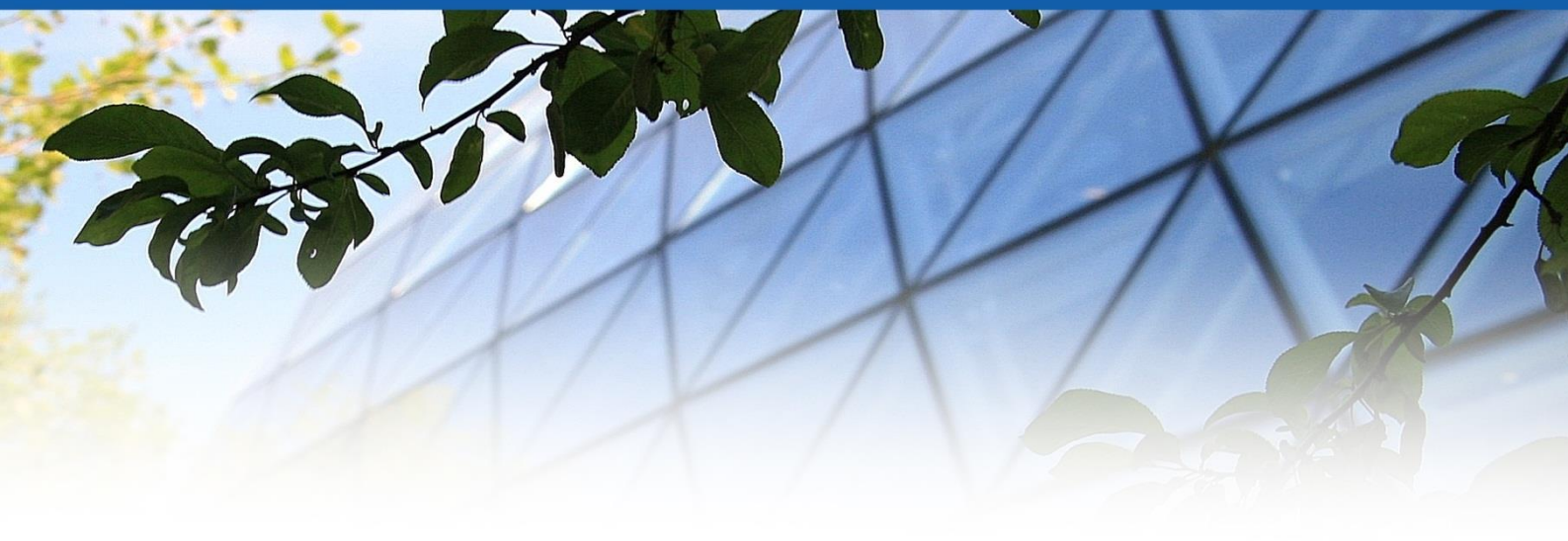
Legal Studies Research Paper Series

UNIVERSITY OF CAMBRIDGE
Faculty of Law



PAPER NO. 14/2020

APRIL 2020

Accountability and the UK Data Protection Authority: From Cause for Data Subject Complaint to a Model for Europe?

David Erdos

Further information about the University of Cambridge Faculty of Law Legal Studies Research Paper Series can be found at http://www.law.cam.ac.uk/ssrn/

Accountability and the UK Data Protection Authority: From Cause for Data Subject Complaint to a Model for Europe?

David Erdos, Faculty of Law, University of Cambridge[1]

Abstract: European data protection has long emphasized the role of the Data Protection Authority (DPA) in ensuring relief for data subjects. However, taking the UK case an example, this article demonstrates that authorities can often adopt a highly discretionary and selective approach to data subject complaints. Although such a stance may appear justified by both the myriad types of potentially impactful processing and often generally poor compliance, it is precisely this environment makes a reasonably comprehensive regulatory approach important. However, whilst both the General Data Protection Regulation and increasingly Court of Justice jurisprudence specify important procedural and substantive duties for DPAs as regards complaints, a severe practical accountability gap may remain. It is argued that, notwithstanding disappointing case law to date, the UK's recent empowerment of its accessible tribunal system to order the DPA to progress complaints could provide a valuable model of European DPA accountability going forward even after Brexit.

