Written evidence submitted by Professor David Erdos, Professor of Law and the Open Society, Co-Director, Centre for Intellectual Property and Information Law Faculty of Law, University of Cambridge[1] (DPDIB31)

Written Evidence on Addressing the Supervisory Enforcement Gap

Section One – Context and Overview

The General Data Protection Regulation (GDPR) formally provides for a high level of personal data protection. It also seeks to entrust and empower Data Protection Authorities (DPAs) to secure "strong enforcement" (Recital 7) of these provisions. Indeed, Article 83 requires DPAs to administrative 'effective, proportionate and dissuasive' fines of up to €20 million or 4% of annual global turnover (if higher) and Recital 148 clarifies that fines should be imposed for any infringement unless minor or involving a disproportionate burden to a natural person where it is stated that a reprimand can be administered instead. In practice, notwithstanding recent fines of €746m against Amazon and €225m against WhatsApp,[2] regulatory enforcement has generally been limited across Europe. Part of the reason for this has been the ongoing difficulty of administering the EU GDPR's so-called One-Stop Shop (OSS) cooperation mechanism.

Following the implementation of Brexit on 1 January 2021, the UK continued to mirror the substance of the GDPR but the Information Commissioner's Office (ICO) has become fully and directly responsible for all UK data protection regulation without the need to coordinate this through the OSS. Despite this or, as a cynic might argue, because of the absence of this pan-European oversight data protection enforcement has been especially limited in the UK. Indeed, during the 2021-22 period the ICO secured no enforcement notices or criminal prosecutions and issued just four GDPR fines, all of which concerned data security[3] and which came to a grand total of just £183k (down from £633k following the ICO's decision in

[1] This submission focuses entirely on the issue of supervision enforcement. A fuller summary than set out in section one is provided in David Erdos, "UK Regulatory Enforcement of Data Protection: Current Concerns and Pathways to a More Effective Framework", *Oxford Business Law Blog* (March 2023), https://blogs.law.ox.ac.uk/oblb/blog-post/2023/03/uk-regulatory-enforcement-data-protection-current-concerns-and-pathways-more. The rest of the submission has been developed from sections five and six, as well as the appendix, of the following much longer working paper: David Erdos, 'Towards Effective Supervisory Oversight? Analysing UK Regulatory Enforcement of Data Protection and Electronic Privacy Rights and the Government's Statutory Reform Plans' (*University of Cambridge Faculty of Law Research Paper No. 16/2022*) (currently available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4284602).

[2] Tom Bateman, *WhatsApp rewrites its European privacy policy after a record €225 million GDPR fine* (2021), https://www.euronews.com/next/2021/11/22/whatsapp-rewrites-its-europe-privacy-policy-after-a-record-225-million-gdpr-fine.

[3] Information Commissioner, *Annual Report and Financial Statements 2021-22* (2022), https://ico.org.uk/media/about-the-ico/documents/4021039/ico-annual-report-2021-22.pdf, pp. 32-33.

November 2022 to reduce its fine against the Cabinet Office by an order of magnitude to just £50k[4]).

In contrast to these very low enforcement numbers, the ICO indicates that in 2021-22 it handled over 40k data subject complaints.[5] Nevertheless, as in previous years, the vast majority were closed without formal action. Moreover, despite the Data Protection Act 2018's provision of a new Order to Progress Complaints mechanism, avenues to challenge ICO inaction which are open even to respected civil society groups are extremely limited. This is principally because the mechanism's policing of the duty placed on ICO to take "appropriate steps in response" to a complaint (DPA 2018, s. 165(5)) has been interpreted, including by the Upper Tribunal in *Killock and Veale, EW and Coghlan* (2021), to be of a purely procedural as opposed to substantive nature (a holding further narrowed by the Administrative Court decision of *R (on the application of Delo) v Information Commissioner (2022)* which found that the ICO was not obliged to investigate each and every complaint). Holistic scrutiny has also been lacking, with the House of Commons' Digital Culture Media and Sport (DCMS) Committee failing to carry out a single formal review of the ICO during the (almost) half a decade since the GPDR has been in effect.[6]

