Response to Department for Digital, Culture, Media and Sport Call for views and evidence - Review of Representative Action Provisions, Section 189 Data Protection Act 2018

22 October 2020

Open Rights Group would like to thank the Department for Digital, Culture, Media and Sport for the opportunity to respond to the consultation on representative action provisions in the Data Protection Act 2018. Open Rights Group are a not for profit digital rights campaigning organisation, focusing on the right to privacy online, freedom of expression and government surveillance. Our work often focuses on data protection law and we have been part of high profile actions towards data controllers in the public and private sector.

Open Rights Group express support for the inclusion of new representative powers in the Data Protection Act 2018. Implementing Article 80(2) of the General Data Protection Regulation which would allow properly constituted organisations to take complaints to the Information Commissioner's Office will provide a number of benefits:

- it will improve the enforcement options available for challenging practices that breach data protection law that are not being addressed, in particular highly complex systemic issues and taboo or sensitive processing
- It will meet the Government's goal in the National Data Strategy of improving fairness, transparency and trust in the data economy.

- Other alternative measures for these actions have profound hurdles that restrict action or fail to accommodate the suite of remedies that Article 80(2) can provide.

Q1. Are you responding to this consultation as:

d. A third sector organisation, (e.g. charity, social enterprise)

Q2. What is your view on the uptake and operation of representative action provisions to date and what can be done to improve it? Please provide any relevant data and, where possible, make clear its source. For adults and children respectively, please explain what advice and support is currently available in relation to these provisions.

There is no reliable data on the uptake of these complaints. This is likely partly due to the lack of actions taken as the consultation notes set out, but it is also a data collection issue. The Information Commissioner's Office does not record the form of complaints in a meaningful way that separates out traditional representative actions (a solicitor, a member of a family with power of attorney) with the civil society representative actions.[1]

It is worth noting that the uptake and operation of representative actions across Europe has been relatively low. The Fundamental Rights Agency of the European Union in released a study in June 2019 one year on from GDPR's adoption that showed that of 103 organisations surveyed that have data protection as a core area of their work, only four had filed a complaint without being mandated by an individual

1
See response from ICO to a request under Freedom of Information Act 2000 from Matthew Rice, 7 May 2020, https://www.whatdotheyknow.com/request/659874/response/1569198/attach/html/2/response%20letter%2007.05.2020.pdf.html

(i.e. under the Article 80(2) measure) and of those same 103 just 3 had been mandated by an individual to file a data protection complaint.[2] These numbers suggest that the representative actions are not something that every organisation reaches for automatically in their work, we discuss why below, but also responds to the perceived risk of a floodgates argument. These are not powers that when enacted have lead to complaints flooding in and disrupting the work of a regulator, they are a much smaller number in practice.

Q4. Do you think children's rights organisations should be permitted to bring claims on behalf of children in the same way as relevant non-profit organisations are able to currently? Please explain.

Open Rights Group are supportive of allowing appropriate organisations to take actions under Article 80(2) / section 188. The framing of this question suggests that children's rights organisations would not be a relevant not-for-profit organisation in the current formulation. Article 80 can clearly accommodate appropriate children's rights organisations in its current scope Open Rights Group feels it would not be necessary to create additional or separate permission standards and avoid creating confusion.

There is nothing in the adoption of Article 80.2 that would preclude children's rights organisations from bringing claims. The terms of Article 80 set out conditions that an organisation has to satisfy that the UK has adopted into 2 conditions set out in section 187 of the Data Protection Act 2018:

> The first condition is that the body or organisation, by virtue of its constitution or an enactment—
>
> (a) is required (after payment of outgoings) to apply the whole of its income and any capital it expends for charitable or public purposes,

2
Fundamental Rights Agency - GDPR One Year On, June 2019, pg 13, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-gdpr-one-year-on_en.pdf.

(b) is prohibited from directly or indirectly distributing amongst its members any part of its assets (otherwise than for charitable or public purposes), and

(c) has objectives which are in the public interest.

