Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

The Information Commissioner's Office response to the Department for Digital, Culture, Media and Sport's Call for views and evidence - Review of Representative Action Provisions, Section 189 Data Protection Act 2018

Introduction

The ICO welcomes the opportunity to contribute to the review of the representative action provisions contained in the GDPR and Data Protection Act 2018 (DPA18).

A key objective of the ICO's Regulatory Action Policy (RAP) is to respond swiftly and effectively where breaches of legislation affect vulnerable people such as children and victims of crime. It was in this context that the Information Commissioner made it known during the passage of the data protection legislation that she supported, in principle, the ability of non-profit organisations to act on behalf of individuals who have not specifically authorised them to do so (Article 80(2) GDPR), as one of a number of potential mechanisms for providing redress to individuals.

The United Kingdom has an active and robust civil society involved in promoting rights and protecting the vulnerable. As a regulator, we recognise the significant role civil society has played, particularly over the last two years, in bringing well researched complaints to the ICO in order to help us regulate more effectively.

The ICO has been responsive in taking up civil society complaints irrespective of whether there is a named individual or not. The ICO has a number of illustrative case studies including facial recognition technology, misuse of data collected by data brokers, the police use of mobile phone extraction data; and cases involving children's data such as the Gangs Matrix or access to the National Pupil Database. In determining which cases to take forward, we use a risk based proportionate approach that focuses on where the greatest harms lie to individuals. The approach is set out in our RAP which has been widely consulted on. It is therefore the

case that current legislation already gives us the flexibility and discretion to act appropriately in response to civil society complaints.

However, the ICO is aware that advances in technology and the growth of big data means that there is an increase in invisible data processing. Individuals may not necessarily be aware of what data is being held about them by an organisation or what is being done with it. In such circumstances, individuals might not be expected to know how to exercise their data protection rights. The ICO therefore remains committed to ensuring that the risk based approach set out in our RAP enables us to take on cases that raise thematic data protection issues with a broad public interest. In this light the ICO remains supportive of the aims of Article 80(2).

Article 80 provisions

Article 80(1) of the GDPR allows data subjects to appoint "properly constituted" not-for-profit bodies or organisations (which could include child advocacy services or other organisations representing the interests of children) to exercise their right to:

- bring a complaint to the ICO or another supervisory authority.;
- appeal against a decision of a supervisory authority; or
- bring legal proceedings against a controller or processor.

Article 80(2) of the GDPR provides that Member States can legislate to allow such bodies or organisations to exercise these rights on behalf of data subjects without the data subjects' authorisation.

As the body responsible for handling complaints about potential breaches of the legislation, our submission focuses on our operational experience to date of Article 80(1) and other complaints brought by non-profit organisations. Our response particularly covers our risk based approach to determining which complaints we take forward, as set out in our RAP. Our response also considers the potential regulatory and resourcing implications for the ICO if the Government decided to implement the provisions in Article 80(2) that would allow non-profit organisations to act on behalf of individuals who have not given express authorisation.

Current approach to complaints from non-profit organisations

The ICO received 38,514 complaints in 2019/20; the overwhelming majority of these were from individuals concerned about how an organisation has handled their personal data. Under S165(4) and (5) of the DPA18, we must take the appropriate steps to respond to a complaint or inform the complainant of progress in handling their complaint, normally within 3 months. If a complainant feels we have not fulfilled our obligations, they can apply to the First-tier Tribunal (General Regulatory Chamber) under S166 DPA18 who can order the ICO to progress a complaint.

Our current understanding of the law is that the Commissioner must take appropriate steps to respond to the complaint but that does not extend to a requirement that the Commissioner take appropriate steps to resolve the complaint. We recognise though that this principle is currently subject to challenge in a number of pending cases before the Tribunal.

By contrast, the number of complaints that have met the criteria under Article 80(1) since it came into force in May 2018 is fewer than 100. This might be due to the strictly-drawn definition of the type of representative body that can bring a complaint; they must be able to demonstrate "statutory objectives which are in the public interest" and that they are "active in the field of the protection of data subjects' right and freedoms". It also relies on individual data subjects - who may not be aware in a given instance that their data rights have been breached- to take action and give the mandate; and for the non-profit organisation to maintain that mandate throughout the lifecycle of the complaint or court case, which can be lengthy.

It is therefore not uncommon for individuals linked to non-profit organisations to act collectively as the data subject in a strategic test case in a complaint to a supervisory authority. However, Article 80(1) is normally only engaged if the data subjects, on whose behalf the organisations are acting, are named.

As set out earlier, it is important to note that the ICO has a significant track record of working with non-profit organisations to investigate data protection complaints in the public interest that pre-date and fall outside the criteria set by the Article 80(1) provisions. As mentioned in the introduction, the ICO has a number of case studies that have arisen from a complaint or complaints by non-profit organisations. A specific example is the recent mobile phone extraction investigation[1] that originated from a complaint made by Privacy International. Many of the examples of our investigations involve data processing that might pose a significant harm to data subjects, but because of the non-transparent nature of the processing the individuals may not know that their rights are being breached. The investigations also engage strategic public policy issues and result in policy or operational recommendations with wider public interest benefits.