Unfortunately, whilst there is merit in some of the changes proposed including reconstituting the ICO as a multi-member Commission, the DPDI (No 2) Bill could further undercut the ICO's de jure responsibilities to act as an independent and comprehensive upholder and champion of core data protection rights. In the first place, the Bill ignores binding case law which establishes that that the ICO's "primary responsibility" is to monitor and enforce the law[7] and would establish the promotion of "public trust and confidence in the processing of personal data" as an independent and coequal ICO objective alongside "secur[ing] an appropriate level of data protection" (s. 27). It would also empower the Secretary of State to issue a potentially skewed and very partial list of strategic priorities which the ICO would then need to have regard including in relation to enforcement (s. 28). Finally, it would grant the ICO broad discretion to refuse to act on complaints unless the controller has been given 45 days to respond, despite there being clear scenarios where this would be unreasonable or impracticable for the data subject.

As well **analysing the current proposals in the Bill in more detail (section 2)**, this submission put forward **new proposals in response to the unaddressed issues (section 3).** First, it argues that the Order to Progress Complaints mechanism should be amended so that it clearly requires the Tribunal to police the appropriateness of the ICO's substantive as well as procedural actions and inactions. Civil society groups should also be permitted to lodge representative complaints even without the mandate of data subjects in order to encourage well-argued, strategically important cases. Second, and at least as importantly, it proposes

[4] Information Commissioner's Office, *ICO and Cabinet Office reach agreement on New Year Honours data breach fine* (2022), https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/11/ico-and-cabinet-office-reach-agreement-on-new-year-honours-data-breach-fine/.

[5] Information Commissioner, *Annual Report and Financial Statements 2021-22* (2022), p. 42.

[6] An Inquiry into the Work of the ICO did commence in April 2019 but was discontinued after a single oral session and without any output from the Committee.

[7] C-311/18 Data Protection Commissioner v Facebook Ireland and Schrems EU:C:2020:559 at [108].

that a duty should be placed on the Equality and Human Rights Commission to carry out periodic holistic scrutiny of the ICO's enforcement track-record from a human rights perspective. A full summary of all **proposed amendments** is set out in an **Appendix** to the main submission.

Section 2 - Summary and Discrete Analysis of DPDI (No 2) Bill Proposals:

2.1 – Summary

Turning first to the **ICO's powers**, the DPDI (No 2) Bill proposes to enhance these along two lines. Firstly, with certain technical modifications, the ICO's Data Protection Act 2018 powers related to data protection *stricto senso* would be extended to its policing of the e-privacy provisions.[8] Secondly, it would be granted certain additional investigative powers including to be provided with documents and not just information[9] and to require individuals to be subject to an interview if they are suspected of having failed or failing in their data protection responsibilities.[10] In addition and as regard structure, the ICO would cease to be a corporation sole and would instead be reconstituted as corporate Information Commission composed of a majority of non-executive members, the Chief Executive (effectively the current Information Commissioner) and any other executive members whom those serving in a non-executive capacity may wish to appoint.[11]

Turning to the **ICO's objectives and priorities**, the current requirement set down in the Data Protection Act 2018 that it have regard to the importance of "an appropriate level of protection for personal data, having regard to the interests of data subjects, controllers and others and matters of general public interest"[12] would be replaced by a refashioned provision which would add as a further primary objective the promotion of "public trust and confidence in the processing of personal data".[13] In addition, the ICO would be fixed with specific responsibilities under the data protection framework itself to have regard as it considers relevant to the desirability of promoting both innovation and competition, the importance of preventing, investigating, detecting and prosecuting criminal offences and the need to safeguard public security and national security. The ICO would also be obliged to consult other relevant regulators as to how the exercise of its functions may affect economic growth, innovation and competition.[14] These duties would be addition to the ICO's existing obligation to have regard to the desirability of promoting economic growth under section 108 of the Deregulation Act 2015 and to broad principles of regulation set out in the section 21 of the Legislative and Regulatory Reform Act 2006.[15] The Secretary of State would be empowered