The second condition is that the body or organisation is active in the field of protection of data subjects' rights and freedoms with regard to the protection of their personal data.

These conditions are sensible and proportionate, ensuring that claims are brought by groups that are in the public interest and are likely to address key concerns regarding data protection. It would protect against any remote risk of floodgates or vexatious or spurious claims coming forward. Importantly, these conditions do not prevent a childrens' rights organisations from taking an action, it merely requires them to demonstrate those appropriate conditions are in place.

Questions for non-profit organisations who have represented individuals

Our organisation is yet to launch a formal complaint to the ICO or represent individuals in courts but we feel it important to note that we are in the process of preparing for such a complaint and to give some understanding of the sort of resource investment that goes into these actions. We will not refer to the facts but speak more generally about the activities and investments, financially and strategically, that are required in representing individuals.

Firstly, Open Rights Group does not provide a service to act on behalf of individuals. A service implies that regardless of the type of grievance an individual has Open Rights Group would seek to represent them. We would only consider taking actions that are in our strategic interest considering our purpose as an organisation and that we can handle the resource burden that comes from establishing such claims.

In the current example we have been working with a group of data subjects since June this year to challenge what we consider a breach of their rights under the Data Protection Act 2018. This has included:

- Liaising with the data subjects, explaining to them the case , their rights and their options for challenging the disputed practice.
- Seeking instructions from the data subjects and their authority to act on their behalf.
- Discussions with the data controller around the alleged breach, seeking to establish the facts and the reasoning behind the decision taken by the data controller.
- Discussing those responses with the data subjects to get their perception of the issue and collect further evidence if necessary.
- Return to the data controller with that further information and seek to engage in further deliberations.
- Throughout this time we are drafting of potential lines of inquiry and complaint to discuss internally and with the data subjects, including the evidence gathered, the law at issue, the facts of each data subject and the response of the data controller, drawing that to an argument as to whether or not a breach had occurred.

This process has taken at least 3 members of staff to progress this work and is currently still in discussion 4 months after the potential infringement. It has required a significant amount of staff time investment into the work for which we sought funding from other sources to ensure financial stability, not from the data subjects. This is not easy nor light work, it requires careful and considerable work to establish the facts and push things forward. This perhaps explains the somewhat low take-up of representative actions in that relevant organisations would take their responsibility regarding establishing a breach of data protection law seriously.

Lack of take up of representative provisions and how to improve their effectiveness

Other factors that may have caused these provisions to not be as effective are that individuals are not aware of such provisions to allow for an organisation to represent their interests. This could be seen with the reported low level of awareness of the ICO in the United Kingdom in comparison to other Member States[3] despite a high awareness of rights within the UK relative to Member States of the European Union[4]. This is something worth exploring, with a high degree of recognition of the GDPR and the rights within it, but a lack of knowledge of the institutions empowered to enforce, could explain some of the lack of take up of representative actions.

Options to improve this could include:

- A central repository of organisations that would be willing to discuss representative actions available both via the ICO but also through Citizen's Advice or other forms of dispute support websites.
- A space on the ICO's site dedicated to representative actions and how they operate, which could include the above register of organisations, but more generally seeks to inform individuals.

This is similar to the proposals set out by the European Commission's Directive on representative actions where "qualified entities" designated by the Member States are placed in a publicly available list.[5] If this initiative were to go ahead we stress that this is a communication of the existing powers, and not something requiring additional law or additional conditions for organisations to satisfy. If the central repository were to be created the presence or absence of an organisation of that

---

3
Figure 11, Fundamental Rights Agency, Your Rights Matter: Data Protection and Privacy, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-fundamental-rights-survey-data-protection-privacy_en.pdf.

4
Ibid Figure 10.

5
Article 4(1), Qualified Entities, Directive on representative actions for the protection of the collective interests of consumers, https://eur-lex.europa.eu/resource.html?uri=cellar:adba9e47-3e34-11e8-b5fe-01aa75ed71a1.0001.02/DOC_1&format=PDF.

repository should not determine their legitimacy to take an action under those powers.

