Consultation on ICO's Privacy notices code of practice: summary of responses

Introduction

This document summarises the responses to the ICO's consultation on the Privacy notices code of practice held between 2 February 2016 and 24 March 2016. There were 53 responses to the consultation, and we are grateful to those that took the trouble to comment. We have carefully considered the views we received and they have assisted us in producing the final version of the code.

The published version of the code sets out:

• the fair processing requirements that data controllers have to comply with under the Data Protection Act 1998 (the DPA); and

• the ways that data controllers can produce clear, effective and engaging privacy notices.

By providing explanations, examples and advice on how to produce effective and engaging privacy notices, 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.

This consultation was undertaken before the outcome of the UK's referendum on its membership of the European Union. As such, a large percentage of respondents' submissions focused on what the major issues are in relation to the upcoming EU General Data Protection Regulation (GDPR). We have tried to ensure that the code will be helpful to data controllers in complying with the transparency requirements of both the DPA and the GDPR, and we have included an annex in relation to the GDPR specifically.

Comments received in response to consultation questions

Below is a summary of the major themes that we have identified in relation to each ICO consultation question.

1. How clear do you find the code?

The majority of respondents found the code clear and to a lesser extent, very clear. However, there were a few recurring themes that respondents felt would make the code clearer.

The first point raised was that the code assumed too much knowledge on the part of its audience. It was considered that the code was understandable for a person well versed in the DPA, but for what could be termed the lay person, some of the terminology was not clear. This related mainly to the techniques described in the code, such as just-in-time notices and dashboards. Following on from this, there were suggestions that a glossary of terms would be a useful addition to the code.

A further point was that some respondents felt the code needed to be clearer on what were the mandatory requirements for a privacy notice and, similarly, what was the minimum required. Respondents felt the code could be more direct in outlining what data controllers are required to do.

A connected point was raised by other respondents, who said that the code should make clear which information should go into which layer of a layered privacy notice.

Respondents felt that it would make the code clearer if the good versus bad examples that are in the currently published version of the code, were re-introduced. It was felt that these were useful for those who use paper privacy notices and as an illustrative tool.

Other points that respondents suggested to make the code clearer included providing sector specific examples and not quoting a large amount of the legislation in the body of the code.

2. In your view, what are the main issues arising from the GDPR that this code should address?

A large percentage of submissions focused on this question, particularly as this consultation ran before the result of the referendum on the UK's membership of the European Union.

The main issue was the further requirements under the GDPR about what information must be provided in a privacy notice (ie those requirements listed in Articles 13 and 14 GDPR). Concerns were raised about having to provide this extra information while meeting

the GDPR requirement for conciseness and clarity. These were seen as conflicting requirements.

In relation to the GDPR, some respondents raised the issue of having to explain the legal basis of a data controller's processing, in particular where the processing condition was legitimate interests. Respondents felt that this required further explanation.

Similarly, the issue of consent as the basis of processing under the GDPR was raised as an issue, with particular focus on the requirement placed on data controllers to be able to evidence consent from data subjects and how to do this.

Respondents also felt that detail would be needed on explaining retention and international transfers within privacy notices under the GDPR.

3.

    a. Aside from issues arising from the GDPR, do you think that all relevant topics (including technological developments) are covered?

    b. Are they covered in enough detail?

    c. Is there any further information you feel the code should include?

Most respondents felt that the code covered all the relevant topics and did so in sufficient detail.

However, some respondents felt that there could be more detail about paper privacy notices and privacy information provided verbally. Respondents suggested, in relation to the paper notices, that the reintroduction of the good versus bad paper examples (also discussed above) may help to address this issue.

Some respondents also felt that the code could address in more detail how to produce privacy notices where the personal data was gained by observation or by inference or where the relationship between data controller and data subject were different, for example, in an employer/employee relationship.

4. **How helpful do you find the new approaches described in the code for example, just-in-time notices, use of icons and symbols?**

On the whole, respondents did find the new approaches recommended in the code useful and a sign that the ICO was

making an effort to engage with developments and encourage data controllers to produce better privacy notices. In particular, just-in-time notices and the privacy notice generator were viewed favourably. The generator was considered as particularly useful for SMEs.