[8] DPDI (No. 2) Bill, cl. 86.
[9] Ibid, cl. 34.
[10] Ibid, cl. 36. Relatedly, providing a deliberately or recklessly false statement in such interviews would come a criminal offence.
[11] Ibid, cl. 100 and Sch. 13.
[12] Data Protection Act 2018, s. 2(2).
[13] DPDI (No 2) Bill, cl. 27.
[14] Ibid, cl. 27.
[15] Namely, necessity, transparency, accountability, proportionality and consistency.

to set out a statement of strategic priorities and the ICO would be obliged to publicly explain in writing how it would have regard to this. However, this wouldn't affect the carrying out of functions related to a particular person, case or investigation, would be subject to Parliamentary veto under the negative resolution procedure and could only be amended every three years or in particular prescribed circumstances.[16]

Turning finally to the **complaints and other scrutiny mechanisms**, the ICO's existing right to refuse to deal with "manifestly unfounded" complaints would be replaced with a right to refuse to those which are "vexatious"[17] and also any where the controller has not been given 45 days to handle the complaint itself. In sum, each controller would acquire explicit obligations to respond to complaints and inform on their outcome as well as to facilitate the making of these.[18] The ICO would also be required to publish guidance in this area and, if a complaint was not handled, then an appeal to the Tribunal would be possible.[19] Turning to other mechanisms for scrutiny, the ICO would be obligated to prepare and publish a strategy for carrying out its functions in accordance with its duties and to review this from time to time.[20] The ICO would also be explicitly required to prepare and publish at least annually an analysis of the ICO's performances using "key performance indicators"[21] and to prepare and publish an annual report on GDPR investigations and the exercise of the ICO's enforcement powers.[22] The former would be further specified as "factors by reference to which the Commissioner's performance can be measured most effectively"[23] and the latter as including information on the number of investigations, the different types of act and omission that were its subject matter, the enforcement powers exercised in connection with the investigations, the duration of investigations ending in the reporting period and the different types of outcome.[24]

[16] Namely, if Parliament vetoed the previous version, a general election has taken place or a significant change in the government policy relating to data protection has occurred. See Ibid, cl. 28. Whilst this is related principally to standard-setting, the last provision would link to a new statutory right of the Secretary of State to veto (without any parliamentary oversight) the adoption of any statutory Code of Practice prepared by the ICO and to require the ICO to prepare a Code in any newly prescribed area (which would be subject to the negative resolution procedure). The ICO would also be obliged to carry out and publish an impact assessment whenever it prepares a Code of Practice and (unless exempted by the Secretary of State under the negative resolution procedure) establish a panel of experts and representatives who would be required to transparently report on any draft Code and be responded to if their recommendations are not adopted. Ibid, Cl. 30

[17] DPDI (No 2) Bill, cl. 32.

[18] Ibid, cl. 39. In addition, the Secretary of State would be empowered via the negative resolution procedure to require a controller to notify the ICO of the number of complaints made to it.

[19] Ibid, cl. 40.

[20] Ibid, cl. 27.

[21] Ibid, cl. 33.

[22] Ibid, cl. 38.

[23] Ibid, cl. 33.

[24] Ibid, cl. 38.