Keywords: data protection, judicial review, redress mechanisms, regulation, monetary penalties, privacy, tribunals.

I. Introduction

The ever-greater spread, retention and use of personal data is exercising an increasing impact on all facets of our lives - social, political and economic. The growing salience of the data protection framework is a natural corollary of this and (putting to one-side its many flaws and even absurdities) the General Data Protection Regulation 2016/679 (GDPR) puts in place a powerful set of subjective rights and expectations to safeguard our interests as data subjects within this very challenging environment. These relate in particular to an expectation that competing interests including our own will be balanced fairly, that standards such as data minimization and accuracy we be adhered to, that data use will be transparent and that we will be able to exercise a degree of control over processing especially when the data or context is of a sensitive nature. Whilst the GDPR has introduced many (both positive and negative) substantive changes, much of this framework dates back at least to the very beginnings of EU data protection.[2] But how, in the face of unrelenting socio-technological pressures, are we to ensure that this formal rights and expectations don't in become a 'dead letter' in reality? Building on the former Data Protection Directive (DPD) 95/46, the

[1] I am very grateful to Jon Baines for pointing me in the direction of relevant First-Tier Tribunal (Information Rights) case law on the matters discussed in this piece. Any errors remain my own. Comments welcome which should be directed to doe20@cam.ac.uk.

[2] See Paul De Hert and Vagelis Papakonstantinou, "The new General Data Protection Regulation: Still a sound system for the protection of individuals?" *Computer Law & Security Review* (Vol. 32(2), pp. 179-194) (2016).

GDPR suggests a number of answers to this conundrum including enabling individuals (and, in some circumstances, even collective bodies) to pursue private actions for injunctive or compensatory relief in the event of breach.[3] However, also following on from the Directive, the GDPR's primary answer is to enable data subjects to reach out to statutory Data Protection Authorities (DPAs) which it not only sees as "essential component"[4] of the framework but also endows with an unprecedented range of tasks and powers to ensure compliance with, and punish infraction of the law.

II. Data Subject GDPR Accountability Rights before the DPA

Turning specifically to the interface between DPAs and data subjects, the GDPR grants individuals a specific right to lodge claims of infringement of data protection as complaints before a DPA[5] which is then obliged to "handle" the complaint, "investigate, to the extent appropriate" and to "inform the complainant of the progress and the outcome of the investigation within a reasonable period".[6] Putting to one side the complexities of competence which can arise with cross-border processing under the GDPR's cooperation and consistency mechanism,[7] this Regulation grants DPAs far-reaching investigative powers[8] which they must use "to the extent appropriate".[9] Moreover, it is also clear that insofar as any investigation discloses an infraction of the law then the DPA must also look at using its far-reaching corrective powers.[10] In particular, for almost all significant infractions of the law, the regulator is obliged to administer a system of administrative fines which "in each individual case" must be "effective, proportionate and dissuasive".[11] Indeed, Recital 148 of the GDPR indicates "[i]n order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for *any* infringement of this Regulation" (emphasis added). In partial derogation from this, the Recital does acknowledge that in the case of a "minor infringement" or where "the fine likely to be imposed would constitute a disproportionate burden to a natural person" a "reprimand" may be issued in lieu of this. Such a reprimand is also defined as a formal corrective powers of DPAs[12] alongside both warnings and a variety of injunctive orders.