Q12. Do you think the data protection legislation should be changed to allow non-profit organisations to act on behalf of individuals who have not given express authorisation? Please explain whether and why to permit such action in relation to the exercise of some or all of a data subject's rights.

Open Rights Group are very supportive of the reform to data protection legislation to allow for organisations to take complaints independently of a data subjects mandate. Significant aspects of data protection law are not enforced because the UK currently lacks a more complete suite of enforcement options in the space.

At present, a data subject is always required in order to bring a claim or complaint to a supervisory authority. Indeed, the operation of data protection legislation is demanding of a data subject. Whether through direct action or under s 187 DPA, a data subject will have to be named and engaged. In practice, a data subject is not always identifiable nor willing to bring action to address even the most egregious conduct.

Two key areas that give good reason for allowing organisations to take complaints independently of a data subjects mandate:

- Where processing represents a systemic breach of data protection standards
- Where processing is of a sensitive or taboo nature.

There are leading examples in both of these areas that illustrate the need for a power such as 80(2) to be brought in.

Where processing represents a systemic breach

Data processing is a deeply complex system, one which has much more activity going on behind the scenes than on the user facing side, sometimes referred to as invisible processing or dark patterns. This makes it difficult for the scale of a

systemic problem to be identified by an individual, let alone as something actionable as a complaint.

One leading example of such a problem is online advertising, in particular Real Time Bidding. Real Time Bidding is a set of technologies and practices used in programmatic advertising. It operates a real-time auction for advertisers to present an advert to an individual user when they land on a web page. To do this the user's information is collected and used to create a bid request, that is then put to auction and bidding from hundreds of thousands of companies, all of this takes place in a matter of milliseconds.[6] Bid requests can contain information relating to processing of special category data of individuals such as information relating to Mental Health, Ethnic and Identity Groups, Politics.[7]It raises problems of transparency, security, and appropriate legal basis for operation.[8]

The form of advertising is used in Google's Authorized Buyers service and is prevalent across the internet Adtech ecosystem. This form of advertising has brought the attention of the ICO which described it as a systemic problem[9], containing practices that they agreed were unlawful.[10] Yet to date no enforcement action has been taken. Where complaints have been raised they have come from activists and experts in this space, which have had to prove that they have been harmed or are involved in the bidding process, despite the practice of Real Time Bidding operating

---

6
For further information see Google, Authorized Buyers Overview: This all happens within 100 milliseconds, or in real time.' Available at https://support.google.com/authorizedbuyers/answer/6138000 or Lukasz Olejnik and Claude Castellucia, To bid or not to bid? Measuring the value of privacy in RTB, https://lukaszolejnik.com/rtb2.pdf.

7
For further information see pg. 13 of the Information Commissioner's Office Update report into adtech and real time bidding, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.

8
ibid, page 15.

9
Adtech - the reform of real time bidding has started and will continue, Information Commissioner's Office, 17 January 2020, https://ico.org.uk/about-the-ico/news-and-events/blog-adtech-the-reform-of-real-time-bidding-has-started/ .

10
Adtech and the data protection debate – where next?, Information Commissioner's Office, 20 December 2019, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/12/adtech-and-the-data-protection-debate-where-next/.

on many websites that all of us visit everyday, hence the systemic nature of the issue.

This particular state of affairs would have directly benefited from an 80(2) type action. This issue is not related to one data subject's experience but is a function of a core part of advertising ecosystem online, treating it as one data subjects grievance is a poor reflection of the issue and would be much better served in an 80(2) action.