Regulatory Discretion: How does the ICO determine which cases or investigations to pursue?

The complaints the ICO receives from the public, including civil society, are crucial to helping us develop a rich picture of the information rights landscape. We can identify sectoral trends, multiple complaints about a controller, identify data breaches or where there has been suspected poor compliance. As a result, our guidance, investigation and enforcement work can be targeted in the right areas which benefit the public and encourage better compliance.

We have therefore concentrated resources on the investigation of cases aimed at improving data security practices, reducing unlawful access, and addressing compliance concerns about the use of new surveillance technology. These areas, along with nuisance calls and texts, are a key focus of our investigative and enforcement activities.

We assess all potential cases according to where they stand against our regulatory priorities. We have a robust framework to help us make these judgements, and which allows the highest priority cases to undergo a

[1] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/06/ico-releases-findings-on-the-use-of-mobile-phone-extraction-by-police-forces/

detailed risk assessment. This framework is informed by the intelligence and information gathered through our Annual Track survey, to ensure we are reflective of the priorities of stakeholders and the public. In short, this enables us to identify where risk, impact or harm is highest and to allocate resources accordingly.

Representative action without authority

As previously stated, the ICO has been supportive of the principle of non-profit organisations being able to bring complaints without the authority of named individuals (an opt-out model). We recognise that there is a significant amount of invisible processing taking place and therefore it will not always be the case that individuals know their rights might have been breached and are therefore able to take action against the organisation responsible for the breach.

It is important to note, however, that although the UK has not implemented Article 80(2), the ICO has taken forward a number of investigations at the request of non-profit organisations as set out above. These investigations have involved large scale non-transparent processing and therefore encompass significant numbers of individuals who would not be aware of the potential breaches of their data protection rights.

The vast majority of our resources are spent on our statutory obligations which include handling and investigating complaints from individual data subjects and providing advice to organisations to comply with data protection law. Where we have discretion, we take the risk-based approach described above to determine which investigations to pursue to ensure we are targeting resources appropriately.

The ICO is currently funded from fees from data controllers, the majority of which are small and medium size businesses. It is incumbent upon us to continue to deliver value for money to fee-paying organisations.

While the ICO has been supportive of the principle of Article 80(2), there are a number of factors which need to be weighed in considering the application of this provision.

As very few EU member states have implemented this provision, we could expect the ICO to be the go-to supervisory authority in Europe for Article 80(2) complaints if the provision were implemented in the UK. Without sufficient evidence of how this provision is working in other jurisdictions, it is not clear what level of complaints the ICO could expect to receive each year.

It should be noted that the ICO would still have a duty to comply with the timescales for handling complaints under S165 DPA18, potentially placing an increased burden on the office arising from the additional number of complaints which would need to be responded to. There is the potential for such cases to be resource intensive and the ICO would therefore welcome a fuller analysis of the budgetary and resourcing implications.

In the Government's consultation document on Article 80(2), it was rightly noted the emphasis on the need to protect children online, including from the misuse of their data. There has been suggestion that if Government decided to implement Article 80(2) it could be undertaken in a phased manner, with children and other vulnerable groups being prioritised and the evidence base reviewed before rolling out more widely. Again, an assessment of the wider implications of such an approach would be welcomed and the ICO would stand ready to play a role in that assessment.

Effective judicial remedy including compensation

The GDPR provides individuals with a right to an effective judicial remedy (Article 79(1)), and a right to monetary compensation from the controller or processor if they have suffered material or non-material damage if their data rights have been infringed (Article 82). The ICO does not have the power to award financial compensation.

In cases involving large data breaches or serious infringement of rights there is likely to be significant interest in taking claims to the Courts. An example of this is the recent British Airways data breach which led to the granting of a group litigation order by the High Court which could involve approximately 500,000 customers whose personal data was compromised by the incident.

Lastly, it is important to note that the ICO is a regulator and does not have the functions of an Ombudsman. That means we would not be able to provide a finite remedy in cases brought under 80(2), including issuing compensation. This is likely to result in cases for compensation being sought on an individual basis, with implications for both the judicial system and business.

Conclusion

The ICO remains supportive of efforts to ensure greater awareness and greater understanding of data handling and data misuse, and the ability of individuals and civil society to contribute to the protection of the rights of data subjects. We recognise that in principle the implementation of Article 80(2) has the potential to contribute to that. However, as set out above, we believe that there are a number of relevant factors to be considered as part of this implementation decision.

Regardless of the outcome of the government's decision on the implementation of Article 80(2) the ICO will continue to work with civil society to protect the information rights of individuals in the UK.

The ICO hopes this submission is informative and remains ready to engage further on the substantive points including providing case studies of previous relevant examples to DCMS where helpful.

October 2020