III. DPA Accountability Duties Specified in Court of Justice Case Law

Turning back to the former DPD, this instrument similarly set out DPA duties as regards data subject claims or complaints. Moreover, although its detailed elucidation of these was largely limited to the investigative stage,[13] recent human rights influenced jurisprudence from the Court of Justice has provided further important elucidation which clearly also specify DPA obligations to

[3] GDPR, art. 76.
[4] Ibid, recital. 117.
[5] Ibid, art. 77(1).
[6] Ibid, art. 57(1).
[7] Ibid, art. 60-76. For a recent concerning analysis of this mechanism see Nicholas Vinocur, "'We have a huge problem': European regulator despairs over lack of enforcement" *Politico* (27 December 2019), https://www.politico.eu/article/we-have-a-huge-problem-european-regulator-despairs-over-lack-of-enforcement/ (accessed 17 January 2020).
[8] GDPR, art. 58(1).
[9] Ibid, art. 57(1).
[10] Ibid, art. 58(2).
[11] Ibid, art. 83(1).
[12] Ibid, art. 58(2)(b).
[13] Ibid, art. 28(4).

ensure corrective action. For example, in the seminal right to deindexing case of *Google Spain* (2014), the Court found that

> Where the controller does not grant the request, the data subject may bring the matter before the supervisory authority or the judicial authority so that it carries out the necessary checks *and orders the controller to take specific measures accordingly*.
>
> In this connection, it is noted that it is clear from Article 28(3) and (4) of Directive 95/46 that each supervisory authority is to hear claims lodged by any person concerning the protection of his rights and freedoms in regard to the processing of personal data and that it has investigative powers and effective powers of intervention enabling it to order in particular the blocking, erasure or destruction of data or to impose a temporary or definitive ban on such processing.
>
> It is in light of those considerations that it is necessary to interpret and apply the provisions of Directive 95/46 governing the data subject's rights when he lodges with the supervisory authority or judicial authority a request such as that at issue in the main proceedings.[14]

Meanwhile, in the case of *Schrems I* (2015) which struck down 'Safe Harbor' - the EU-US' personal data transfer mechanism - the Court held that in cases where an individual "whose personal data has been or could be" transferred under such a mechanism contests

> the compatibility of that decision [which authorized such a mechanism] with the protection of the privacy and of the fundamental rights and freedoms of individuals, it Is incumbent upon the national supervisory authority to examine the claim *with all due diligence*.[15]

Finally, we must consider the ongoing case of *Schrems II* which was originally involved concerns lodged under the DPD as regards the workings of the standard contractual clauses data transfer mechanism but looks set to be decided as per the new provisions of the GDPR. In an Opinion issued late last year, the Advocate General Opinion in this case developed the logic of *Schrems I* and held that:

> [A] supervisory authority must examine with all due diligence the complaint lodged by a person whose data are alleged to be transferred to a third country in breach of the standard contractual clauses applicable to the transfer. Article 58(1) of the GDPR confers on the supervisory authorities, for that purpose, significant investigative powers.
>
> The competent authority is also *required to react appropriately to any infringements* of the rights of the data subject which it has established following its investigation. In that regard, each supervisory authority has, under Article 58(2) of the GDPR, a wide range of means – the various powers to adopt corrective measures in that provision – of carrying out the task entrusted to it.
>
> Although the choice of the most effective means is a matter for the discretion of the competent supervisory authority having regard to all the circumstances of the transfer at issue, that authority is required to carry out in full the supervisory task entrusted to it. *Where appropriate, it must suspend the transfer* if it concludes that the standard contractual clauses are not being complied with and that appropriate protection of the data transferred

[14] C-131/12 *Google Spain*, EU:C:2014:317 at [77]-[79] (emphasis added).
[15] C-362/14 *Schrems v Data Protection Commissioner*, EU:C:2015:650 at [63] (emphasis added).

> cannot be ensured by other means, where the exporter has not itself put an end to the transfer.[16]

IV. The Emergence of a Highly Discretionary and Selective DPA Approach:

In light of the above, and notwithstanding suggestions which are sometimes put forward in the literature,[17] it should be clear that European DPAs have not just wide-ranging powers but also owe far-reaching duties to data subjects which they cannot legally derogate from. In practice, however, many regulators have pursued an extremely, and at least until onset of the GDPR increasingly, discretionary and selective approach. Whilst far from unique, [18] this later approach was particularly championed by UK DPA, the Information Commissioner's Office (ICO). Thus, notwithstanding a binding statutory obligation to assess such complaints lodged with it under the DPD, in 2013-14 the ICO sought relabel these as mere 'concerns' and introduce considerable discretion in this regard:

