OPEN RIGHTS GROUP

Representative actions under the UK GDPR

Guide and lessons learnt

April 2022

In this Report

1 Introduction

This report is about Open Rights Group (ORG) experience with representative actions under article 80(1) of the UK GDPR and Section 187 of the Data Protection Act 2018 (DPA). It is meant to help other organisations consider representative actions to challenge infringements of data protection laws.

As technology advances, more and more decisions affecting our rights, welfare or expectations are mediated by digital, data-driven systems. Employers use data to raise or deduce salaries, hire or fire workers. Online platforms use data to favour or discriminate against their customers. Advertisers, banks, insurance companies, landlords, and even law enforcement authorities use personal data to make decisions that may include, exclude, favour, or disfavour individuals.

Data protection laws are meant to protect individuals from unfair, adversarial or otherwise detrimental uses of their data. The UK General Data Protection Regulation provides:

- Obligations to use personal data in a legal, fair, transparent, and respectful manner;
- Rights for individuals, and remedies against abuses;
- Powers for the Information Commissioner's Office to oversee and enforce data protection laws.

The UK GDPR also provides a new right for public interest organisations to represent individuals. In other words, not-for-profit bodies can represent victims of data protection infringements before the ICO or Courts.

This report is a reflection of our experience. ORG attempted to commence representative action before the ICO as part of our Data and Democracy project, which dealt with illegal profiling for electoral purposes during the 2019 UK General Elections. The subject of our complaint was resolved without the need to litigate. Nevertheless, we believe that sharing our experience will help other organisations to get a head start.

In particular, we will elaborate on:

- When and why should you consider representative action?
- What are the legal requirements?
- What are the risks involved?
- What lessons did we learn?

2 ORG experience in a nutshell

During the 2019 UK General Election, Open Rights Group provided an online tool to support individuals willing to file Data Subject Access Requests to main UK political parties.[1] The project was a reaction to the Cambridge Analytica investigations and the ensuing revelations about political parties widespread abuses of electoral data for illegal profiling or other campaign activities.

One of these political parties systematically failed to answer DSARs and took an uncooperative attitude toward individuals filing these requests. In turn, this effectively frustrated their right of access under Article 15 of the UK GDPR. ORG became a representative organisation under Article 80(1) of the UK GDPR for a pool of individuals who stood up against this abuse.

1 https://www.openrightsgroup.org/campaign/who-do-they-think-you-are/

3 What are representative actions?

In short, representative actions are an opt-in collective redress mechanism that allows representative organisations to exercise data protection rights on individuals' behalf.

Section 187 of the UK's Data Protection Act 2018 (DPA) provides a new right for organisations to represent individual's in complaints to the Information Commissioner's Office for breaches of UK data protection law or in Court. These powers mirror those provided for in Article 80(1) of the UK General Data Protection Regulation.

These provisions enable a data subject to authorise a body or other organisation that meets certain conditions to exercise rights on their behalf. The rights available for exercise under the UK GDPR are:

- The right to lodge a complaint with a supervisory authority (Art 77);
- The right to judicial remedies against the supervisory authority (Art 78) and judicial remedies against controllers and / or processors (Art 79);
- The right to "receive compensation", as far as provided for in domestic law (Art 82).

In addition, s187(2) DPA allows certain organisations to bring certain actions on behalf of data subjects concerning "the processing of personal data to which the GDPR does not apply". Those actions under the DPA are substantially mirroring those of the UK GDPR, namely:

- Rights under Section 165(2), (4)(d) and (6)(c): complaints to the Commissioner;
- Rights under Section 166(2): orders for the Commissioner to progress complaints;
- Rights under Section 187(1): compliance orders
- The right to promote judicial review against the Commissioner.

Activities that explicitly fall outside of the UK GDPR are using data for Law Enforcement purposes (Chapter 3 of the DPA 2018) and for Intelligence Services Processing (Chapter 4). Furthermore, Section 24 of the DPA 2018 provides a list of activities exempted from the UK GDPR, for instance, "Manual unstructured data held by FOI public authorities".

It is worth noticing that representative actions can be used to represent one or multiple individuals. In any case, representative actions are strictly opt-in: you will need the authorisation of each individual you represent.