The predominant issue for respondents was the use of icons in the new approaches. Although the majority of respondents felt that icons could be an effective tool for providing privacy information, they also felt that they must be standardised to be effective – either by the ICO, by UK government or by the EU. Respondents felt that without standardisation, icons would neither be taken up by organisations nor be effective if they were taken up.

The other recurring view was that the new approaches, although useful on a whole, may not be very clear or understandable for vulnerable individuals and those with impairments, if the data controller deploys several of these techniques as part of their privacy information.

5. **Do you see any barriers for you, to putting the code's advice into practice? If so, what are they?**

The major barriers that respondents identified were the cost of implementing the suggested techniques within the code (this was mainly SMEs and those other organisations with greater budgetary restraints); the appetite within an organisation to implement these changes; and, the technological capability to implement the changes.

6. **How clear is the explanation of what to consider when providing privacy notices on smaller screens (eg on mobile phones and tablets)? If you think it can be improved, please provide details.**

Respondents were generally happy with the explanation and detail provided about privacy notices on smaller screens.

One point raised was that use of the suggested techniques may be effective on smaller devices but may be affected by data usage or bandwidth/signal availability. It was felt that this issue could be explained in more detail.

Also, that the ICO should recommend the use of zoom functionality on smaller devices, as people are used to this and it would not hinder their experience.

7. **Do you think there are any contradictions between the advice provided in this code and other information published by the ICO? If so, please provide details.**

The vast majority of respondents did not identify any contradictions between the code and other information published by the ICO.

Some respondents felt the code's suggestions about the level of detail required in relation to consent and sharing personal data were written as if they were requirements. It was suggested that this was in contrast to the ICO's Direct Marketing guidance, which made clear that these were just good practice suggestions.

8. **Is the code of practice easy to use and navigate as a webpage document? Are there any improvements or changes that you would suggest?**

No issues were raised about the ease of use of the Code as a webpage and its navigability.

Part B – Additional resources and tools

1. **An online privacy notice generator**

2. **Examples of just-in-time privacy information for websites and mobile apps**

3. **An example of a layered privacy policy**

4. **An example of an online video to complement a privacy policy**

5. **An example of dashboard tool**

6. **How useful would these proposed tools and resources be to you? Would you use it to help produce your own privacy notices?**

Respondents were generally supportive of a privacy notice generator and indicated it would be particularly useful for SMEs.

Respondents felt that examples of all of the above would be useful additions to the code, and a large number of respondents felt that these examples would be useful in helping them produce their own privacy notices (where they would be capable of incorporating these tools).

The only issue raised related to the point noted above about the need for standardised icons.

List of respondents

Association for Financial Markets in Europe and the British Bankers' Association (joint response)
Association of School and College Leaders
Bates Wells Braithwaite LLP
BBC
BCS, The Chartered Institute for IT
BMW Financial Services
Callcredit Information Group
Citizens Advice Bureau
Cornwall Council
Craven District Council
The Direct Marketing Association
Ernst & Young LLP
Finance and Leasing Association
The General Medical Council
The Guinness Partnership
Internet Advertising Bureau UK
ISOS Housing Limited
Lawyers in Charities
Leeds City Council
Lewis Silkin LLP
LexisNexus
London Borough of Barnet
Manchester City Council
Market Research Society
Mydex CIC
News UK
NHS National Services Scotland
North Wales Information Governance Group
NSPCC
Office of the National Data Guardian
Opt-4
Pact
Principality Building Society
Royal College of Physicians
The Scottish Government
Sky
Society of Computers and Law
South Devon and Torbay Clinical Commissioning Group
Southampton University

Standard Life
Travers Smith LLP
Walgreens Boots Alliance – Boots UK and Republic of Ireland
Webtrends
Western Sussex Hospitals NHS Foundation Trust
Zurich Insurance Plc
Six members of the public and two unnamed individuals