Response to DCMS Review of Representative Action Provisions, Section 189 Data Protection Act 2018

5Rights Foundation
October 2020

Introduction

We are grateful for the opportunity to provide views and evidence in response to this consultation.

5Rights Foundation speaks specifically on behalf of and is informed by the views of young people. Therefore, our comments reflect, and are restricted to, how the Data Protection Act should protect users under the age of 18. However, we recognise that many of our approaches are relevant to other user groups and we welcome any efforts that government makes to make the digital world more equitable for all user groups, particularly the vulnerable.

In this consultation response, we call for Article 80(2) GDPR to be implemented to allow children's rights organisations to take action on users' behalf in response to systemic infringements of data protection law. This would allow the comprehensive protection that the Data Protection Act envisages to be realised for children who cannot be expected to navigate the current routes available.

Our response is based on our experience as a non-profit active in this field, the experiences of young people and advice from legal experts, academics and regulators. There is widespread agreement amongst these communities that the implementation of Article 80(2) in the UK is a necessary step for children.

We note that this consultation is formulated in a manner that makes it very difficult for many groups of people to reasonably understand or respond effectively, particularly parents, teachers and children themselves – the very people with whom the Government is required to consult under s189(5) of the Data Protection Act.

About 5Rights Foundation

5Rights Foundation develops new policy, creates innovative projects and challenges received narratives to ensure governments, regulators, the tech sector and society understand, recognise and prioritise children's needs and rights in the digital world. In all of our work, we maintain and advocate that a child or a young person is anyone under the age of 18, in line with the UN Convention on the Rights of the Child.

Our work is pragmatic and implementable, allowing us to work with governments, intergovernmental institutions, professional associations, academics, and young people across the globe to build the digital world that young people deserve.

Responses to Consultation Questions

1. **Are you responding to this consultation as:**
- a. An individual
- b. A private sector business/organisation
- c. A public sector organisation
- d. A third sector organisation, (e.g. charity, social enterprise)
- e. Other (e.g. informal group, other organisation)

We are responding to this consultation as a third sector organisation—specifically, a non-profit organisation, active in the field of data protection and dedicated to young people's rights online.

2. **What is your view on the uptake and operation of representative action provisions to date and what can be done to improve it?**

The existing representative action provisions under Article 80(1) GDPR and section 187 DPA —by which an individual can request that a non-profit organisation act on their behalf in relation to making a complaint to the ICO or bringing an action against a decision of the ICO or against an organisation that has breached data protection law are ineffective and overly restrictive.

Most individuals will not identify injury to themselves from their exposure to the modern data economy. Even if they do, they are unlikely to recognise the actual or potential seriousness of such injury.

Existing representative action provisions only allow non-profits to act as representatives for individuals or groups of individuals who have actively requested such representation. The apparent innocuousness and or opaque nature of exposure makes it unfeasible for non-profits to identify and assemble a large enough group of affected individuals to run complex, protracted, and thus expensive claims against infringing corporations.

Existing representative action provisions thus appear ineffective in enabling access to justice in the case of systemic infringements of data protection law arising out of organisations' business models. This can be resolved by the UK's adoption of GDPR Article 80(2) permitting non-profits to bring representative actions on behalf of individuals without their specific authorisation, which will specifically cater for systemic infringements of data protection law.

3. What, if any, impact might these representative action provisions have had 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)?

The difficulty of understanding or accessing justice makes it unlikely that young people with these characteristics will be able to protect themselves or take action on their own behalf. As noted in our response to Question 14, the introduction of Article 80(2) in UK law would have a positive impact on young people with protected characteristics.

4. 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?

Yes. Users who are under 18 suffer significant additional infringements but are at a stage of life when they could not reasonably be expected to act on their own behalf. Children's rights non-profit organisations should be allowed to bring claims on behalf of children. Our reasoning is presented in our responses to Q15 and Q16.

5. Questions 5-8 are Questions for non-profit organisations who have represented individuals, which does not apply to 5Rights.

9. Question 9 is for individuals who have been represented by non-profit organisations, which does not apply to 5Rights.

10. What, if any, impacts might the provisions discussed in Chapter 2 have had on data controllers which might be the subject of a complaint or legal claim, particularly businesses, including any increase to compliance and other costs, or risks?

We are not aware of any significant impact on data controllers from the current representative action provisions. We note that there has been no 'opening of the floodgates' to frivolous or nuisance vexatious actions under Article 80(1) GDPR despite initial fears this would occur.

