ROPES & GRAY ALERT

Intellectual Property Transactions

July 5, 2017

ICO publishes revised Subject Access Code of Practice incorporating Court of Appeal guidance – dealing with requests from individuals for personal information

Attorneys
Rohan Massey

In the wake of two key judgments from the Court of Appeal, the Information Commissioner's Office has updated its Subject Access Code of Practice – Dealing with requests from individuals for personal information. The revisions, published on 20 June 2017, are designed to promote a spirit of co-operation and openness in terms of a readiness to engage with applicants, a willingness to negotiate in respect of repeated SARs and a readiness to take balanced steps when faced with compliance with a SAR rather than a mere assertion of disproportionate burden. The revised Code also requires data controllers to have in place procedures to find archived, backed up and deleted material, to set aside the applicant's purposes when handling a request. Finally, where an organisation has failed to comply with the subject access provisions, the ICO indicates that it will consider carefully whether there has been damage or distress before serving an enforcement notice.

Background

The ICO published the original version of its Subject Access Code in 2013 in order to help organisations provide subject access in accordance with the Data Protection Act 1998 and good practice. It aimed to do this by explaining how to recognise an SAR and by offering practical advice about how to deal with, and respond to, an SAR. The Code provided guidance on the limited circumstances in which personal data is exempt from subject access and explained how the right of subject access can be enforced when things go wrong.

The Code has now been updated and takes into account the guidance of the Court of Appeal in *Dawson-Damer v Taylor Wessing* [2017] EWCA Civ 74 *and Ittihadieh v 5-11 Cheyne Gardens* [2017] EWCA Civ 121.

Proper evaluation

One piece of good news for business is that the revised Code recognises that the burden on data controllers to comply with SARs is limited to taking reasonable and proportionate steps. Good practice in this area nevertheless relies on comprehensive evaluation of the particular circumstances of each request – businesses cannot merely assert that the burden of compliance is disproportionate.

In the ICO's own words:

"*When responding to SARs, we expect you to evaluate the particular circumstances of each request, balancing any difficulties involved in complying with the request against the benefits the information might bring to the data subject, whilst bearing in mind the fundamental nature of the right of subject access.*"

The revised Code explains that, in order to apply the exception, the burden of proof is on the data controller to show that it has taken all reasonable steps to comply with the SAR, and that it would be disproportionate in all the circumstances of the case for it to take further steps.

Readiness to engage with the applicant

The revised Code states that data controllers should "engage with the applicant". In practice this means "having an open conversation" about the information they require. This benefits the data controller in that engaging with the applicant might help reduce the costs and effort that might be otherwise incurred in searching for the information.

In the revised Code the ICO warns data controllers that:

"*If we receive a complaint about your handling of a subject access request, we may take into account your readiness to engage with the applicant and balance this against the benefit and importance of the information to them, as well as taking into account their level of co-operation with you in the course of the handling of a request.*"

The need for co-operation is particularly relevant to repeated SARs. The ICO explains that it would accept that a data controller may attempt to negotiate with the requester to get them to restrict the scope of their SAR to the new or updated information; but if they insist upon a full response then provision of all the information is necessary.

Purposes of an SAR

The Code of Practice is now also clear that the requester's purposes in making an SAR are strictly irrelevant to the obligation of a data controller to comply with an SAR. However, in the spirit of openness and co-operation, the ICO suggests that an understanding of the requester's purposes may help ensure that data controllers find what they are really looking for.

Archived data, back-up records and deleted information

The process of accessing electronically archived or backed-up data may be more complicated than the process of accessing "live" data and the revised Code covers these issues in some depth. For example, the ICO confirms that procedures should be in place to find and retrieve personal data that has been electronically archived or backed up.

Businesses will be required to provide archived or backed-up information in response to a SAR since copies of the data have after all been retained for future reference.

The ICO adds that data controllers will be presumed to be able to find the data, possibly with the aid of location information from the applicant, so they "*will be required to provide such information in response to a SAR*". In other words, the same effort that data controllers put into the search mechanisms to allow them to find archived or backed-up data for their own purposes should be employed to find information in order to respond to an SAR.

On the issue of deleted data, the revised Code states that the "*Commissioner does not require organisations to expend time and effort reconstituting information that they have deleted as part of their general records management.*"

Private emails

On the issue of staff and their private emails, the new Code states that generally speaking, the ICO would not expect staff to be instructed to search their private emails or personal devices in response to an SAR unless the data controller has a good reason to believe they are holding relevant personal data.

Enforcement notices

In another amendment to the Code, the ICO targets its own powers to get involved in disputes about SARs. The ICO explains that it can serve an enforcement notice, but adds that:
"*The Information Commissioner will not necessarily serve an enforcement notice simply because an organisation has failed to comply with the subject access provisions. Before serving a notice she has to consider whether the contravention has caused or is likely to cause any person damage or distress. She can serve a notice even though there has been no damage or distress but it must be reasonable, in all the circumstances, for her to do so. She will not require organisations to take unreasonable or disproportionate steps to comply with the law on subject access*."

Comment

The key message in the ICO's revised guidance is that data controllers should try to engage constructively with the individual making the request and in the spirit of co-operation seek to accommodate that request regardless of the motivation behind the SAR. The ICO will not, for example, allow a data controller to invoke the "disproportionate effort" exception in s 8(2) of the DPA to refuse to supply data in permanent form, without engaging with the individual to determine what information is actually required. As the court made clear in Dawson-Damer, steps need to have been taken to convince the court (and by implication the ICO) that the burden is discharged. Essentially, the court/ICO will want to see evidence showing what the data controller has done to identify the material and to work out a plan of action. A court, and presumably the ICO, will not draw inferences from mere argument.