2.2 - Discrete Analysis

There is an understandable targeted rationale for the core of many of the concrete proposals put forward in the DPDI (No 2) Bill. Nevertheless, certain caveats to this must be emphasised not least since as currently drafted some risk providing a *de jure* entrenchment of the ICO positioning away from being a comprehensive upholder of core data protection rights. Discrete changes, therefore, remain imperative. Turning first to the **powers and structure**, the limited sanctioning and other powers which the ICO enjoy in the specific area of e-privacy are clearly inadequate to the scale of challenge and many of the augmentations to the powers under the GDPR respond to concerns raised by the ICO over a significant period of time. For example, the Information Commissioner signalled before the DCMS Committee as early as 6 November 2018 that inability to "compel individuals to be interviewed" had caused investigatory difficulties.[25] Nevertheless, the Commissioner also stated "[w]e do have new powers that makes us a fit for purpose regulator".[26] Moreover, given for example the ICO's ability to issue large fines,[27] limit or even prohibit processing,[28] gain "access to all personal data and to all information necessary for the performance of its tasks"[29] and "obtain access to any premises of the controller and the processor"[30] this would appear correct as regards powers under the GDPR. Nevertheless, four and a half years on what is striking is, as Table 1 vividly illustrated above, how little these formidable powers have been effectively deployed. Similarly, at least in relation to its critical protection a natural person's right to confidentiality of communications including as this effects cookies, a serious breach of e-privacy will almost inevitably also lead to breach of the GDPR itself especially if special category or criminal offence data is thereby processed. This much is clear from the ICO's investigation into, for example, Real Time Bidding by the AdTech industry. Nevertheless, what is also apparent from this example is that, in any case, the ICO has avoided addressing this issue through deploying its formidable GDPR corrective powers. The extent to which any further powers would impact the enforcement landscape is, therefore, at best unclear. The proposal to reconstitute the ICO from a corporation sole into a multi-member corporate body similarly responds to long-standing recommendations dating back at least to the Thomas and Walport Data Sharing Review in 2008[31] and the Leveson Inquiry into the Culture, Practices and Ethics of the Press in 2012[32] and has the potential to raise the ICO's stature and capabilities, which given its enormously broad remit and role, would clearly be valuable. Nevertheless, it is important to

---

[25] House of Commons, Digital, Culture, Media and Sport Committee Sub-Committee on Online Harms and Disinformation, *Oral evidence: Disinformation and 'fake news' 6 November 2018,* https://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/oral/92327.html, Q3090.

[26] Ibid, Q3977.

[27] UK GDPR, art 83.

[28] Ibid, art 58(2)(f).

[29] Ibid, art 58(1)(e).

[30] Ibid, art 58(1)(f).

[31] Richard Thomas and Mark Walport, *Data Sharing Review* (2008), https://amberhawk.typepad.com/files/thomas-walport-datasharingreview2008.pdf, pp. 69-70.

[32] Rt Hon Lord Justice Leveson, *An inquiry into the culture, practices and ethics of the press: Report Volume III*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/270942/0780_iii.pdf, pp. 1109-10.

note that a core part of at least Leveson's recommendation was that the regulator would be led by a corporate body reflective of the various sectors and topics which it needed to be engaged with. In sum, he recommended "an Information Commission, led by a Board of Commissioners with suitable expertise drawn from the worlds of regulation, public administration, law and business and that active consideration be given in that context to the desirability of including on the Board a Commissioner from the media sector".[33] There is no certainty that this will be effected by the proposals as currently set out in the Bill or even as further elaborated in the Government's policy statements. Furthermore, it would be possible for the Chief Executive (effectively the erstwhile Information Commissioner) to be the only executive member of the Commission. **At the least, a Commissioner with specific responsibility for enforcement should also be mandatorily appointed to the Commission** in order to give monitoring and enforcement the priority specified in C-311/18 *Schrems II*.

