ICO Subject Access Code of Practice – Consultation Summary

Introduction

This document summarises the responses to the ICO's consultation on the Subject Access Code of Practice (the Code) held between 29 November 2012 and 21 February 2013. There were 86 responses to the consultation, and we are grateful to those that took the trouble to comment. We have carefully considered the views we received, many of which are reflected in the final version of the Code.

The published version of the Code now sets out even more clearly:

- the rights individuals have to access their personal data under the Data Protection Act 1998 (the DPA); and
- the duties data controllers have to provide access to personal data.

By providing explanations and advice on how to recognise and handle a subject access request (SAR), together with links to other ICO guidance resources, the Code is a practical reference document that we hope will be helpful to many organisations and individuals.

Comments received, and the ICO's response

The majority of respondents welcomed the Code: "a comprehensive and useful document"; "Provides comprehensive explanation of how the DPA provides rights for individuals and how organisations should comply"; and "The draft Code explains ….. subject access rights clearly and succinctly". We received many constructive suggestions on ways to improve the Code.

The comments provided by all respondents demonstrated their positive engagement with the consultation exercise and provided us with much food for thought as to how we could make the Code an even more useful resource. We have endeavoured to address a high proportion of the concerns. Below we set out some of the major themes which emerged.

Size of organisation

Some people commented that the Code failed to meet the needs of organisations of widely differing sizes. Respondents from large and small

organisations each expressed the view that the Code was more appropriate for organisations of a completely different size, which seemed to indicate that perhaps we had hit the correct balance.

ICO response

The Code has to cover a wide range of organisations in different sectors – all of which are subject to the DPA. It would be impractical for the ICO to produce a Code for each type or size of organisation. Chapter 1 of the Code makes our position clear: "Although the practices that organisations adopt to respond to SARs are likely to differ, depending on their size and the nature of the personal data they hold, the underlying principles concerning subject access are the same in every case".

Disproportionate effort in finding and retrieving personal data

We received a number of comments on our approach in relation to disproportionate effort and the retrieval of personal data, and the interpretation of section 8(2) of the DPA.

ICO response

We have slightly revised the Code to explain our view that, in line with the High Court's decision in *Ezsias*, in order to find and retrieve information for the purpose of responding to a SAR, a data controller must take all necessary steps, provided that they are not unreasonable or disproportionate. This duty has to be understood in the light of the fundamental importance of the right of subject access. Thus we will normally expect a data controller to make extensive efforts to find and retrieve the necessary information to respond to a SAR. We have indicated in the Code how the data controller should respond to a requester where personal information is hard to access. The exemption in section 8(2) applies only to supplying the requested information in permanent form, and may only be relied upon in limited circumstances.

SARs made via social media

Many responses expressed concern about SARs made by means of social media, such as Facebook and Twitter. In particular, those responding doubted whether data controllers could adequately and efficiently identify SARs made via social media channels; they also expressed concerns as to how to verify a requester's identity, how to collect a fee and how to provide the requested information securely to the requester.

ICO response

Whilst social media might be perceived as a less than ideal mechanism for submitting a SAR, it is already permissible under the DPA. To provide assistance, we have therefore expanded the Code to explain how an organisation should handle SARs made via social media, and to provide advice on the practicalities of responding to requests received in this way.

SARs and disclosure in legal proceedings

Some of those responding sought further guidance on the interaction between the right of subject access and the power of a court or tribunal to order disclosure of documents in legal proceedings.

ICO response

The Code sets out how personal data protected by the concepts of legal professional privilege (in English law) and confidentiality of communications (in Scottish law) is exempt from the right of subject access. The Code also explains that, apart from those scenarios, an organisation must not refuse to supply information in response to a SAR merely because related litigation is contemplated or has been commenced. Obviously, the ICO recognises that the court has discretion as to whether to order compliance with a SAR. However, we state clearly in the Code that the possibility that the court will decline to order compliance does not, in itself, entitle a data controller to refuse to respond to a SAR.

Inclusion of a SAR handling checklist

Some responses gave their support to the retention of a SAR checklist or a flowchart, to help staff who handle SARs.

ICO response

We recognise the value of the SAR checklist, which previously took the form of a separate piece of formal guidance. We have decided to make it an even more useful tool for organisations by presenting it in a clearer flowchart format in an Appendix to the Code, as well as featuring it in interactive web pages on our website and publishing it as a freestanding leaflet.

The handling of bulk requests

In the light of comments, in Chapter 5 we have added a section on the handling of bulk requests, which are often received in particular by the financial sector. This section provides guidance on principles to bear in mind in these situations, including the fact that a SAR within a bulk request remains valid, and an acknowledgement that the organisation will wish to verify the individual's identity.

Style

Other guidance on SARs on the ICO website

There were concerns that confusion might arise between existing ICO guidance on SARs and the SAR Code.

ICO response

The Code is intended to consolidate the separate items of guidance on this subject, so as part of this exercise we are removing old guidance which duplicates its contents.

Navigation

Many respondents asked us to improve navigation within the Code and between other useful pieces of guidance.

ICO response

We have inserted links to other guidance and to the Guide to Data Protection. We have also included an index with links to each named / numbered chapter and section.

List of respondents

- Pennine Acute Hospitals NHS Trust
- Investec Wealth and Investment Ltd
- Mannin Security, protection and Investigation Services
- Kirklees Active leisure
- CIFAS
- Cabot Credit Management Ltd
- Perth and Kinross Council
- Muscular Dystrophy Campaign
- London Borough of Merton Council
- An unnamed national charity
- IBM
- Inverness College (university of the Highlands and Islands)
- Parliamentary and Health Service Ombudsman
- Disclosure and Barring Service (Home Office)
- Flintshire County Council
- Chief Fire Officers' Association
- Lloyds Banking Group
- The Church of England Archbishops' Council
- A member of the public
- Shell International Ltd
- Unison
- Hill Hofstetter Ltd
- Cumbria County Council
- DAS Legal Expenses Insurance
- An anonymous response
- Another member of the public
- Birmingham Law Society
- Equifax

- Western Health and Social Care trust, Northern Ireland
- The Building Societies' Association
- RSA Insurance plc
- Callcredit
- Southern Health and Social Care Trust (Northern Ireland)
- Airbus
- Department for Work and Pensions
- Privacy International
- Immigration Law Practitioners' Association
- Conservative Party
- Willis Group Ltd
- Barclays PLC
- General Medical Council
- Consumer Focus
- Canada Life
- Southern Water
- Department for Education
- Allen and Overy LLP
- Experian
- Brunel University
- Barnardo's
- Cornwall County Council
- Department for Transport
- Virgin Atlantic Airways
- Shoosmiths LLP
- BskyB
- NHS National Services Scotland
- Clarkslegal LLP
- Oxford University
- National Subject Access Group (part of ACPO)
- A local authority solicitor
- Macmillan Cancer Support
- Royal College of Physicians
- Wrightington, Wigan and Leigh NHS Foundation Trust
- NHS Health and Social Care information Centre
- Cardif Pinnacle
- National Information Governance Board for Health and Social Care
- Leeds City Council
- Information and Records Management Society
- BP Oil International Ltd
- Employment Lawyers Association
- Finance and Leasing Association
- Engineering Employers' Federation Northern Ireland
- BAE Systems
- Clyde and Co LLP
- Media Lawyers' Association

- EEF, the manufacturers' organisation
- British Retail Consortium
- Transport for London
- Association of British Insurers
- Welsh Government
- Brewin Dolphin Ltd
- Prudential
- Relate
- Institute of Chartered Accountants in England and Wales
- British Banking Association
- BBC
- National Association of Data Protection Officers