> The approach we intended to take to deal with each concern will depend on whether we identify an opportunity to improve information rights practice … We may make an assessment under section 42 of the [UK] DPA [Data Protection Act 1998] where we think this adds value or where the customer has asked us to do so. We may simply offer advice to both parties and ask the organisation to take ownership of their customer or client's concern. We will decide how we can best tackle each concern on a case by case basis.[19]

The perspective behind this was encapsulated well the following year by the UK Information Commissioner Christopher Graham in a speech delivered at the 2015 European Data Protection Authority Spring Conference in Manchester:

> In the face of the challenge we face, we will only be effective if we accept that we will not achieve anything worthwhile if we try to do everything, including some activities that are worth very little in any event. 'Less' really is 'more' – or as my predecessor Richard Thomas used to put it 'Be selective, to be effective'.[20]

---

[16] C-311/18 *Data Protection Commissioner v Facebook Ireland, Schrems* (Advocate-General Opinion), EU:C:2019:1145 at [146]-[148] (emphasis added).

[17] Thus, for example, Hijmans (2016) states that "the powers and duties of DPAs, by nature, imply a high level of discretion" (p. 359) although he does caveat this somewhat by acknowledging that "DPAs are free to set their own agenda, but with one limitation, which is their obligation to handle complaints" (p. 383). See Hielke Hijmans, *The European Union as Guardian of Internet Privacy* (Springer, 2016).

[18] Not only has the ICO not been alone amongst European DPAs but it also has not been the most extreme in this regard. To the contrary, during the latter days of the Directive the Dutch DPA (in)famously withdraw all modalities for data subjects to contact them in a way which would secure a reply, replacing this only with an ability to offer a 'tip' (see Autoriteit Persoonsgegevens, *Tip ons* (n.d.), https://web.archive.org/web/20160215002019/https://autoriteitpersoonsgegevens.nl/nl/contact-met-het-cbp/tip-ons (accessed 17 January 2020). Under the GDPR, this stance has been modified. See Autoriteit Persoonsgegevens, *Klacht melden bij de AP* (n. d.), https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/gebruik-uw-privacyrechten/klacht-melden-bij-de-ap (accessed 17 January 2020).

[19] Information Commissioner's Office, *Consultation: Our New Approach to Data Protection Concerns* (2013), https://ico.org.uk/media/about-the-ico/consultations/2019/a-new-approach-consultation.pdf (accessed 17 January 2020), pp. 5-6.

[20] Graham, Christopher, "Spring Conference Keynote" (2015), https://web.archive.org/web/20150924064449/https://ico.org.uk/media/1431716/christopher-graham-spring-conference-speech-190515.docx (accessed 17 January 2020).

At least until recently, the ICO was clearly indicating that they intended to maintain this very selective and discretionary approach into the GDPR-era. Thus, writing in August 2017, the current UK Information Commissioner Elizabeth Denham stated:

> Issuing fines has been and will continue to be, a last resort. Last year (2016/2017) we concluded 17,300 cases. I can tell you that 16 of them resulted in fines for the organisations concerned.[21]

V. Critique of the Highly Discretionary and Selective DPA Approach:

Seen from the perspective of the regulator, it is possible to have a good deal of sympathy for this focus on (self)-selection and discretion. DPAs are generally endowed with very limited resources[22] but are confronted with regulating an almost unfathomable range of personal data processing across political, social and economic life. Even more problematically, this processing often – and quite probably increasingly - is not conducted in a way which pays proper heed to an individual's legal rights. Thus, to give just two examples, an October 2017 ICO review of thirty websites "in the retail, banking and lending, and travel and finance price comparison sectors" found that most were "too vague and generally inadequate". In particular, 87% failed to adequately explain whether they shared data with third parties and if so who, 87% failed to specify how and where information would be stored and 80% made no reference to their retention policy.[23] Meanwhile, in June 2019 an ongoing ICO inquiry into just one aspect of the adtech business (namely, real time bidding for spots on data subjects' information stream) located a litany of endemic legal failings including that