What, if any, impacts might the current provisions have had on the ICO and the judicial system and their capacity to handle claims? What, if any, measures might help to manage pressures?

We are not aware of any significant impact on the ICO and the judicial system from the current representative action provisions. We note that there has been no 'opening of the floodgates' to frivolous or nuisance vexatious actions under Article 80(1) GDPR.

11. 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.

Yes. The data protection legislation should be changed to allow non-profit organisations to act on behalf of young people and who have not given express authorisation.

The purpose of the GDPR and its implementation through the Data Protection Act 2018 (DPA) is to ensure the "effective and complete" protection of data subjects from illegal and unfair processing.1 But the current regime relies on data subjects to assert their rights, both to the ICO and ultimately the courts. It requires them to understand that there has been a breach of their rights, and to have the technical knowledge to understand the implications and the harms arising from the breach, the motivation to take action, the time to pursue a claim, and the money to pay for it.

This is an impossibly high bar for young people and others with vulnerabilities.

The wording of this question suggests that the operation of Article 80(2) GDPR would enable a non-profit organisation to act against the express authority or wishes of a data subject. This is not the case.

Article 80(2) allows appropriately constituted organisations to bring proceedings concerning infringements of the data protection regulations in the absence of a data subject. Thus, the Regulation is designed to ensure that proceedings may be brought in response to an infringement rather than on the specific facts of an individual's case.

It is likely that data infringements will be systemic in nature, and affect groups or categories of users, enabling non-profits to represent these groups will offer greater numbers of data subjects more effective protection of their rights. This is particularly important given the technical complexity and opaque nature of data processing, and the vast array of data subjects, some of who have vulnerabilities and/or lack of skills and knowledge in this area,

Article 80(2) addresses infringements of the rights of data subjects at the macro level. In turn, those actions can address systemic infringements that arise by design, rather than requiring an individual to evidence the breaches and the specific damage to them, which they may not even be aware of.

Example: A child who accesses mental health support services has considerable rights over their data, derived from their status as a child, but which also arise from the nature of the data they have shared, and what is inferred from their engagement. However, as has been identified repeatedly in similar circumstances, data has been shared, sold or the child's profile made available to commercial companies, including cosmetic surgery businesses and advertisers of high salt/fat foods.

[1] The "effective and complete protection" formulation was first used in the *Google Spain* judgment (Case C-131/12 Google Spain SL, Google Inc v Agencia Española de Protección de Datos and Mario Costeja González [2014] ECLI:EU:C:2014:317) and since in the judgments such as *Weltimmo, Schrems, Wirtschaftsakademie* and *Jehovan todistajat*.

These children have unknowingly suffered an infringement, in that an organisation has used and profiled their vulnerable mental state – *for which they were actively seeking support* – to sell services that prey on their low self-esteem without their knowledge or consent.

Why is Article 80(2) needed

Article 80(2) was deliberately designed to ensure the reach of data protection legislation would provide "effective and complete" protection to data subjects. Particularly for those who are least able to access justice for themselves. Current legislation has been shown to be ineffective precisely because Article 80(2) GDPR has not been brought into domestic law.[2]

During the passage of the Data Protection Act, government ministers repeatedly gave a commitment to young people and parents that the protections under the DPA and the Children's Code would be sufficient to adequately protect them. They accepted the argument that young people could not be expected to undertake action on their own behalf, and they deliberately allowed for this review to consider children as a separate user group. The introduction of 80(2) is required to ensure that commitment is fulfilled.

Flaws in the s187 procedure

At present, a 'named' data subject is always required in order to bring a claim or complaint to a supervisory authority. Whether through direct action or under s187 DPA (Representation of data subjects with their authority), a data subject will have to be named and engaged. This requires a data subject to understand and identify motivated by an infringement of the data protection regulations. In practice, the s187 process is not dissimilar to a data subject bringing such claims in their own name. The data subject would also have to engage an appropriate non-profit organisation, who is ready, able and committed to bring such an action.

However, a data subject is not always identifiable, may not know (or find it hard to evidence) that they have been directly affected by the unlawful processing, or may find it hard to bring action to address even the most egregious conduct. Nor are the vast majority of UK data subjects – particularly children - in a position to identify an NGO with this expertise. This is the gap that 80(2) is intended to fill.

Even a motivated data subject may be unwilling to take action due to the risks involved. For instance, it is reasonable for data subjects to not want to become involved in a lengthy and costly legal process. This is particularly pressing where the infringement concerns systemic concerns rather than where an individual has suffered material or non-material damage as a result of the infringement.