Having such a measure available in the United Kingdom would have allowed for an appropriate organisation to raise the concerns regarding the systemic breach that Real Time Bidding presents. This would have formally engaged the Information Commissioner's Office in their regulatory responsibility including enforcement, and the responsibility to keep the complainants updated about the progress of the complaint. Instead the ICO has adopted a sectoral fact finding approach that has given them arguably too much discretion on the progress of the issues evidenced by their decision to pause their investigations as they did in May this year.[11]

There are other forms of law where complaints have been raised by organisations regrading systemic problems that affect consumers that are too complex or difficult for a consumer to notice which have provided huge benefits to consumers. The leading example would be the mis-selling of Payment Protection Insurance which was raised by the Citizen's Advice Bureau raised in 2005[12] under super-complaint powers in the Enterprise Act 2002. This issue lead to one of the longest running consumer rights investigations, and remedies, that the UK has ever seen. It perhaps would not have occurred without the ability for a designated organisation to engage the regulator in their responsibility through the super-complaint function because the scale of the problem was not immediately clear from the perspective of one consumer. It is also worth noting that the super-complaint power has been used sparingly by the organisations concerned, only as a last resort where particularly

11
ICO statement on Adtech work, 7 May 2020,
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/05/ico-statement-on-adtech-work/.

12
Banks face inquiry over credit insurance 'racket', The Guardian, 13 September 2005
https://www.theguardian.com/money/2005/sep/13/debt.business.

systemic problems have been identified. Open Rights Group considers it likely that a similar situation in data protection law would be seen, where the powers would be viewed as a strategic last resort when other actions have already been attempted.

Where processing is sensitive or taboo

We spend a great deal of our lives online now, the current situation with a global pandemic. This means that more of us will be living sensitive parts of our private lives online, such as accessing mental health websites. The organisation Privacy International found in September 2019 that such websites were allowing third party advertisers and trackers to track users of mental health websites, information which is subsequently used in advertising.[13] This occurred before a user was able to accept or reject the consent to allow for processing, a clear breach of GDPR standards.

However unsurprisingly no individual mandated Privacy International to take that complaint to a supervisory authority. This is likely because of the stigma attached to mental health It would take a brave person to step forward and mandate an organisation to exercise their rights on their behalf. If 80(2) were available a complaint could be raised by an appropriate organisation that this systemic and sensitive issue is occuring and bring it to the attention of the ICO or a judicial authority without the individual having to lose their anonymity or confidentiality to take the case on.

This could be a very powerful development for challenging those practices that are sensitive or taboo but merit the challenge. Relying on an individual to mandate an organisation is unlikely to occur in these sensitive areas of data processing meaning enforcement is less likely to occur. Instead empowering individual organisations to take claims as a systemic problem, not identifying any specific data subject, instead a systemic abuse in a taboo or sensitive area of data processing is a positive development for securing the effective and complete protection of data subjects and making the UK a safer place to be online.

13
Your mental health for sale, Privacy International, 2 September 2019, https://privacyinternational.org/news-analysis/3188/taking-depression-test-online-go-ahead-theyre-listening.

Q13. Should a children's rights organisation be permitted to exercise some or all of a data subject's rights on behalf of a child, with or without being authorised to do so? Please explain

Yes. Rights are only meaningful if they can be exercised. Children are inherently less able to exercise their legal rights than adults and require support to do this. Recital 38 of the GDPR acknowledges that children merit specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.

Children's rights organisations are well placed to offer this support but we see no reason why the current conditions set out in section 187 would prevent appropriate children's rights organisations from taking complaints forward and making complaints in relation to the processing of a child's data. We believe that the current criteria set out in section 187 are not an insurmountable hurdle for children's rights organisations to take forward and would query why the framing of the question would suggest that a separate and additional measure should be created for children's rights organisations.

Q14. What, if any, impact might allowing non-profit organisations to act on behalf of individuals who have not authorised them to do so have an impact on people who identify with the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)?

Article 80(2) cases should be concerned with infringements of the data protection regulations, rather than relating to specific individuals. As such, the impact on individuals would be negated. The individual data subject need not be named or identified, or any protected characteristic revealed; the infringement is the only concern.