- "[p]rocessing of non-special category data is taking place unlawfully at the point of collection due to the perception that legitimate interests can be used for placing and/or reading a cookie or other technology (rather than obtaining the consent PECR[24] requires)",
- "processing of special category data is taking place unlawfully as explicit consent is not being collected (and no other condition applies)",
- "[p]rivacy information provided to individuals lacks clarity whilst also being overly complex",
- "[t]housands of organisations are processing billions of requests in the UK each week with (at best) inconsistent application of adequate technical and organisational measures to secure the data in transit and at rest, and with little or no consideration as to the requirements of data protection law about international transfers of personal data",

---

[21] Denham, Elizabeth, *GDPR – Sorting the Fact from the Fiction* (2017), https://ico.org.uk/about-the-ico/news-and-events/blog-gdpr-sorting-the-fact-from-the-fiction/ (accessed 17 January 2020).

[22] The resource gap continues to be highlighted by European DPAs as a major problem Thus, the 2018 Annual Report of the European Data Protection Board stated that "[m]ost of the SAs [Supervisory Authorities] (17) stated that they required an increase of around 30-50% to perform their duties. However, almost none of the SAs received the requested amount. In some extreme cases, SAs have a need for up to double their current budget". See European Data Protection Board, 2018 Annual Report: Cooperation and Transparency (2019), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_annual_report_2018_-_digital_final_1507_en.pdf, (accessed 17 January 2020), p. 21.

[23] Information Commissioner's Office, *International enforcement operation finds website privacy notices are too vague and generally inadequate* (2017), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/10/international-enforcement-operation-finds-website-privacy-notices-are-too-vague-and-generally-inadequate/ (accessed 17 January 2020).

[24] Privacy and Electronic Communications (EC Directive) Regulations 2003/2426 which implements the e-Privacy Directive 2000/58/EC (as amended) in the UK.

- "[t]here are similar inconsistencies about the application of data minimisation and retention controls" and
- "[i]ndividuals have no guarantees about the security of their personal data within the ecoysystem".[25]

However, looking at this from the perspective of the data subject, it is precisely the same picture of wide-ranging, legally problematic and (at least potentially) highly impactful processing which makes it so important that there is a clear avenue for redress. Moreover, research has long highlighted that in the great majority of situations the only reasonably available avenue is to make contact with the DPA. Thus, a report in 2013 by the EU Agency for Fundamental Rights found that DPAs "play a crucial role in processing the overwhelming majority of data protection complaints", whereas "very few data protection cases [were] initiated" in the regular courts and data protection issues were "marginalised".[26] This practical centrality of the DPA is particularly apparent in the UK (and indeed other predominantly common law jurisdictions such as Ireland) given the notoriously high cost of securing justice through the regular court system.[27] At the very least, therefore, it is vital that a data subject is able to ensure that a DPA is operating according to the law and that it can robustly justify any discretionary choices and priorities that it is setting. Again, this acquires particularly importance in the UK given that the ICO's historically highly discretionary stance has arguably sat in considerable tension with even the former DPD's supervisory framework as elucidated in binding Court of Justice case law. Moreover, for reasons elucidated above, such tensions could easily become far more acute under the GDPR. Thus, contrary to the thrust of Elizabeth Denham's remarks above, an *ex ante* stance which led to only around 0.001% (16/17,300) of 2016/17 cases being closed with a fine clearly requires fundamental reassessment in light of the requirements for formal intervention that are established by the GDPR. This is especially the case given the ICO only positively established that no further action was required on the part of the data controller in around-third of these cases[28] and that the authority's use of its other formal corrective powers such as injunctions have been similarly low.[29]

[25] Information Commissioner's Office, *Update Report into Adtech and Real Timing Bidding* (2019), https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf (accessed 17 January 2020), p. 23.

[26] EU Agency for Fundamental Rights, *Access to Data Protection Remedies in the EU Member States* (2013), https://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en.pdf (accessed 17 January 2020).