Moving on to consider the proposals related to the **ICO's objectives**, data protection is manifestly "not an absolute right" and since it in tension with many other rights and interests "must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality".[34] There is, therefore, nothing intrinsically wrong about explicitly requiring the ICO to take into account, and even gain expert advice, on such factors as innovation and competition, the need to counter criminal activity and to safeguard public security. The framing of the ICO's core objectives and strategic priorities raises more tricky issues. Much of the thinking here appears to be based on an understanding that "the ICO is obliged to fulfil a long list of tasks, as set out in Article 57 of the UK GDPR, but without a strategic framework to guide its work".[35] In fact, case law makes clear that monitoring and enforcing the law, the first tasks listed in Article 58, are the ICO's "primary responsibility"[36] and so in examining this issue it should be of immediate concern that this prioritisation doesn't seem to have been reflected in ICO's own actions. Beyond this, the ICO is already subject to an albeit vague statutory objective of having regard to the importance of securing "an appropriate level of protection for personal data".[37] The difficulty of adding the promotion of "public trust and confidence in the processing of personal data" to this as an absolutely coequal objective is that it undercuts the general understanding that the overriding way in which a DPA ensures proper trust and confidence is by securing an appropriate level of data protection and, at the least, that it must not undertake any action which is "incompatible"[38] with this core duty. What must absolutely be avoided is a situation where a DPA might be pressured into not counteracting or perhaps even positively encouraging trust and confidence in a certain type of processing which is based on an incorrect apprehension that strong safeguards are present and is therefore misplaced. In an environment not infrequently characterised by very poor levels of compliance with even the core aspects of data protection this is far from inconceivable.

[33] Ibid, pp. 1109-10.
[34] UK GDPR, recital 4.
[35] UK Government, *Data: A New Direction* (2021), p. 115.
[36] C-311/18 *Data Protection Commissioner v Facebook Ireland, Schrems*, EU:C:2020:559, 79.
[37] Data Protection Act 2018, s. 2(2).
[38] GDPR, art. 52(2).

Therefore, **the second limb should be reformulated so that it is only applies "insofar as compatible" with the requirement to "secure an appropriate level of data protection"** which would thereby be accorded lexical priority. Concerns also arise from the proposed empowerment of the Secretary of State to issue a statement of strategic priorities which the ICO would need to have general regard including in relation to enforcement. In light of the wide sweep of data protection there is an understandable desire to ensure some democratic engagement in the setting of priorities and attempts have also been made to ensure that this wouldn't descend to ad hominin or ad feminam targeting of particular controllers or in other ways amount to micro-management. Nevertheless, as indicated by the DCMS Committee track-record in this area, there is an acute danger that politicians will end up focusing almost entirely on a small sub-set of trendy newsworthy topics to the detriment of broader matters which are more important but less alluring. The danger of an ad hoc approach could be exacerbated by the general lack of transparent scrutiny of government regulations made under the negative resolution procedure. To address these challenges, **the Secretary of State should at the least be required to seek the independent published advice of the Human Rights and Equality Commission (HREC) and then of the DCMS Committee on a draft Statement of Strategic Priorities before ensuring that they also obtain the active assent of Parliament under the positive resolution procedure**. Placing such a new responsibility on the HREC would dovetail with the wider role, to be introduced and explored in the next section, which it is proposed they should undertake in scrutinising the data protection regulatory enforcement more generally.

Turning finally to mechanisms for **scrutiny and accountability**, the placing of a requirement on the ICO to publish key performance indicators[39] and an annual report on GDPR investigations and the exercise of its enforcement powers[40] could do something to address many of the serious inconsistencies and lacunae as regards transparency. It would however be helpful to explicitly address the problems arising vis-à-vis the handling of data subject complaints by adding requirements to publish anonymized information on the subject matter of the complaints received from data subjects, findings on the merits and (as regards those held to be well-founded) how this fed into enforcement action. However, the ICO is already obliged to issue an annual report on the carrying out of its functions[41] and it must be questioned whether, absent more structural reform, the publication of further information would lead to effective scrutiny. These broader issues will be considered in the next section.

Section 3 - Responding to Issues Unaddressed in the Current DPDI (No 2) Bill

3.1 – Complaint Handling

Section one of this submission noted the very limited extent of ICO enforcement action even as regards serious breaches of data protection and notwithstanding the large number of bona fide data subject complaints, the manifest inconsistencies in that regard with the expectations

[39] DPDI (No 2) Bill, Cl. 33.
[40] Ibid, Cl. 38.
[41] Data Protection Act 2018, s 138.

of the (UK) GDPR itself, the lack of an accessible mechanism for data subjects to ensure that their complaints are properly responded to and the lack of an effective holistic scrutiniser of ICO's enforcement activity. However, these interrelated issues are not directly addressed by the DPDI (No 2) Bill at all. Given their seriousness, this constitutes a much graver problem with the Bill than the discrete issues considered above and so it is important to attempt to frame an appropriate response to them.

