we could consider this to be moderate harm.

Grounds for judicial review

67. The Framework is inconsistent with the UK GDPR, and the high level of protection for personal data it is designed to achieve. As a result of the operation of the Framework, it is envisaged that significant number of complaints are triaged and logged for information purposes but never investigated. This number is likely be substantial – albeit there is no estimate in the Impact Assessment – because the justification for the Framework given

in the Consultation Document and Response is that it will help reduce the complaints backlog currently faced by the Commissioner.

68. For the reasons given below, the Framework:

(a) Is incompatible with the principle from *Gillick v West Norfolk and Wisbech Area Health Authority* [1986] AC 112, in that it imposes *"requirements which mean that it can be seen at the outset that a material and identifiable number of cases will be dealt with in an unlawful way"*: *R (A) v SSHD* [2021] 1 WLR 3931 at §63; and

(b) Frustrates the legislative purpose behind the UK GDPR: *Padfield v Minister of Agriculture Fisheries & Food* [1968] AC 997, at 1030; *R (Palestine Solidarity Campaign Ltd) v Secretary of State for Housing, Communities and Local Government* [2020] 1 WLR 1774, e.g. at §46.

69. Mr Killock relies on three points in particular.

70. **First**, the consequence of the Framework is that the Commission will, in many cases, not undertake any investigation at all. That is incompatible with the UK GDPR (including, in particular 57(1)(f) and Article 77) and frustrates the legislative purpose behind it. Although the Claimant accepts that the Commissioner has a discretion as to the appropriate scope of an investigation, it is not lawful for the Commissioner to refuse to investigate a complaint at all.

71. The purpose of an investigation is – applying the reasoning from *Delo* at §80 – to *"reach and express a view about the likelihood"* that the data controller has committed an infringement. It is not possible for the Commissioner to satisfy this standard if the complaint is simply logged for information purposes at a very early stage. That is *a fortiori* where the justification for logging the complaint is unrelated to the question of infringement, but is instead primarily based on an initial impression of the *harm* suffered by the data subject. It is also not possible, pursuant to the requirement in Article 57(1)(f) UK GDPR, to *"inform the complainant of the progress and the outcome of the investigation"* if, as a result of the triaging process, no investigation has taken.

72. The Framework includes references to the "*handling*" of complaints (per Article 57(1)(f) UK GDPR) and the need to assess "*individual circumstances*" (per Recital 129): see §58 above. However, there is nothing in the Framework to suggest that, where complaints are immediately logged for information purposes, there is any investigation beyond an initial triaging process. There is a material difference between the triaging of complaints and their investigation. Triage is concerned with classification and prioritisation, whereas investigation involves an assessment of the facts in order to reach conclusions about compliance with the law. The mere triaging of a complaint under the Framework does not fall within the ordinary meaning of the word "*investigation*" at Article 57(1)(f) and Recital 141 of the UK GDPR. Indeed, the Framework makes clear that it is only where a complaint is allocated to a case officer that an individual within the ICO *"weighs up the facts of what's happened, fairly and impartially"*.

73. **Second**, the approach in the Framework seriously undermines the purpose of the Article 77 UK GDPR complaints mechanisms. As the CJEU made clear in *SCHUFA* at §58, the complaints procedure *"is not similar to that of a petition"*

and *"is designed as a mechanism capable of effectively safeguarding the rights and interests of data subjects"* (emphasis added). See also the AG's Opinion at §42, making clear that the complaints procedure must be a *"genuine administrative remedy"*. The Framework falls way short of fulfilling this statutory purpose. Indeed, in cases where complaints are logged for information purposes, the Commissioner's approach falls squarely within the prohibited territory considered by the AG in *SCHUFA* at §39, namely where a supervisory authority proceeds on the basis that it has a *"discretion as to whether or not to handle complaints."* Whilst the Commissioner has a discretion as to *how* an investigation is conducted, the Framework is wrong to conflate this with a discretion about *whether* to investigate in the first place.

74. These matters have severe real-world implications for the effective protection of data rights:

(a) Complaints that do not raise *"the most serious data protection issues"* are not investigated under the Framework, even if an investigation might reveal that the data controller has infringed the data subject's UK GDPR rights. These complainants will be deprived of access to justice. The Commissioner's decision not to investigate will leave them with an invidious choice between defending their data rights through costly and time-consuming court proceedings or accepting an unremedied violation of those rights.

(b) The failure to enforce the UK GDPR in a significant number of cases will moreover reduce the incentives on data controllers to comply with their obligations. Many respondents raised this concern in the consultation, and at least one did so on the basis of economic analysis demonstrating that *"[b]y announcing low-risk complaints won't be investigated, there may be an increase in violations."* The Commissioner rejected these concerns in the Consultation Response, albeit his basis for doing so is unclear.