[27] See, for example, Owen Bowcott, "Top judge says justice system is now unaffordable to most", *The Guardian*, 13 January 2016, https://www.theguardian.com/law/2016/jan/13/uk-most-senior-judge-says-justice-has-become-unaffordable-to-most (accessed 17 January 2020) (reporting comments of the then Lord Chief Justice for England and Wales, Lord Thomas of Gwmgiedd).

[28] Information Commissioner's Office, *Annual Report and Financial Statements 2016/17* (2017), https://ico.org.uk/media/about-the-ico/documents/2014449/ico053-annual-report-201617-s12-aw-web-version.pdf (accessed 17 January 2020), p. 18

[29] For example, in 2017/18 it appears to have issued just six enforcement notices under the DPA 1998, with fourteen further preliminary enforcement notices being drawn up and ten enforcement notices issued under PECR. See Information Commissioner's Office, *Annual Report and Financial Statements 2017-18*, https://ico.org.uk/media/about-the-ico/documents/2259463/annual-report-201718.pdf (accessed 17 January 2020), p. 22.

VI. A New Mechanism to Ensure DPA Legal Accountability?

Theoretically, UK data subjects even during the time of DPD could have addressed some of these legality and reasonableness concerns through the modality of judicial review. In practice, however, the formidable barriers – especially, but not only, financial – to accessing the administrative courts have meant that the ICO appears never to have been subject to a full judicial review action – successful or unsuccessful – for any of its data protection work to date.[30] Effective legal accountability has, therefore, essentially been absent throughout this period. However, in a refreshing departure, the UK's Data Protection Act (DPA) 2018 sought to address this accountability gap by establishing a new right for data subjects to apply for an "order to progress complaints"[31] through the UK's free and accessible tribunal system. This provision built on an explicit stipulation within the GDPR[32] that mandates access to an "effective judicial remedy" where a DPA "does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint".[33] Set out in section 166 of the UK DPA 2018, this provision states:

(1) This section applies where, after a data subject has made a complaint under section 165 or Article 77 of the GDPR, the Commissioner –
   (a) fails to take appropriate steps to respond to the complaint,
   (b) fails to provide the complainant with information about progress on the complaint, before the end of the period of 3 months beginning when the Commissioner received the complaint, or
   (c) if the Commissioner's consideration of the complaint is not concluded during that period, fails to provide the complainant with such information during a subsequent period of 3 months.

(2) The Tribunal may, on application by the data subject, make an order requiring the Commission –
   (a) to take appropriate steps to respond to the complaint, or
   (b) to inform the complainant of progress on the complaint, or of the outcome of the complaint, within a period specified in the order.

(3) Section 165(5) applies for the purpose of subsections (1)(a) and (2)(a) as it applies for the purpose for the purposes of section 154(4)(a).

Meanwhile, the relevant parts of section 165 state:

(4) If the Commission receives a complaint … the Commissioner must –
   (a) take appropriate steps to respond to the complaint,
   (b) inform the complainant of the outcome of the complaint,
   (c) inform the complainant of the rights under section 166, and
   (d) if asked to do so by the complainant, provide the complainant with further information about how to pursue the complaint.

(5) The reference in subsection 4(a) to taking appropriate steps in response to a complaint includes –

[30] The (again often merely theoretical) availability of an alternative remedy in the form of private court action against the controller has also been invoked by the Administrative Court in refusing requests. See, for example, *R (Khashaba) v Information Commissioner* (CO/2399/2015) (declaring inadmissible the applicant's attempted judicial review of the ICO for refusing to take action against Google's refusal to deindex his personal information on the grounds *inter alia* that he had an alternative remedy through suing Google directly).
[31] Data Protection Act 2018, s. 166.
[32] and also article 53(2) of the Law Enforcement Directive 2016/680.
[33] GDPR, art. 78(2); LED, art.53(2).

(a) Investigating the subject matter of the complaint, to the extent appropriate, and
(b) Informing the complaint about progress on the complaint, including about whether further investigation or coordination with another supervisory authority or foreign designated authority is necessary.