4 When should you consider a representative action?

In short, representative actions present many opportunities in advocacy and strategic litigation. Their potential deserves to be explored with a realistic approach, taking stock of the resources and staff time that needs to be allocated to manage data subjects' cohorts.

Representative organisations must act with the authority of the individuals they represent. In turn, you will need to coordinate with the individuals you represent, ensuring that they are involved in the proceeding and responsive to its developments. While this may be time-consuming and require adequate resourcing and staff time, the advantages of this approach are not to be underestimated.

Firstly, where data protection infringements affect large numbers of individuals, representative actions will help draw attention to the systemic nature of these violations. While individual complaints may be useful to repair specific wrongdoings, representative actions are naturally suited to advocate for wide-ranging structural changes. Furthermore, privacy and data protection harms can sometimes be small from the standpoint of an individual, but become substantial if aggregated from the perspective of society. For instance:

> In the aftermath of the Cambridge Analytica scandal, Open Rights Group published "who do they think you are", an online tool to support individuals willing to file Data Subject Access Requests to main political parties in the UK. The law requires organisations to answer these requests within one month, but one political party systematically breached this statutory timeline. Some individuals had their requests fulfilled up to one year after they submitted.
>
> ORG sought to prevent digital technologies from eroding public trust in the democratic process and promote change in the way political parties handle and take responsibility for using data. Representative actions were a useful tool to establish that the issues we complained about were not isolated cases, but structural and repeated failures.

Secondly, data protection Regulators are notoriously struggling to cope with the growing number of abuses, either because they lack adequate staffing and resources or face opposing political forces. Representative actions may be of help:

- Organisations can use representative actions to produce evidence of malpractice from different angles and build a complaint that comprehensively describes issues and their root causes. In turn, this reduces the time and resources that a regulator must invest in dealing with your complaint.
- Regulators usually act upon complaints with a significant degree of discretion. The Information Commissioner's Office will prioritise regulatory action infringements that are severe, cause a "high degree of damage to the public", or affect many people. Representative actions help bring larger numbers of complainants together, thus emphasising that the breach isn't trivial or an isolated case. Further, large numbers of individuals "opting in" to a representative action are helpful to prove that the public is concerned about the issues you are raising.
- Representing multiple individuals in Court benefits the functioning and efficiency of the judicial system.

Finally, individuals — especially those in vulnerable situations — would benefit from civil society organisations' organisational and financial capacity. In turn, representation rights can enable and facilitate individuals in responding to abuses and exercising their rights.

5 What are the legal requirements?

In short, representative organisations must qualify as not-for-profits that operate in the public interest, apply and distribute their resources for charitable or public purposes, and are active in the field of data protection. Organisations must also act with the authorisation of the individuals being represented.

You will need to satisfy the qualifying criteria for representative organisations, as set forth by the Data Protection Act 2018. You will also need to be properly mandated by the individuals you wish to represent. These criteria are described below in greater details.

It is worth noticing that, following the UK departure from the European Union and the amendment of the "UK GDPR", article 80(1) does not include anymore the qualifying criteria of the "EU GDPR".

5.1 Organisational requirements

Section 187(3) and (4) of the UK Data Protection Act 2018 provide that, to represent data subjects with their authority, an organisation

- Must (after payment of outgoings) apply the whole of its income and any capital it expends for charitable or public purposes;
- Must not directly or indirectly distribute amongst its members any part of its assets (otherwise than for charitable or public purposes);
- Must have objectives that are in the public interest;
- Must be "active in the field of protection of data subjects' rights and freedoms with regard to the protection of their personal data".

The requirement to be considered "active in the field of data protection" is quite vague. Open Rights Group would have surely met this requirement, but it is reasonable to assume that organisations that do not work in the digital rights field may still satisfy the criteria as well. For instance...

- Confidentiality of health data;
- Consumer protection against consumer reporting, credit ranking, predatory commercial practices based on consumer's profiling etc...
- Challenges to immigration practices such as fingerprint scanning or VISA algorithms;
- Challenges to employment practices such as automated hirings and firings, performance evaluations and wage deductions;
- Challenges to illegal disclosures or unfair decisions based on protected characteristics such as gender, race, political views or health conditions;
- Challenges to law enforcement reliance on surveillance technologies;

...are all areas or activities that engage, to different degrees, with data protection. Organisations should evaluate their position on a case by case basis and, where adequate, seek legal advice before ruling out their eligibility for a representative action.