Turning first to the oversight of complaints handling, the most obvious and potent reform would be to amend sections 165 and 166 of the Data Protection Act 2018 so that this provides **oversight through the Tribunal of the appropriateness of the ICO's action in response to complaints not only in purely procedural terms but also in terms whether it has resorted to regulatory action including use of the ICO's formal enforcement powers as appropriate.** It is this wider understanding of "appropriate action"[42] which the Court of Justice referred to in *Schrems II* when examining the complaints lodged by Max Schrems with the DPA in Ireland. It is also the type of scrutiny which would secure the kind of oversight which was hoped for and expected by many when sections 165 and 166 were originally enacted. This should be coupled with an amendment to provide that a non-profit-profit entity with "statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms"[43] may bring otherwise bona fide complaints concerning illegality to the ICO even without the mandate of data subjects. This has long been called for by "privacy groups, children's rights organisations and consumer rights groups" including in the Government's review on this and related issues in 2020.[44] This would make it much more likely that the complaints mechanism would be used to bring well-argued, strategic issues to the ICO's attention which, if effectively responded to, could significantly improve the general data protection landscape.

The Tribunal should develop jurisprudence under a reformed section 166 remedy in line with the legal expectation, set out in recital 148 and article 83 of the (UK) GDPR, that infringements of data protection which are not "minor"[45] should (at least if the relevant actor is a legal as opposed to natural person) lead to formal enforcement action on the part of ICO in the form of "effective, proportionate and dissuasive"[46] administrative fines or, at the very least, similar corrective action. As indicated in section one, this is so radically different from the current status quo that it is likely that the concept of non-minor infringement would be broadly construed such that only clearly serious infringements would attract an expectation of a direct formal enforcement response. If Parliament was so minded, then it could explicitly provide for this by limiting such a remedy to cases which raised matters of public interest. Either way,

---

[42] C-311/18 *Data Protection Commissioner v Facebook Ireland, Schrems* at [111].
[43] UK GDPR, art 80(1).
[44] Department for Digital, Culture, Media and Sport, *UK Government response to Call for Views and Evidence – Review of Representative Action Provisions, Section 189 Data Protection Act 2018* (2021), https://www.gov.uk/government/publications/call-for-views-and-evidence-review-of-representative-action-provisions-section-189-data-protection-act-2018/uk-government-response-to-call-for-views-and-evidence-review-of-representative-action-provisions-section-189-data-protection-act-2018, para. 1.5. This review was mandated by a provision inserted in the Data Protection Act 2018.
[45] UK GDPR, recital 148.
[46] Ibid, art 83(1).

such an expectation should clearly apply to the sort of grave and systematic infractions of data protection brought to the ICO's and then the Tribunal's attention by Killock and Veale (both linked to the Open Rights Group) as regards Real Time Bidding (RTB) in *Killock and Veale v ICO, EW v ICO, Coghlan (on behalf of C) v. ICO* (2021). Therefore, under the reformulated law, the Tribunal would need to have required the ICO to pursue such formal action with "all due diligence",[47] leaving Killock and Veale's complaint open during this time and keeping them informed of progress.

3.2 – Improving Holistic Scrutiny – A new role for the Equality and Human Rights Commission

The continued restriction of active Tribunal interaction to a select number of cases highlights that such a remedy may be insufficiently powerful on its own to drive systematic change especially in more routine areas of data protection enforcement. In light of both the increasingly important rights which data protection upholds in many areas and, as importantly, its increasingly serious tensions with many other rights and interests, elected bodies clearly have an important role to play in ensuring better holistic scrutiny of a regulator such as ICO. Nevertheless, these bodies have a proclivity to concentrate on a small number of trendy newsworthy topics to the exclusion of a truly comprehensive analysis which is systematically structured according to relevant legal rights and duties. There is, therefore, a need for another body to be charged with carrying out and publicising such scrutiny for the benefit of the ICO itself, the Government, Parliamentary proceedings including the DCMS Committee and the public at large.