As enacted, this right enabled the data subject to challenge the ICO response to their complaint under both certain bright-line procedural standards and an open-textured standard of "appropriate[ness]". It, therefore, appeared to offer individuals a powerful new redress mechanism. This understanding also received support from statements made to Parliament by Ministers during the parliamentary passage of the DPA 2018. For example, Lord Ashton of Hyde – the Minister who shepherded this Act through Parliament - stated the

> [Information Commissioner's] role is to help us to comply with the law to regulate its operation, which involves fairly handling complaints from data subjects about the processing of their personal data by controllers and processors, and to penalise those found to be in breach.[34]

Unfortunately, however, early case decisions from the UK's First-Tier Tribunal (Information Rights) indicates that it is interpreting this new remedy in an extremely narrow and entirely procedural manner to the clear detriment of data subject's rights and interests.

In sum, from January 2019 onwards, the First-Tier Tribunal (Information Rights) has decided at least six cases (all but one[35] of which was decided on the papers) curtly rejecting the data subject's claim for an order in only three pages of judgment apiece and with practically no individual reasoning. In all these cases the Information Commissioner has clearly argued that "the Tribunal's jurisdiction is limited to procedural failings and is not intended to serve as an appeal against outcome"[36] and the Tribunal has (at least implicitly) accepted the validity of this claim. Indeed, in its last four judgements the Tribunal has explicitly stated that the "appropriate steps" which must be taken by the Information Commissioner are "defined by s. 165(5) DPA 2018 as investigating the subject matter of the complaint 'to the extent appropriate' and keeping the complainant updated as to the progress of inquiries".[37] Meanwhile, its website appears to conceptualize this right in an even narrower and more formalistic manner, suggesting that a data subject should only consider applying "if [they] have not heard from the ICO three months after making a complaint under Section 165 of the Data Protection Act 2018".[38] Finally, in the most recent published tribunal case where the applicant provided evidence that the Information Commissioner *had* failed in the procedural duty to respond within three months, the Tribunal's response was limited to a finding that this failing had "been remedied"[39] as the Commissioner had responded by the time the case was heard. In sum, therefore, this new provision has not yet provided data subjects with the accountability and potential redress which they may have hoped for.

---

[34] UK Parliament, House of Lords, *Hansard*, 20 November 2017, https://hansard.parliament.uk/lords/2017-11-20/debates/934984ICA-96BC-43FB-B747-6A5E09B62DAD/DataProtectionBill (17 January 2020).
[35] *Shiel v Information Commissioner* [2019] UKFTT 2019/0018 (GRC).
[36] See, for example, *Platts v Information Commissioner* [2019] UKFTT 2018/0211 (GRC).
[37] See, for example, *Shiel v Information Commissioner* [2019] UKFTT 2019/0018 (GRC) at [11].
[38] HM Courts and Tribunals Service, *Information Rights and Data Protection: Appeal Against the Information Commissioner* (last updated 10 September 2018), https://www.gov.uk/guidance/information-rights-appeal-against-the-commissioners-decision (accessed 17 January 2020).
[39] *Smith v Information Commissioner* [2019] UKFTT 2019/0069 (GRC) at [12].

VII. Orders to Progress Data Subject Complaints – A Correct and Promising Approach

It would clearly be absurd if the ICO or any other European DPA was obliged to exhaustively investigate every data subject complaint and/or respond to any infraction located using it strongest corrective powers. This would be highly disproportionate vis-à-vis both the data controller and the DPA and would anyway be unachievable given the highly problematic (non)compliant environment within which European DPAs must deploy their limited resources. Such an exacting approach is also manifestly not required in the scheme laid down by either the GDPR or the UK DPA 2018 and it is also clear that the latter scheme neither requires nor enables the UK First-Tier Tribunal (Information Rights) to simply substitute its own judgments for those of the UK Information Commissioner. Nevertheless, what the Tribunal must ensure is that the entirety of the ICO's response to a data subject's complaint is comprehensively "appropriate".[40] This duty is additional to policing the bright-line formal guarantee of an information update on any complaint at least within three months.[41] Moreover, quite contrary to perspective put forward by the ICO and in the tribunal judgments above, 'appropriate[ness]' is not defined by section 165(5). Instead, this section simply provides a non-exhaustive elucidation of some aspects which it "includes". It is also not merely procedural. Instead, this concept requires full and generous interpretation in accordance with the standards set down in both the GDPR and in Court of Justice case law. As elucidated in sections II and III above, these standards have significant procedural and substantive elements. Thus, at least where serious and far-reaching infringements are alleged, a DPA is obliged to examine a complaint with "all due diligence" using its "significant investigative powers"[42] as necessary. Moreover, the DPA is "also required to react appropriately to any infringements of the rights of the data subject which it has established following its investigation".[43] In that regard, the GPDR does clearly establish a presumption that a DPA will issue effective, proportionate and dissuasive fines or at least take comparable formal corrective action as regards significant infringements of data protection.[44] Moreover, case law going back to *Google Spain* (2014) has also established that a DPA may be similarly obliged to take injunctive action.[45]