If Article 80(2) were to operate in this way, it would address one of the main limiting factors associated with Article 80(1) - that individual data subjects may fear exposure or retaliation if they are named. As we set out above, processing of personal data in

sensitive or taboo areas may not be challenged because an individual is reluctant to be named or identified with an action because of the reaction to their use of a service. This is an understandable concern for an individual, and one that can be set aside if 80(2) powers were in place.

There is evidence that those with vulnerabilities can experience additional obstacles when it comes to exercising their data rights compared with the general population. The Fundamental Rights Agency have detailed how individuals belonging to vulnerable groups may face structural problems such as lack of financial resources, inadequate level of legal literacy and empowerment in exercising access to justice in general.[14] Recent revelations regarding online advertising technology targeting of LGBTQ+ people during the Polish Parliamentary Election and profiling of Black Lives Matters protestors shows how protected characteristics can be abused by third parties in data processing.[15]

Ultimately we see a benefit for communities or individuals that identify with protected characteristics as it would not require the significant investment of time or the step of putting themselves forward as a data subject to centre a complaint around.

Q15. What safeguards, if any, should operate to avoid the speculative or vexatious use of any new powers for non-profit organisations to act without the consent of individuals and avoid a disproportionate administrative burden on either the regulatory or courts systems?

There are safeguards already built into the Article 80 conditionst that organsations must satisfy; potential organisations involved will have internal restrictions that will

14
See Fundamental Rights Agency, Handbook on European Law Relating to Access to Justice (Luxembourg: Publications Office of the European Union ,2016
https://fra.europa.eu/en/publication/2016/handbook-european-law-relating-access-justice
and Fundamental Rights Agency, "Access to Data Protection Remedies in the EU Member States" (Luxembourg: PublicationsOfficeoftheEuropeanUnion,2013) for specific reference to the data protection field.
https://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states

15
According to a report dated 21 September 2020 by Dr Johnny Ryan, Senior Fellow of the Irish Council of Civil Liberties (ICCL). Report available here:
https://fra.europa.eu/sites/default/files/fra_uploads/fra-ecthr-2016-handbook-on-access-to-justice_en.pdf .

act as a safeguard; and further there are safeguards within the regulatory and court system. We are unsure there is a need for further safeguards but the Secretary of State has discretion to establish further procedural rules. These first two safeguards could explain why there are relatively low uptake of representative provisions.

Despite the risk of a floodgate of complaints when the current representative provisions were being debated in Parliament, this did not materialise. It should be noted that the Information Commissioner's Office expressed support for 80.2 of GDPR at the time of the Data Protection Bill passing through Parliament and expressed no reservations in that support about administrative burdens if the power were to be enacted.[16]

Firstly, Article 80(2) establishes conditions an organisation must satisfy to be in a position to take an action. These conditions are already established in section 187 DPA and discussed above, that an organisation must be a not for profit with objectives in the public interest, and active in the field of data protection. This will provide some restrictions in restricting complaints. It would be self-defeating for such organisations to create an administrative burden by flooding complaints into the supervisory authority and court system and thus undermine the legitimacy of the representative provisions.

Secondly, the non-profit organisations that would satisfy conditions have limited resources which will impact how many claims they can reasonably bring or indeed, whether bring claims at all. As we detail above as a not for profit active in the field of data protection we take our responsibility seriously. We seek to establish complaints that meet our strategic goals, and that the complaints have merit by investing resources into evidence gathering and discussion with the parties involved. This is a time consuming process that requires us to direct limited staff resources and time. It is likely that as a result claims that appear speculative or vexatious would be rejected as it would risk our reputation, be a waste of resources, and ultimately fail to achieve our strategic objectives of effective enforcement of data protection law.