[2] Data and Democracy in the Digital Age, *Hankey et al*, The Constitution Society, July 2018; and Political campaigning – the law, the gaps and the way forward, *Naik et al*, Oxford University, October 2019.

Example: a young person may not wish to pursue cases where they have been involved with material or activities that are exposing. It may not feel 'worth it' to pursue a global company even if they routinely ask or take data that is not in line with data minimisation principles. Each individual infringement may be small but over a childhood may seriously impact on a child's life.

And, in the case of systemic failure to uphold age limits or providing detrimental material, individual cases slowly going through a court system is neither efficient, sufficiently urgent nor in the spirit of the law

How Article 80(2) could assist

Introducing Article 80(2) would help to realise the change in data protection practices that GDPR envisaged (and promised) for young people and other vulnerable groups. Crucially it would enable non-profits to take representative action based on breaches of the law that have systemic impacts. Non-profit organisations active in the data protection field have built up the considerable technical capacity needed to understand the nature of these infringements which will allow them to bring these actions more effectively.

Example: There is wide-spread concern that the ICO has been unable to act in the area of Advertising Technology (AdTech). Specifically, the current limit to such action is identifying a data subject who has suffered sufficient harm and the difficulty for ICO in seeking such a subject – in spite of seeing a breach. Article 80(2) would remove that conflict and allow the courts to engage with the systemic issues that AdTech presents and many groups, including the Society of Editors and many parts of the advertising industry, would like to see.

Had Article 80(2) been implemented, a non-profit could have brought proceedings against the issues that have been brought to the ICO, without the need to identify a specific data subject.

12. 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. Young people are inherently less able to exercise their legal rights than adults and they are regularly given additional support to do so (for example as victims and witnesses in the court system and during child protection proceedings). Children's rights organisations are well placed to provide this support. Given the complexity of data protection legislation it is simply impossible to expect a child to act on their own behalf. Indeed, evidence from the Information Commissioner's

Office found that nearly all adults (who would be expected to have a better understanding than children) barely understand it.[3]

Position of children in the GDPR

Children are entitled to special protection for their personal data under the GDPR[4] as well as under the statutory Age Appropriate Design Code (also known as the Children's Code).[5] The Children's Code is a set of 15 standards that online services should meet to protect children's privacy. The Children's Code confirms that the best interests of the child should be a primary consideration when designing and developing online services. The standards are rooted in the GDPR which has many child-specific provisions, including that information notices addressed to children must be child-friendly.

Recital 38 GDPR says 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." Recital 75 GDPR adds that children are "vulnerable natural persons", and the EDPB guidance on DPIAs has previously observed that the processing of personal data of vulnerable persons – including children – is something that can contribute towards processing being high risk.

There is an inherent imbalance of power and information (sometimes referred to as "information asymmetry") whenever children are using devices that are designed not for them but for adult users. Children have limited capacity to understand the complexities associated with data processing and what they are signing up to. They have less experience and awareness of risks and rights and can be more easily exploited. In other words, children can be more prone to making unwise decisions online (sometimes referred to as "decisional vulnerability).[6]

Many online services make almost no effort to help children overcome these barriers. They set out their published terms and conditions in forms that are incomprehensible for a child and consequently those terms rarely read and poorly upheld.[7] They are presented at times and in ways that encourage agreement without engagement and take an implausible amount of time to read through.[8] As a result, children are understandably confused about their data rights and how to exercise them. According to ICO research conducted in advance of the Code, children described data practices as "nosy", "rude" and a "bit freaky".[9]

The Children's Code has garnered UK regulators and government significant accolades around the world, and is being considered as 'best practice' by other jurisdictions now wishing to offer similar protections for children.

During the passage of the Bill Ministers were sympathetic to the notion that children cannot access rights without support, and suggested that in all eventualities the Government would support introduction of 80(2) for children. It would further enhance the UK's reputation, and fulfil the promises made by government to parents and children to ensure they had expert redress under the law.

---

[3] In a survey for ICO it was found that just 8% of UK adults say they have a good understanding of how their personal data is made available to third parties and the public by companies and organisations in the UK, ICO survey shows most UK citizens don't trust organisations with their data, ICO, November 2017

[4] Recital 38 GDPR.

[5] Age appropriate design: a code of practice for online services, *ICO*, September 2020.

[6] See, for instance, Children's Data and Privacy Online, *Mariya Stoilova, Sonia Livingstone, and Rishita Nandagiri*, London School of Economics and Political Science, 2019.