5.2 Consent requirements

Individual data subjects must properly mandate organisations. The form and content of this mandate will depend on the case's specific circumstances. At a minimum, mandates will have to set out:

- That the individual wants your organisation to act for them;
- That the mandate would be exercised under Article 80(1) of the UK GDPR or s187(2) of the DPA 2018—depending on whether you would address data processing that is regulated by the UK GDPR or not;
- That your organisation have authority to make representations on their behalf.

Civil society organisations are (usually) not law firms. If you are not a legal representative, it would be important to clarify this so individuals know what "representation" means and understand the related limits to such action. In practice, this can be achieved by setting the terms of this relationship upfront. If you instruct lawyers on that action, you would need to discuss and clarify the terms of the cooperation among your organisation, the law firm and the individuals being represented.

6 What are the risks involved?

In short, you will face financial risks in Court proceedings. You should seek legal advice to evaluate your options and limit or contain such liabilities.

If you use representation rights to complain to the Information Commissioner's Office, you will not bear any liability: complaints can be lodged free of charge, and there are no adverse costs.

If you use representation rights in Court, the general rule is that the unsuccessful party will be ordered to pay the successful party's costs, pursuant to CPR 44.2(2)(a). There are options to limit liability for adverse costs, such as:

- Protective Cost Orders (Section 51 of the Senior Courts Act 1981) for Judicial Reviews;
- Costs Capping Order (sections 88 and 89 of the Criminal Justice and Courts Act 2015 and CPR 46.16 to 46.19) for Judicial Reviews, including third parties' interventions;
- Costs Capping Orders in an Aarhus Convention claim, for Judicial Reviews related to some environmental matters;
- Costs Capping Orders (CPR 3.19) for proceedings other than Judicial Reviews;
- Litigation insurances or funding.

Rules and evidentiary threshold to be granted these orders are diverse, and the opportunity to rely on any of these instruments will depend on the specific circumstances of your case. The same is true for litigation funds and insurances. You should assess your options and seek legal advice on this matter.

7 What lessons did we learn?

At this stage, we assume that:

- You are determined to commence representative action, and you understand whether you would be exercising representation rights under article 80(1) of the UK GDPR or Section 187 of the Data Protection Act 2018;
- You assessed your eligibility as a representative organisation, and took stock of the risks involved.

Based on our experience, your next priorities should be to assess and allocate adequate resources to the project, and plan in advance.

7.1 Lodging a representative complaint

We discuss the steps required (or foreseen) to commence representative action before the Information Commissioner's Office, because this is the scenario where we have direct experience. Gathering evidence, contacting defendants, and escalating issues are all activities that may also apply to judicial proceedings. Still, you must be mindful of the different requirements you must fulfil to be admitted in Court.

You will need to onboard individuals you wish to represent as a first step. The right way to recruit them will depend on your case: you may have to look for victims of abuses or data breaches, or need volunteers to help you investigate and complain against infringements. In any case, you will need to

- Find data subjects who want to be represented;
- Explain to them the terms of your and their involvement;
- Prepare a mandate they can subscribe to, that explains these terms; and
- Collect their consent, which authorises you to act on their behalf.

To lodge a GDPR complaint, complainants must be able to explain and prove that there was an infringement of data protection laws, and their data was involved in such infringements.

This is the bare minimum, but there are other steps you may want to take to strengthen your position and increase the chances that the ICO take your complaint seriously. For instance, you may want to emphasise the impact and harm these infringements had on the individuals you are representing.

You may also want to file a Data Subject Access Request to collect further evidence. Indeed, DSARs can be a powerful tool to prove that individual data was held and

misused. It would be desirable to contact the actor or organisation you are willing to complain about with the grounds of your complaint before contacting the ICO. On the other hand, the circumstances of your case may suggest that contacting the perpetrator could endanger the victims you are representing or otherwise help them to dodge responsibility (for instance, by shredding evidence). Showing that you tried to resolve the complaint privately will strengthen your position and increase the chances that your complaint is dealt with by the ICO, but it is not a legal requirement.