16
Data Protection Bill, House of Lords second reading, Information Commissioner's briefing, https://ico.org.uk/media/about-the-ico/documents/2172484/dp-bill-commissioner-briefing-lords-second-reading.pdf

Thirdly, courts and regulatory systems are well-developed and well-versed in dealing with speculative and vexatious complaints in other contexts. Any vexatious claims in court are likely to be struck out. The Information Commissioner has discretion to determine whether to pursue a complaint and further investigate. Under section 165(4)(a) the Commissioner has responsibility to take appropriate steps to respond to the complaint which amounts to investigation the complaint "to the extent appropriate"[17] and "informing he complainant about the process on the complaint, including about whether further investigation... is necessary".[18] This gives the Commissioner a good deal of discretion to deem a complaint vexatious or speculative and dismiss it as not requiring further investigation without suffering a disproportionate burden.

All of these factors taken together it is unlikely that establishing an Article 80(2) mechanism in the United Kingdom would create a disproportionate burden on either the regulatory or courts systems.

If there were to be measures necessary, under section 188(1) DPA 2018 the Secretary of State "may by regulations make provision for representative bodies to bring proceedings before a court or tribunal." This includes the power to make "provisions about proceedings", which encompasses:

(a) the effect of judgments and orders;

(b) agreements to settle claims;

(c) the assessment of the amount of compensation;

(d) the persons to whom compensation may or must be paid, including compensation not claimed by the data subject;

(e) costs.

17
section 165(4), Data Protection Act 2018.

18
section 165(5), Data Protection Act 2018.

However we remain unconvinced of the necessity of further safeguards given the safeguards already in place and if they were deemed necessary, we encourage careful consideration regarding how such a process would be structured.

Q16. What conditions, limitations or safeguards should apply if non-profit organisations act on behalf of individuals who have not authorised them to do so? For example, should individuals be given the right to object to a non-profit organisation taking action on their behalf without their consent? Please explain.

It is not clear that a data subject needs to be named or identified under Article 80(2) GDPR for the provision to be effective. Rather, Article 80(2) operates on a macro basis, where the organisation considers that infringements of rights have occurred. Further, organisations are unlikely to be acting contrary to the interests of data subjects in these cases, as any cases would relate to the infringement that a data has been subject to. Such a claim would therefore be consistent with both the organisation''s mandate and wider public interest goals, as well as the interests of the data subject to remedy infringements of the data protection regulations.

Were a data subject to be named as part of a complaint or action under Article 80(2), that data subject could be afforded the right to object to / opt out of that complaint or action. Should the need to name the data subject arise there would need to be an initial right to opt-out at the point at which the data subject may be named and an ongoing right to opt-out as data subjects may not be aware of a complaint / action until after the action has commenced, or developments along the way could cause an individual to change their mind. However this would only be required if the organisation were seeking to name or identify the data subject, which would not be necessary or consistent with the purpose of the 80(2) regime or the wording of Article 80(2).

Q17. If the new provisions discussed in this chapter were adopted, what impacts do you anticipate on data controllers which might be the subject of a complaint or legal claim, particularly businesses, including any increased costs or risks?

"Floodgates" arguments are misplaced. Similar fears were raised in an Article 80(1) GDPR context and have not materialised. It is also worth noting that the Information Commissioner's Office did not express any concerns about increased costs or risks when they expressed support for the provisions to be adopted during the Bill debates.[19] Further there are factors that already limit the uptake of representative provisions, like the conditions an organisation must satisfy, which should continue to apply in 80(2) actions, and wider environmental factors for not-for-profit organisations such as:

- Restrictions through our own mandates an resources.
- The time required to find the infringement, build a case and then potentially have the matter litigated.
- The UK costs regime in CPR 44, with a "loser pays" principle at its heart, poses a significant barrier to not for profit organisations bringing cases forward.
- Organisations cannot claim damages in their own right under Article 80(2) as Recital 142 of the GDPR sets out.

In sum, an organisation will need to be extremely motivated to bring an Article 80(2) action and such actions will be reserved for exceptional cases only. This view is seen by the current uptake of representative provisions.