[7] Most Online 'Terms of Service' Are Incomprehensible to Adults, *VICE News,* February 2019; We Read 150 Privacy Policies. They Were an Incomprehensible Disaster, *New York Times,* June 2019.

[8] Social Site Terms Tougher Than Dickens, *BBC News*, July 2018.

[9] Information Commissioner's foreword, Age appropriate design: a code of practice for online services, *ICO*.

Additionally, many children do not have 'engaged parents' with the skills and knowledge to support a data protection action either to regulator or court – indeed it is arguable that only a tiny minority of UK children have such parents. Data protection law in its current form is new, complex, and importantly there is little case law in the area.

How Article 80(2) could assist

There are specific difficulties when supporting young people to exercise their data rights. In particular, using the s187 procedure would likely require the public naming of the young person, and the permanent linking of their identity with the infringement. This is likely to have long-lasting impacts on their digital footprint, and will disincentivise many young people from pursuing action. It is important for government to note that some (not all) data breaches that involve children centre around issues and sensitivities that they may not wish to be public. For example, where they may have made payments, accessed explicit material, had protected characteristics such as sexuality or race exposed, or have a persistent and *erroneous* digital footprint. Childhood is a time of great sensitivity and being public for many young people is simply not an option.

Under s187, a young person would need to be able to understand and articulate the harms they have suffered as a result of the infringement, and be able to give their consent to the non-profit taking action. In most cases, parental consent would also be required which for the same reasons given above, may create its own barrier.

Both of these issues make it less likely that a complaint under s187 will progress and will result in lasting change to protections for young people's data. Both would be alleviated by the introduction of Article 80(2). Allowing a non-profit to challenge the infringements of the GDPR, would minimise the risk to children being involved in such action and the practical barriers.

Article 80(2) will ensure that infringements are brought to the attention of regulatory authorities and courts driving positive change. In turn, illegal practices will diminish and accountability will increase, which will result in an increase in effective and complete protection of data subjects' rights.

It is crucial to understand that data risks and infringements end in real world harms such as identity theft, making children's location visible to predators, profiling to make depressed children buy products or services– or profiling them to deliver content such as self-harm or promotion of suicide. When considering whether to implement Article 80(2), the Government must respond to the serious nature of the breaches and the lack of agency or action available to children – some who are still only 8 or 9 years old.

13. 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. The individual data subject need not been named or identified; the infringement is the only concern. Therefore, there should be no negative impact on individuals with protected characteristics.

However, implementing Article 80(2) would address one of the main limiting factors associated with both individual claims and those under s187 - that individual data subjects may not come forward because they fear exposure or retaliation if they are named in the complaint. For example, LGBTQ+ young people may be less willing to complain about the

illegal collection and processing of their data on a dating app, as the very fact that they have complained may out them, putting them at social and physical risk.

There is evidence that those with vulnerabilities can experience additional obstacles when it comes to exercising their data rights compared with the general population. Research suggests that this is due to numerous factors, including due to enhanced "information asymmetries."[10] The Fundamental Rights Agency (FRA) 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.[11] People with protected characteristics, and vulnerable populations, may also find themselves exposed to increased data protection harms. For example, the recent revelations regarding AdTech's targeting of LGBTQ+ people during the Polish Parliamentary Election and profiling of Black Lives Matters protestors[12] demonstrates the manner in which data can be used by third parties to exploit and profile individual data subjects.

The introduction of Article 80(2) would help to facilitate greater protection of those who identify with protected characteristics, including vulnerable persons, at the macro level, with positive effects that would then impact on the individual level. Those individuals would also be protected from having to be named in such proceedings.

14. 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?

It is not clear that any safeguards are needed. Fears that the introduction of such regulations would create a "floodgates" scenario is misplaced. Indeed, similar arguments were made in the s187 context[13] yet the predicted deluge of cases has not materialised. As the introduction to this consultation affirms, the "uptake of representative action provisions appears to be quite low."

However, it should be noted that safeguards already exist both within organisations and within the existing court and regulatory systems.

Existing organisational safeguards

Some practical barriers and safeguards already exist to ensure the cases being taken under Article 80(2) have merit. Many of these are inherent within the structures of non-profit organisations.