To summarise, you will need to:

- Collect relevant evidence from the data subjects;
- Consider the data protection law at issue;
- Construct grounds of complaints;
- Compare your ground of complaints with the evidence at your disposal, consider whether you need to gather further evidence to prove your point;
- Contact the data controller with the grounds;
- File a data subject access request (conditional to the need or desirability to collect further evidence in this manner).
- Liaise with data subjects on the discussions with the data controller;
- Based on conversations, there could be further dialogue between the data controller and data subjects;
- Record your interactions and those of the data subjects with the controller, make sure they reflect and answer to the grounds of your complaint;
- If appropriate, try to negotiate a solution with the rights infringer before lodging your complaint to the ICO.

Finally, if you reach the stage where you exhausted the conversation with the rights' infringers, you should finalise your complaint and escalate to the ICO. Complainants may want to call on the ICO to take specific actions to address the violation they were subjected to, but this is not strictly necessary. A more generic call to investigate or to take action against systemic infringements would also suffice, insofar the complaint you are lodging is related to an issue within the remit of the ICO.

Thus, you should prepare to

- Progress the complaint to formal submission to the Information Commissioner;
- Engage with the Commissioner on their deliberations;
- Seek updates from the Commissioner within three months of the complaint lodged;
- Reflect any outcome on the submission of the complaint to the Commissioner, to the data subjects;
- If you aren't satisfied with the outcomes, discuss with complainants and provide advice on the next steps (for instance, a representative action in Court against the ICO).

As a reference, Open Rights Group were broadly involved up to chasing the data controller to make sure they answered to DSARs and discussed the grounds of our complaint. This required the work of 3 members of staff requiring a month of staff time, equivalent to 1 member of staff working full time for a month on the action.

7.2 Issues and how to avoid them

The biggest challenge you are likely to face is managing and coordinating with the individuals you represent during your representative action.

As you need to establish the facts of each individual and how these relate to the infringement you are complaining about, you will need them to provide this information to you. This may take the form of documents, witness statements, or any other relevant medium. If you haven't this evidence already, individuals will need to collect or produce them, and pass them to you.

The individuals you represent will have different backgrounds, responsiveness, and attentiveness to what you are doing and what they are required. They may lose or dispose of important documents or other evidence without realising it. They may miss your emails or take their time to respond. If you don't address these risks and practicalities upfront, you may easily lose plenty of time.

7.2.1 Collecting evidence

- You should develop a clear understanding of what evidence you need to prove your thesis, and how to obtain it;
- If evidence already exists, you should ask data subjects to give it to you and store it as soon as possible;
- If you can use data subjects' authorisation to obtain this evidence on their behalf, this should be your preferred course of action;
- If individuals need to obtain evidence autonomously, you must make sure they know precisely what they need to do, and ask them to send this evidence as soon as they get it.

For instance, Open Rights Group made an online tool available for individuals willing to file DSARs requests to political parties in the UK. At this stage, we were facilitating and not representing these individuals, who acted autonomously. One political party failed to answer these requests, and participants were invited to volunteer for our representative action.

In turn, individuals interacted with the political party autonomously at the early stages of this project. ORG kept in touch with them, but we later spent significant time collecting each email, letter, or other relevant items to establish the facts of each and single individual involved. We found out that some complainants had trashed letters or lost evidence without realising it. Further, some individuals were taking a long time answering emails. Tracing and producing the documentation we needed to corroborate our claims became a significant source of stress.

This scenario could have been avoided by collecting evidence instantly through the online DSAR tool or proactively asking for these documents as our relationship with data subjects progressed. Alternatively, you could consider obtaining the authorisation to act on their behalf before submitting DSARs to interact directly and from the beginning with the organisation you want to complain about.

7.2.2 Dealing with data controllers

Organisations are seldom enthusiasts about receiving and answering Data Subject Access Requests. They have a terrible track record of non-compliance before the entry into force of the GDPR, and they are lobbying hard to get rid of this requirement. Non-compliance, negligence, and fear to disclose information that can hold them to account will make an offender naturally inclined to resist your requests.

While the UK GDPR provides a solid right of access to one's personal data, there are leverages that organisations can try to rely on to reject or slow your action. Namely:
Data controllers are entitled to "request the provision of additional information necessary to confirm the identity of the data subject", under Article 12(6) of the UK GDPR.

Data controllers must act upon your requests within one month. This period "may be extended by two further months where necessary, taking into account the complexity and number of the requests".