There may be benefits for controllers in the proper introduction of Article 80(2) actions, as controllers will have issues dealt with on the basis of a single targeted complaint, which will be considered and well-articulated in contrast to scattergun and inconsistent actions by data subjects. This would limit the controller's exposure and reduce costs (as compared to a situation where it finds itself at the other end of hundreds of claims).

19
See footnote 14.

Finally, note that to date Article 80(1) / section 187 has proven incapable of providing sufficient protection by itself - recalling arguments set out above about systemic data protection infringements and taboo areas of processing - and thus Article 80(2) fills a gap by overcoming those limiting factors that have resulted in the lack of actions under 80(1) so far.

Q18. If the new provisions discussed in this chapter were adopted, what are the likely impacts on the ICO or the judicial system, which will be required to consider representations made by non-profit organisations? What is their capacity to handle new claims brought under any new provisions, and how might the design of any new provisions help to manage pressures?

Due to the limitations of who can bring Article 80(2) actions, there is unlikely to be a huge increase in the number of actions brought before the courts or ICO. On the contrary, the same benefits set out above could be seen in the ICO, namely single, targeted, well-articulated complaints from appropriate organisations, These complaints may represent hundreds of thousands of individuals processing, which would potentially have been brought by those individuals creating a large resource burden for the ICO and courts. Article 80(2) could prove to be a cost saving measure and help manage some of the pressure that the ICO and other DPAs already face in resourcing and clearing backlogs of complaints.[20] Furthermore, the ICO has discretion as to which cases to take on and has currently deployed a very restrictive approach to enforcement.

As well as helping to change practices, setting precedents in Article 80(2) cases would also encourage future settlements, making these issues less likely to be litigated through courts for compensation in the future.

20
GDPR's two-year review flags lack of 'vigorous' enforcement, Tech Crunch, 24 June 2020, https://techcrunch.com/2020/06/24/gdprs-two-year-review-flags-lack-of-vigorous-enforcement/

Finally, it should be noted that the ICO has never publicly raised concerns about their capacity to handle new claims brought under 80(2), and where they have had the opportunity to comment on the provision have given unqualified support for it.[21]

Q19. What are the alternative means or mechanisms by which non-profit organisations are currently able to bring complaints to the ICO or to court using existing Civil Procedure Rules? Please provide any evidence of their use or operation to date.

The procedures under CPR 19 envisage compensatory claims brought on behalf of a group of similarly effected individuals, although they can extend to other forms of action.

Under the CPR 19, there are two main mechanisms for bringing collective actions. One is the group litigation order (or GLO) which occurs on an "opt-in" basis. GLOs provide for claims giving rise to common or related issues of fact or law to be heard together. However, this mechanism would not appear available to a non-profit unless it was itself a claimant in the action.[22] As a result it is a poor alternative for a non-profit organisation to bring complaints to the ICO. The claim will also require a court to direct management of the claim.

Additionally, there is provision for a representative action procedure under CPR 19.6.Under CPR 19.6 the court may direct that where more than one person has the "same interest" in a claim, that claim may be begun or continued by one or more of those persons as representatives of any other person who has that interest. The scope of such actions will likely be determined by the Supreme Court in *Lloyd v Google* (on appeal from the Court of appeal judgment [2019] EWCA Civ 1599[23]). However, there are a few features that are pertinent:

21
see footnote 14.

22
Practice Direction 19B, Group Litigation,
https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part19/pd_part19b

23

Lloyd v. Google, [2019] EWCA Civ 1599 https://www.bailii.org/ew/cases/EWCA/Civ/2019/1599.html

- The "person" who is representing others could be a legal person such as a non-profit organisation.
- The rules require the "person" to have the "same interest". This is difficult to apply in a data protection context, as the non-profit is unlikely to have the same interest as the data subject.