- An organisation has to meet two stringent qualifying criteria under s187 of the Data Protection Act (DPA). Firstly, s.187(3) requires the organisation to have certain features, including that it must be a non-profit and have objectives that are in the public interest. Secondly, s.187(4) DPA requires the organisation to be "active in the field of protecting data subjects' rights and freedoms with regard to the protection of their personal data". These criteria limit the number of bodies which can take

[10] Vulnerable data subjects, Malgieri, G. and Niklas, J., *Computer Law & Security Review*, 37, p.105415, July 2020.
[11] Ibid
[12] According to a report dated 21 September 2020 by Dr Johnny Ryan, Senior Fellow of the Irish Council of Civil Liberties (ICCL).
[13] See for instance, The "Tidal wave" of data protection-related class actions: Why we're not drowning just yet..., *Bird & Bird*, November 2018, which observes that *"prior to the GDPR's entry into force in May this year, much was being said about the "inevitable" deluge of class actions likely to flood the UK court system as a result."*

representative action in a s187 context and should also apply to any action under Article 80(2).

- Non-profits are restricted by their own limited resources, and their mandate or charitable objects. They are only likely to consider claims or other action in limited circumstances, where there is a particularly meritorious matter that would otherwise not be brought. This is a high internal barrier that will limit the use and abuse of the mechanism. Any prospect that non-profits would use scarce resources to bring speculative or spurious claims is remote.
- Fears that a non-profit may "go rogue" and bring complaints or actions that a data subject would be dissatisfied with are similarly unfounded. Enactment of Article 80(2) would not enable the organisation to seek monetary redress for themselves or a data subject but rather to test the legality of practices. Properly constituted bodies will only bring such issues to the regulator or court where they have identified an infringement, which is within their mandate to consider, and where no other actor is bringing the action.
- While a non-profit may be able to bring a compensation action, depending on how Article 80(2) is introduced, it will not receive that compensation itself. This ensures that there is no financial incentive for the non-profit to bring spurious claims, adding a further layer of protection.
- For any damages claim, Article 82 GDPR requires a person to show material or non-material damage in order to be eligible for compensation. Non-profit organisations would not be able to show such damage unless they were themselves the subject of an infringement. If that was the case, then they would be able to claim for damages in their own right without the need for an Article 80(2) process.
- Finally, the costs risks of bringing an action make cases and regulatory actions unlikely unless the non-profit is willing to take those costs risks. The costs regime in CPR 44, with a "loser pays" principle at its heart, poses a significant barrier to non-profits bringing cases forward. Such risks will have to be weighed against the merit of the case and the lack of action by others to address the issue.

These safeguards are sufficient to ensure that the operation of the regime will be rare and limited to meritorious claims. Indeed, non-profits are likely to see their role as an option of last resort, where no data subject is able to bring a case in their own name.

Taken together, non-profits are highly unlikely to bring vexatious or speculative actions, particularly when factoring in the prospect of adverse costs.

Existing court and regulatory safeguards

In addition to the internal controls within organisations, courts and regulatory system are well-versed in dealing with speculative and vexatious complaints in other contexts. Any vexatious or unmeritorious claim in court is likely to be struck out at an early stage, while the regulatory authorities have a cultural history of dealing with unmeritorious cases, and a policy basis to filter these out.

Coupled with the internal limits within organisations, the well-established filters within courts and regulatory authorities mean there are unlikely to be copious claims that the ICO and courts will have to deal with.

Prospective safeguards

Under s188(1) DPA 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 "provision about the 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; and
(e) costs.

Thus, the Secretary of State is already empowered to consider how non-profits bring claims or actions. Should further safeguards be deemed necessary, the Secretary of State could introduce them by Regulations. For example, if there was a concern about a large number of cases from unqualified non-profits, Regulations could specific that before a claim is brought, the non-profit must be required to apply to court as having met the criteria within s187 DPA. However, this is unlikely to be necessary given the existing safeguards and limitations outlined above.

15. 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?

Firstly, 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 non-profit considers that infringements of rights have occurred. Further, non-profits are unlikely to be acting contrary to the interests of data subjects in taking these cases, as any cases would relate to the infringement that a data subject has been subject to. Such a claim would therefore be consistent with both the non-profit's mandate and wider public interest goals, as well as the interests of the data subject to remedy infringements of the data protection regulations. Data subjects are thus unlikely to take issue with non-profits seeking to change practices on their behalf.

However, were a data subject to be named as part of a complaint or action under Article 80(2), that data subject should be afforded the right to opt-out of that complaint or action. However, this would only be required if the non-profit were seeking to name or identify the data subject, which is neither necessary nor consistent with the Article 80(2). Should the need to name the data subject arise, there would need to be both (1) an initial right to opt-out at the point at which the data subject may be named (2) as well as an ongoing right to opt-out, as data subjects may only become aware of a complaint/action after the action is commenced, or there could be developments along the way that could cause an individual to change their mind about wanting to be a part of it.

