Data Protection Act

How we deal with complaints and concerns

A guide for data controllers

ico.
Information Commissioner's Office

Data Protection Act

How we deal with complaints and concerns

The ICO is the UK's independent public authority set up to uphold information rights. We provide a range of services to help us do this. These include dealing with information rights concerns raised by members of the public and using them to help improve the practices of those we regulate.

This guidance explains how we deal with concerns raised with us that those responsible for processing personal information, known as data controllers, have not complied with the Data Protection Act 1998 (DPA).

We deal with data protection concerns in line with our Information Rights Strategy. This means we take a 'case by case' approach. We will consider the concerns raised with us and put most of our effort into dealing with matters we think will make the biggest difference to information rights practice, either in that case or to address a more systemic concern.

Any action we take could take a variety of forms. In the most serious cases, we can serve monetary penalties of up to £500,000.

What does the law say?

Under section 42 of the DPA, any person who is, or believes that he is, directly affected by the processing of personal data, can ask the Information Commissioner to consider whether the processing is likely to comply with the law.

On receiving such a request, the Commissioner is obliged to consider the concern and make an assessment. The Commissioner can do this in whichever way he or she believes is most appropriate. The Commissioner will usually share the view formed and any action taken as a result.

Our approach

Good information rights practice doesn't just mean complying with the law. Organisations that hold and process personal information should also be clear and open about their practices – even when things go wrong.

If a member of the public is concerned about your information rights practices, we believe that you, as the organisation responsible, should deal with it.

We expect you to respond to any information rights concerns you receive, clarifying how you have processed the individual's personal information in that case and explaining how you will put right anything that's gone wrong.

How we deal with each concern we receive

We will not usually look into an information rights concern about your organisation unless the member of the public concerned has first raised it with you. If it appears that they haven't, we will tell them to do so, pointing them to relevant advice to help them.

If the member of the public has raised their concern with you, we will usually ask them for copies of:

- any relevant documents evidencing their concern, and
- the correspondence they have exchanged with you in an attempt to resolve it. We would expect this to include a clear explanation from you of the actions taken to address or respond to the concern.

We will assign a case officer to the case, who will be your point of contact throughout any investigation we choose to undertake. It will be the case officer's job to decide (in conjunction with other ICO colleagues as necessary):

- whether or not your organisation has breached the DPA; and
- if so, whether we need take any action as a result.

Deciding whether an organisation has breached the DPA

We have considerable discretion when considering compliance with the DPA. We can choose to reach our decisions based solely on the information provided by the member of the public, if we think it appropriate. We will put more resource into reaching decisions if the matter appears to give us an opportunity to improve information rights practice.

If it does not appear that you have breached the DPA, we will tell the member of the public and close the case. It is unlikely that we will contact you, as the matter is unlikely to give us an opportunity to improve information rights practice.

However, we will always tell you if we think you have breached the DPA.

Deciding whether to take action

There are a series of factors case officers will consider to help them initially assess the concern and consider the opportunity it may give us to improve information rights practice. These include (but are not limited to) the following:

- The severity of the potential breach

The case officer will consider whether the matter is serious, in terms of the nature of the data affected, the number of people affected, and the effect (or likely effect) on the individual(s) concerned. The more serious the breach, the more likely it is we will take action in relation to it.

- How you have dealt with any related concern raised with you

The case officer will consider how well you engaged with the member of the public, whether and how well you explained what happened and whether you made reasonable attempts to rectify any problems.

- The context

The case officer will also consider any other relevant information we may hold about the matter, your organisation or your sector along with our own regulatory priorities.

What does this mean for you as an organisation we regulate?

If a member of the public raises a concern with you about your information rights practice, you should take it seriously. In most cases, we will use the explanation you gave to them to make our decision about whether you have complied with the DPA.

As such, it is important that you demonstrate to your customers (and to us as the regulator) that you understand your information rights obligations. A good explanation of how you have applied the principles of the DPA can help avoid escalating disputes unnecessarily.

Rather than simply referring the issue or individual to the ICO, you should retain ownership of the concerns raised and work with the member of the public to try to resolve matters.

Helping you deal with concerns

When dealing with an information rights concern you should review your information rights practices. To help you do this, we provide the following:

- Guidance on our website to help you understand your information rights obligations.
- A helpline to give you the opportunity to ask questions and get advice.
- Informal visits or meetings to help you get things right.
- As a longer term measure, audits of business processes to help you ensure good practices for the future.

If we think you have failed to comply with the DPA, but the breach was minor and does not provide a realistic opportunity to improve your general practices, we will tell you and keep the details on file.

If we identify a possible opportunity for you to improve your information rights practice we will contact you. We will expect you to reconsider your practices and discuss with us how things can improve in future.

If we write to you asking for more information or for your views, we will tell you when we expect your response. It is your responsibility to meet this deadline and make sure you have arrangements in place to allow you to cooperate fully with our investigation.

If you think you won't be able to meet the deadline, you must tell the case officer immediately.

Failure to reply to the ICO's enquiries can result in a formal information notice. It can also result in us making decisions on the case based purely on the information we already have.

Taking action

If we think the concern, or a pattern of concerns, raised with us provides an opportunity for you to improve your information rights practices, we will take appropriate action.

This could take a variety of forms, depending on what we think would be most appropriate and effective in the circumstances. This could be giving advice about the way you respond to the public's information rights concerns, asking you to put right what went wrong in a particular case, asking you to produce an action plan to make improvements to information rights policies or taking more formal action in accordance with our Data protection regulatory action policy. This is not an exhaustive list. Any action or actions we recommend will depend on the circumstances of the case.

We expect you to commit to any actions we recommend to improve your practices and to understand that if you fail to address poor practice, or cause substantial damage or distress through poor practice, we have the power to enforce the law and serve you with a monetary penalty.

Where we don't take direct action in response to an individual's concern, we will keep a record of it and use the information that we hold to inform future regulatory decisions.

Understanding our priorities

We want to be open about our work and so publish information about the action we take and the improvements made by organisations to their information rights practice.

Self reporting incidents

Organisations can also report incidents to us themselves, particularly regarding data security, to help make sure they take the right steps in response.

For more information about how to decide whether to report an incident to us and how to do it, please see the Guidance on data security breach management on our website.

Information requests about the case

If we receive any requests for information about the case, we have a duty under the Freedom of Information Act 2000 (FOIA) to respond. It is in the public interest that we are open, transparent and accountable for the work that we do. It is also important that we do not undermine the trust and confidence of those who raise concerns with us. If you do have reasons why information sent to us in the course of an investigation should not be shared with anyone else, you should explain this to your case officer as part of your submission.

Contacting us

If you have any issues or outstanding queries about a case, contact your case officer. You will find their contact details on the correspondence they have sent.

Feedback on our service

We are committed to providing high standards of service to the public and making sure our work with those we regulate does not represent a disproportionate regulatory burden. All feedback about our service is valuable to us. Feedback about how those we regulate have been treated by the ICO helps us understand what we're doing well, need to put right or improve.

If you think we should have done something differently in how we have handled a concern about your organisation, or how we have treated you,

you can let us know. For more information, please see 'What you can expect from the ICO'.

www.ico.org.uk
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113

Version 1
1 April 2014

Information Commissioner's Office