To mitigate such risks, you should assess any circumstance that may make it difficult for the organisations you are interacting with to identify the data subjects. When this is the case, you may want to file additional documents to address this risk (for instance, you may want to attach an ID to the DSAR request).

There is little you can do to counter an extension of two further months to answer DSARs, except for factoring in possible delays in your plans. You should also keep in mind that if the controller invokes this extension, it will go down on their record: you should ask them to clarify on what basis do they find it necessary to extend the deadline, and you will be able to complain about it with the ICO if and when you escalate your case.

Finally, when you are acting on behalf of the individuals you represent, you are effectively a third party requesting personal information relating to another individual. You need to be properly mandated by data subjects to do it, and any organisation that discloses this information to unauthorised third parties would be committing a breach. Therefore, you should prove that you were given authority by data subjects as soon as you write to the data controller.

For instance, Open Rights Group online DSARs tool sent individuals' requests via an autogenerated proxy email address. This allowed the political party who received the requests to claim that they needed to verify that these messages really came from the data subjects. The law requires that requests filed electronically are answered in the same manner, but the lack of a personal email address allowed them to claim that they had to run this process by conventional mail. This allowed them to slow and frustrate the process, and it could have been easily avoided by including the personal email of each individual in the DSAR.

Furthermore, the political party contested our authority to act on behalf of the data subjects. Thus, we provided written proof, signed by the data subject, to prove our authority.

8 Relevant policy developments

We saw in the previous sections that Article 80(1) representative actions with authority are a bittersweet tool. On the one hand, they help ease access to justice and address power imbalances in a field where individual litigation is unlikely to influence large and powerful technology companies or government agencies. On the other hand, the practicalities are onerous, making this the first step of a longer journey.

Therefore, civil society organisations interested in collective redress mechanisms should also pay attention to UK policy developments in this area.

8.1 Representative actions without authority

The UK GDPR provides for representative actions without authority under article 80(2); however, this needs to be implemented.

The UK Government refused to implement this collective redress mechanism, based on corporate lobbyists argument that collective action would inconveniently expose businesses to litigation. However, the UK Government also stated they would review their position after Google vs. Lloyd. This case has now ended, and the UK Supreme Court reasonably ruled out class-action style litigation in the data protection field.

If the Government stand by their promises, they should review their decision not to implement Article 80(2). Representative actions without authority would be game-changing, as it would allow public interest organisations to litigate against data abuses on behalf of society, without the hurdles of involving and being authorised on an individual basis. If you have an opportunity to do it, you should consider applying pressure to the UK Government to review this decision.

8.2 Post-Brexit data protection laws

The Department for Digital, Culture, Media and Sport (DCMS) presented plans to undermine data protection laws in the UK in the "Data: a new direction" public consultation.

The proposal is trying to undermine individuals' right of access by introducing a DSARs fee regime as well as providing conditions that organisations can leverage upon to reject requests, such as the motives of the data subject or because of cost-

capping limits. As we saw before, DSARs are an invaluable tool to investigate infringements. Further, DCMS proposals would lower standards of protection, reduce accountability to a cosmetic exercise, make it difficult to exercise data protection rights and undermine the independence of the Information Commissioner. If you ever want to use this guide, you will need to prevent the UK Government plans from coming to fruition.

You can find more details on our website or in our answer to their consultation.[2]

2 https://www.openrightsgroup.org/campaign/stop-data-discrimination/

9 Acknowledgments

We would like to thank Reset for their support in taking this action and producing this output. We would also like to thank Ravi Naik at AWO for his fantastic advice throughout the process.

10 About Open Rights Group

Open Rights Group is a UK-based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. With over 20,000 active supporters, we are a grassroots organisation with local groups across the UK. We were heavily involved in the process leading up to the enactment of the Data Protection Act 2018 ("DPA 2018"), and we worked on issues such as data retention, the use of personal data in the COVID-19 pandemic, data protection enforcement, online advertising and the use of personal data by political parties. We have litigated a number of successful data protection and privacy cases, ranging from challenges to the lawfulness of the Regulation of Investigatory Powers Act at the European Court of Human Rights, being a party at the Watson case against UK data retention, through to the recent challenge against the Immigration Exemption in the Data Protection Act. We are also supporting complaints made to the Information Commissioner regarding Adtech and the use of data by political parties.