The UK ICO is likely to strongly resist the application of an accountability framework as mapped out above. The resistance would be understandable given the ICO's (and indeed many other European DPA's) highly discretionary culture that (as seen above) has sometimes resulted in the abandonment of even the pretence at a comprehensive approach to the defence of data subject's rights. However, for at least three powerful reasons, such resistance should be subject to challenge. To begin with, it is clear that the "selective"[46] and discretionary regulatory approach is legally problematic under the European data protection framework, especially as set out in the GDPR. Secondly, it is also an approach that inevitably leads to a lack of sufficient accountability on the part of the DPA and a lack of sufficient empowerment on the part of the data subject. Finally, under the GDPR, the ICO's data protection resources have exhibited a significant increase – from roughly £22m in 2017-18 to almost 41m in 2018-19[47] – and with this comes a greater ability for it to

[40] DPA 2018, s. 166(1)(a).
[41] Ibid, s. 166(b)-(c).
[42] C-311/18 *Data Protection Commission v Facebook Ireland, Schrems*, EU:C:2019:1145 at [146].
[43] Ibid at [147].
[44] GDPR, recital 148, art. 83(1).
[45] C-131/12 *Google Spain* at [77].
[46] Graham, Christopher, "Spring Conference Keynote" (2015).
[47] Information Commissioner's Office, *Annual Report and Financial Statements 2018-19*, https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf (accessed 17 January 2020), p. 106.

truly embrace the entirety of its role. In sum, therefore, the UK's specialist First-Tier Tribunal (Information Rights) should seize the opportunity of developing this framework of accountability under the new provisions set out in the DPA 2018. This should not and indeed cannot result in this Tribunal either acting as a primary decision-making or putting unrealistic demands on the ICO. Instead, it will require the ICO to clearly and convincingly justify both its procedural and substantive choices according to the standards set down in data protection law.

VIII. Conclusions and Wider Context:

With the jury still clearly out on whether the expectations established by the GDPR can be fulfilled, this is clearly a very challenging time for European data protection. In light of the myriad problems confronting the GDPR, such a fulfilment may ultimately prove impossible.[48] However, what is clear is that any chance of a positive answer to this question critically depends on ensuring that DPAs are genuinely accountable for delivering effective data protection at a practical level. The challenges to that explored in this article are certainly not unique to the UK. Moreover, if propertly interpreted and deployed, the UK's empowerment of a free and accessible tribunal system to issue orders compelling subject complaints to be progressed could provide something of an exemplar for DPA accountability going forward. In that regard, it is important to note that even after the transition period, the UK's Brexit regulations provide for a continuation of both the GDPR (with the notable exception of its cooperation and consistency mechanism) and also this order to progress complaints remedy.[49] In sum, therefore, even after Brexit the UK legal framework and this innovative new legal mechanism has an opportunity to provide a potentially useful model of accountability for European data protection regulation more broadly.

[48] For an excellent provocative analysis of some of the most fundamental difficulties see Bert-Jaap Koops, 'The Trouble with European Data Protection Law', *International Data Privacy Law* (Vol. 4(4), pp. 250-261) (2014).
[49] See Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019/419.