The most appropriate existing body to take on a scrutiny role in relation to the ICO's function in upholding core data protection rights would be the Equality and Human Rights Commission (EHRC). Recognised by the United Nations as the UK's National Human Rights Institution,[48] this body was established under the Equality Act 2006 and *inter alia* has duties not only to promote awareness, understanding and protection of human rights but also to encourage good practice in this regard.[49] The relevant statutory recognition of human rights is open-textured and so encompasses all of the "fundamental rights and freedoms of natural persons"[50] which fall within the scope of data protection (as well as rights such as freedom of expression which are generally in tension with this). The EHRC also has a track-record of running inquiries and investigations both in the human rights area and in the more restricted area of equality and non-discrimination where it also has responsibilities.[51]

In order to most effectively engage in holistic scrutiny, **the EHRC should be fixed with a discrete duty to periodically inquire into the ICO's approach to, and track-record of,**

---

[47] C-311/18 *Data Protection Commissioner v Facebook Ireland, Schrems*, 111.
[48] Baroness Kishwer Falkner, *'A status' is welcome recognition of our human rights work* (10 November 2022), https://equalityhumanrights.com/en/our-work/blogs/%E2%80%98-status%E2%80%99-welcome-recognition-our-human-rights-work.
[49] Equality Act 2006, s. 9 (1).
[50] UK GDPR, art 1 (1).
[51] See Human Rights and Equality Commission, *Inquiries and Investigations* (n.d.), https://equalityhumanrights.com/en/our-legal-action/inquiries-and-investigations.

regulatory action in enforcing data protection rights and to publicly report on the same including by setting out any relevant recommendations to guide future action. As with recommendations emanating from other EHRC's inquiries,[52] the ICO as the party under scrutiny should be required to have regard to these recommendations (subject to any being overruled by Parliament) and the report should also be laid before Parliament so that it can feed into and complement political scrutiny including by the DCMS Committee. As regards periodicity, the most straightforward approach would be to mirror the ICO's own duty of annual reporting.[53] However, a yearly report would likely place too much of a burden on both the EHRC and the ICO and also make it likely that Parliament would fail to seriously engage with each report as it was produced. Nevertheless, regularity in reporting remains vital. Therefore, a biennial reporting duty would appear to be most appropriate. Alongside being fixed with this duty, the EHRC should be granted appropriate powers of investigation including to require relevant information from ICO, to audit their operations including on-site, to interview ICO officials and to engage with other relevant parties including complainants. Finally, such a new discrete duty should come with a commitment to ongoing resources as necessary to enable the ECHR to formulate (and then refine) the human rights standards appropriate to such reviews and to carry out and report on them periodically including by engaging throughout with all relevant stakeholders such as data subjects, controllers, the ICO itself and Parliament.

Providing such a role for the EHRC would be in fully in line with the valuable strand of work which the cognate EU body in this area, the Agency for Fundamental Rights, has undertaken over many years, albeit on an extremely wide geographical basis. This agency has already produced a number of influential reports in this area including on the role of National Data Protection Authorities in 2010,[54] on access to data protection remedies in 2014[55] and on citizen understandings of data protection and privacy rights in 2020[56] (which was part of a broader fundamental rights survey). These reports have raised many issues of concern including, on occasion, some specific to the UK itself. For example, the 2020 publication (which reported on survey results from 2019) found that only 35% of UK respondents had heard of the ICO which was significantly lower than the cognate figure for the national DPA in any EU-27 Member State and far lower than the EU-27 national average of 71%.[57] The agency is continuing work connected to data protection enforcement including through a project launched in January 2022 which explores the experience of all EU Data Protection Authorities with the GDPR and which will support the European Commission's evaluation