16. 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. As discussed above, similar fears were raised in an Article 80(1) GDPR context and have not materialised. The safeguards noted under our answer to Q15 are sufficient to ensure that a non-profit will need to be extremely motivated to bring an Article 80(2) action and such actions will be reserved for exceptional cases only.

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 hundred if not thousands of claims).

To date s187 has proven incapable of providing sufficient protection by itself and thus Article 80(2) fills a gap by overcoming many of the limiting factors that have likely resulted in the lack of actions under s187 so far. The increased protection for data subject rights which Article 80(2) promises is a positive development.

Finally, the new provisions would incentivise those data controllers whose business models intentionally infringe data protection law to rapidly modify those business models to become compliant. It will increase accountability, encourage a more compliant culture amongst controllers, and ensure a more effective and complete protection of data subjects. This will increase compliance costs across the data economy in the short term, but also stimulate progressive and compliant business model innovation and result in a more robust and sustainable data economy in the long term.

80(2) does not extend the duties of data controllers, it simply gives victims of data breaches access justice. Every action a data controller does to ensure that action is not taken against them by 80(2) is an action they should have already taken under UK data protection law. In sum, ***for a company compliant with the law there will be no additional cost.***

17. 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?

The ICO is unable to adequately ensure business model compliance with data protection law because it is under-resourced relative to the enormously wealthy global corporations it regulates.

There are clear benefits to these complaints and actions being brought on a systemic-issues basis, rather than being tied to specific individuals. Article 80(2) actions could potentially involve large groups whose rights have been infringed. The ability to deal with these issues on the basis of a single targeted complaint about a systemic infringement would help to free up both the courts' and the ICO's time and resources.

Further, it is likely that only a small number of test cases will be needed to establish infringements of data protection law. Given that such infringements are both widespread and generally similar in nature across corporations, these test cases will likely be adequate for catalysing broad compliance with data protection law across data economy corporations operating in the UK. If the new provisions are adopted, they would thus naturally limit the long-term pressure on the judicial system from such technically complex and protracted cases.

18. 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.

While this question relates to proceedings under the CPR, we also consider it useful to address the alternative mechanisms under s187 DPA here.

Section 187 DPA

Section 187 DPA enables a data subject to mandate a non-profit to act on its behalf. However, as noted above there has not been significant uptake of actions under its provisions to date. This response has highlighted many of the likely reasons why this is the case. In particular, s187 actions are limited to a mandate from data subjects and is therefore likely to operate in very limited contexts.

CPR 19.6 representative actions

The procedures under CPR 19 envisage compensatory claims brought on behalf of a group of similarly affected 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.

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 1559). However, there are a few features that are pertinent.

- 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.

Thus, because these rules are subject to a number of limiting factors which generally preclude their use, such as stringent requirements that parties share the 'same interest', this would likely negate CPR 19 being used in the same way as an Article 80(2) case. We do not therefore consider CPR 19 to be an adequate alternative remedy to Article 80(2) proceedings.

Furthermore, the CPR 19 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, a non-profit can pursue systemic infringements in the absence of identifying data subjects or sharing their interest in the case. This is the 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.

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

Section 187 DPA

There is yet to be any significant uptake of actions under the s187 provisions for various reasons. For instance, a data subject may not even be aware of their data rights 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 s187. The procedure in s187 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. Non-profits 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 representative actions

CPR 19 actions are mainly intended for compensation claims (see previous sections). Non-profits are unlikely to be able to use the CPR procedure as they will are unlikely to have a common interest in the case, such to create a GLO or a representative 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. The current CPR procedures are thus inadequate to address the type of cases which Article 80(2) is aimed at.

Overlap

Introducing Article 80(2) would help to alleviate these difficulties and allow systemic infringements which impact on individuals' rights to be dealt with at a macro level by NGOs who are experts in data rights protection. This will help to ensure more effective and complete protection of data subjects' rights.

Article 80(2) will operate to increase accountability, encourage a risk-averse culture amongst controllers, and ensure a more effective and complete protection of data subjects. It is likely to bring wider societal benefits and its introduction would be a step in the right direction towards complete and effective protection of data subjects' rights.

For further information, please contact:

Tony Stower, Director of External Engagement
tony@5rightsfoundation.com

Building the digital world that young people deserve