75. The impacts are particularly severe for data subjects whose complaints are assessed as raising low or moderate levels of harm. Such complaints will very rarely be investigated, as is clear from the "*harm in complaints*" webpage quoted at §65 above. This approach undermines the high level of protection of personal data that the UK GDPR seeks to achieve. The following points bear emphasis:

(a) As can be seen from the examples given on the "*harm in complaints*" webpage, cases of moderate harm are likely to constitute very significant interference with individuals' data rights – e.g. where an employer is provided with false information that a potential employee has a criminal record, or a child's sensitive data (including medical data) is sent to a small group of external recipients.

(b) The Framework's approach is likely to undermine protection for routine, but nonetheless fundamental, rights under the UK GDPR, such as the right of access at Article 15 or the right to erasure at Article 17. In cases where a data controller respectively refuses to provide personal data or delete such data, data subjects will generally only have effective recourse to the Commissioner where they can point to

a high degree of harm. This is likely to be extremely challenging in a large number of cases that these remedies were designed to address – e.g. in relation to medical, education, financial or employment data,

(c) The Framework is likely to result in arbitrary results depending on *when* the complaint is made. In particular, proactive data subjects seeking to safeguard their rights by complaining at the earliest opportunity may be penalised for doing so. To return to the Article 15 and 17 examples, it will be harder for data subjects who submit early complaints to demonstrate – applying the "harm in complaints" webpage – that the impact is *"significant and lasting"* rather than *"unlikely to continue or happen again"*.

(d) As set out above, even where the immediate impact of any breach may not be especially serious, the cumulative effect of non-enforcement of low and moderate harm cases is however likely to remove disincentives for non-compliance and erode the overall level of protection for data rights.

76. **Third**, these arguments are further strengthened by the CJEU's *Land Hessen* judgment, which at §§43 and 46 concluded that although the supervisory authority has no obligation to use corrective powers where it finds that an EU GDPR infringement has taken place, it must generally do so save in *"exceptional"* cases. This conclusion cannot be squared with the Commissioner's approach here. As set out above, where a complaint is logged for information purposes, the Commissioner will not be able to *"reach and express a view about the likelihood"* of an infringement (*Delo* at §80). As a result, the question of whether the Commissioner should use a corrective power, or exceptionally refrain from doing so, will not arise. Instead, the Framework will have the effect of precluding the use of any corrective power, because, for cases logged for information purposes, the prior issue of infringement will never arise. As a result, the Framework converts the Commissioner's decision not to use a corrective power from the individualised exception contemplated in *Land Hessen* to a blanket rule.

77. This approach entirely undermines *"the requirement of strong enforcement of the rules"* recognised in *Land Hessen* at §§38 and 46. If correct, it would allow supervisory authorities to sidestep the general rule that a corrective power must be used by adopting policies that excuse them from establishing whether an infringement has occurred in the first place.

Relief

78. The Framework is unlawful. Mr Killock will accordingly seek declaratory relief and/or an order quashing the Framework.

The details of the action that the Defendant is expected to take

79. The Commissioner is invited to revoke or alternatively revise the Framework.

ADR proposals

80. Mr Killock reluctantly brings these proceedings and remains very willing to have meaningful dialogue in relation to the issues raised and to consider suitable ADR proposals.

The details of any information sought and documents that are considered relevant and necessary

81. As you will be aware, the duty of candour applies at the pre-action stage. Please therefore provide any key documents which contain evidence relevant to the issues set out in above. Without limitation, please explain and/or provide documents detailing:

(a) The proportion of cases that the Commissioner estimates or anticipates logging for information purposes without any investigation and/or further investigation under the Framework.

(b) Any analysis undertaken by the Commissioner about alternative causes for the increase in complaints in recent years – e.g. analyses considering whether the increased number of complaints may be explained by increased non-compliance on the part of data controllers – to that given in the Consultation Document (see §41 above).

(c) The basis on which the Commissioner has estimated that complaints are expected to increase.

(d) The evidential and/or analytical basis on which the Commissioner dismissed the suggestion raised by various responses to the consultation that the Framework will foster a culture of noncompliance (see §55 above).

82. If you do not provide relevant information in response to this request, Mr Killock reserves the right to argue that the Commissioner has acted irrationally, both as a matter of process and outcome, in promulgating the Framework.

The address for reply and service of court documents:

83. Please respond to:

FAO [redacted]

Mishcon de Reya

Africa House

70 Kingsway

London, WC2B 6AH

84. We would be grateful for a reply within the standard 14 days under the Pre-Action Protocol for Judicial Review.

Yours faithfully

Mishcon de Reya LLP

Mishcon de Reya LLP

[redacted]