The requirement for a "same interest" to be shared, would likely negate CPR 19 being used in the same way as an Article 80(2) GDPR case. We do not consider CPR 19 to be an adequate alternative remedy to Article 80(2) proceedings.[24] The CPR procedure is qualitatively different to the Article 80(2) procedure and pursues different ends. CPR 19.6 requires a person who is representative of a wider group interest. Under Article 80(2), the requirement for a shared interest does not need to exist. Instead, an organisation can pursue systemic infringements in the absence of identifying data subjects or sharing their interest in the case. This is an essential point of Article 80(2) and serves to ensure the "effective and complete" protection of data subjects. The current CPR procedures are thus inadequate to address the type of cases which Article 80(2) aims to address.

It is also worth reflecting on some of the earlier limiting factors for taking representative actions, namely resource. These apply and are even exacerbated by the CPR provisions. In CPR the "loser pays" principle means that there is an enormous cost barrier to challenging practices of large companies that will inevitably bring expensive legal representation to any alleged breach. It is for this reason that Richard Lloyd's claim against Google is relying on a 'third party funder' to meet the legal proceedings costs.[25] These third party funders are essential for supporting representative actions because of the costs but only get involved in cases in return for a share of the damages awarded. There is more to data protection enforcement

24
There are concerns that Article 80(1) actions would have to meet the same strict criteria under CPR 19 where claims for damages are brought. This is a further justification for introducing Article 80(2). See Bird & Bird, 'The 'Tidal wave' of data protection-related class actions: Why we're not drowning just yet...' (November 2018) https://www.twobirds.com/en/news/articles/2018/global/tidal-wave-of-data-protection-related-cases.

25
Google: You Owe Us, FAQ, What will it cost me?
https://www.youoweus.co.uk/faqs/

than seeking damages but the CPR rules, because of their resource burden, create an incentive to seek damages against other enforcement measures so as to have a chance of securing sufficient resource.

Q20. In what ways would the potential measures outlined in Chapter 3 either complement or duplicate these alternative mechanisms?

There is yet to be any significant uptake of actions under the Article 80(1) provisions for various reasons. For instance,a data subject may not even be aware of their rights under GDPR or that they have been infringed. Even if they do have this knowledge, they might find it hard to show that they have been directly affected. More importantly, a data subject may also be unwilling to act due to the risks involved.

Furthermore, there is a practical impediment to the uptake of Article 80(1). The procedure in Article 80(1) GPDR / s.187 DPA is akin to a data subject instructing a lawyer to act on their behalf. The mandate must be clear and for the enforcement of identified data subjects' rights. Organisations are unlikely to want to take such a position of acting on express and limited mandates, where such mandates may be in tension with their need to be independent.

CPR 19 actions are mainly intended for compensation claims and organisations are unlikely to be able to use the CPR procedures as they are unlikely to have a common interest in the case, such to create a GLO or a representative action of a wider group interest. In contrast, in Article 80(2) actions the requirement for a shared interest does not need to exist. Rather, the focus is to allow a non-profit to pursue infringements in the absence of identifying data subjects or sharing their interest in the case. This is the essential point of Article 80(2). The current CPR procedures are thus inadequate to address the type of cases which Article 80(2) seeks to respond to.

Article 80(2) actions do not incorporate the right to receive compensation for the not for profits, Recital 142[26] expressly seeks to restricts this, and we agree with this position. It removes the incentives for an action to be motivated by a potential pay day

26
General Data Protection Regulation, Recital 142,
https://gdpr.algolia.com/gdpr-article-80#recital-142.

and focuses the attention on the changes that should be taken to rectify the practice and provide the effective and complete protection of personal data.

Article 80(2) and representative actions are qualitatively different and provide a different set of incentives and options. They are alternatives and there are some overlaps but there are distinct differences on outcome and procedure that we think means these options can exist in the same system and provide a stronger suite of enforcement options. Ultimately these measures create the outcome of improving fairness, transparency and trust in the data economy in the United Kingdom, an express goal of the current National Data Strategy.[27]

27
National Data Strategy, 7.1 A pro-growth data rights regime, 7.1.2. Fairness, transparency and trust, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy#data-7-1