[52] Equality Act 2016, Sch. 2, para. 18.
[53] Data Protection Act 2018, s. 139.
[54] EU Agency for Fundamental Rights, *Data Protection in the European Union: the role of National Data Protection Authorities* (2010), https://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf.
[55] EU Agency for Fundamental Rights, *Access to data protection remedies in EU Member States* (2014), https://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en_0.pdf.
[56] EU Agency for Fundamental Rights, *Your Rights Matter: Data Protection and Privacy* (2020), https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-fundamental-rights-survey-data-protection-privacy_en.pdf.
[57] Ibid, p. 14.

report on the implementation of this instrument.[58] However, following Brexit, the UK and the ICO is excluded from this valuable scrutiny. This makes it even more vital that the EHRC steps into what otherwise would be a void within this jurisdiction.

15 May 2023

Appendix: Suggested Targeted DPDI (No 2) Bill Amendments

	Powers and Structure
Information Commission (Sch. 13)	Require (under para 3(3) of Sch. 13) that the Executive members of the Commission include not only the Chief Executive but also a Commissioner with specific responsibility for Enforcement.
	Objectives
Principal Objective (cl. 27 – proposed DPA 2018 s. 120A)	State that the second limb of "promoting public trust and confidence in the processing of personal data" applies only "insofar as is compatible" with the first overriding limb to "secure an appropriate level of data protection".
Statement of Strategic Priorities (cl. 28 – proposed DPA 2018 ss. 120E-H)	Make any Statement of Strategic Priorities subject to the positive resolution procedure and require that prior to publishing any draft Statement the Secretary of State seeks the independent advice of the Equality and Human Rights Commission (EHRC) followed by that of the House of Commons DCMS Committee.
	Scrutiny and Accountability
Analysis of Performance (cl. 33 – proposed DPA 2018 s. 139A)	Require that indicators include the subject matter of complaints, the findings as to their merits and what action followed.
Annual Report on Regulatory Action (cl. 38 – proposed DPA 2018 s. 161A)	Require that the report explains how data subject complaints appearing after investigation to be well-founded fed into investigative and/or enforcement action whether on an individual or a collated basis.
Power to Refuse to Act on Certain Complaints (cl. 40 – proposed s. 165A)	Make any refusal to deal with a complaint on the basis that the relevant controller has not handled this subject to (a) it not being impracticable and/or unreasonable to make direct contact with the controller, (b) the time-period (if any) for the controller to handle this not being unreasonable (and in any case not being more than 45 days).
Complaints by Data Subjects (currently s. 165 DPA 2018)	State as new sub-section (c) in s. 165(5) that the reference to "taking appropriate steps in response to a complaint" includes "where a complaint appears after investigation to be well-founded, taking appropriate regulatory action including as appropriate through the use of the Commissioner's

[58] EU Agency for Fundamental Rights, *GDPR – the experience of data protection authorities* (n.d.), https://fra.europa.eu/en/project/2022/gdpr-experience-data-protection-authorities.

	enforcement powers or any of them as set out in Part 6 of this Act."
Representation of Data Subjects (currently art. 80 UK GDPR)	Insert a new section providing that representative complaints may be lodged with the ICO under art. 77 UK GDPR even without the mandate of the data subject by not-for-profit entities with statutory objectives in the public interest and active in the field of the protection of data subjects' rights and freedoms where they consider that rights have been infringed as a result of processing.
Order to Progress Complaints (currently s. 166 DPA 2018)	Replace s. 166(a) on the orders the Tribunal may make with "to take appropriate steps in response to the complaint including steps which require the use of the Commissioner's enforcement powers or any of them as set out in Part 6 of this Act."
Review of Regulatory Action (proposed new section and Schedule)	Require that the Equality and Human Rights Commission (EHRC) undertake a biennial review of the ICO's regulatory action from a human rights perspective using formal powers of information, audit and interview and that it publishes a report on this including relevant recommendations. The ICO should be required to have regard to this (including in drawing up its forward-looking strategy) and the report should be laid before Parliament.