Comments on the Draft Marketing Code of Practice; [redacted]

The code is far too long and is not structured properly. I suspect you have captured all the information you need to present to data subjects, but it needs to be presented in a way that is more manageable for the reader. I have identified several problems below (the more important ones highlighted).

THE SUMMARY

1. Profiling summary should state that profiling with personal data for a marketing purpose usually requires consent. "Explicit consent" is required if special category of personal data are used for marketing profiling. (Note**: I think your document has focused on the right not to be profiled in A.22 and not referred to the right to object to marketing profiling in A.21(2)** – these are separate rights and you don't need to rely on the A.22 requirement (not to be profiled), which to apply, has to have significant impact on the data subject).

2. With respect to data enrichment, you should state that there is no need for data enrichment if the data subject has objected to marketing. If the data subject objects, then the enrichment data should be deleted and the data minimisation principle requires the retention of sufficient personal data to manage a suppression list.

3. The summary should include a summary of the key qualities of consent, opt-in; legitimate interests and opt-out. **Summary should state that opt-out and pre ticked opt-in boxes are not consent**.

4. "Individual rights" summary paragraphs should include the right to withdraw consent at any time. Also state that, if exercised, marketing should stop usually within 1 month (see A.12).

5. "Selling or sharing data" summary should also state that the marketing purpose would usually require consent of the data subject (e.g. for third party marketing) and only in exceptional circumstances legitimate interests.

6. "Sending direct marketing messages" summary should state that email addresses and telephone numbers are very likely to be personal data so both the PECR and GDPR marketing rules apply.

OTHER COMMENTS

7. Page 13: Section 122(5) of the DPA2018 states that the definition of "direct marketing" relates to Section 122 **only** (and the Code); is this a problem? Could a marketing organisation argue that the definition of direct marketing does not apply in general (i.e. beyond S.122). Can you rely on that extension?

8. Page 17 uses "opt-in" for the first time. You should expressly define what you mean by "opted in" (e.g. tick the box if you want it to happen). Otherwise it is left hanging whether the return of a prominent unticked opt-out can be equated with an "opt-in". My own view is that I can live with "opt-out" equating with consent: (See "*Marketing by opt-in, opt-out, consent or legitimate interest? Consider your ABC*" on

https://amberhawk.typepad.com/amberhawk/2016/05/marketing-by-opt-in-opt-out-consent-or-legitimate-interest-consider-your-abc.html).

9. Page 23 marketing/service difference. The example with GP should **EXPLICITLY** compare the marketing message ('*Our flu clinic is now open. If you would like a flu vaccination please call the surgery on 12345678 to make an appointment*") with a service message for flu jabs ('*Our flu clinic is now open. This is a reminder that you qualify for a priority flu vaccination: please call the surgery on 12345678 to make an appointment)*. **I am concerned that some OAPs who need their flu jabs will not get the message if they opt out of marketing and GPs get your advice wrong**.

10. Page 33: There is no equation of Article 6 "consent" with "opt-in" until you get to the text at the bottom of page 33 ("Pre-ticked opt-in boxes are banned under the GDPR. You cannot rely on silence, inactivity or default settings – consent must be separate, freely given, unambiguous and affirmative. Failing to opt-out of direct marketing is not valid consent" – **should be much more prominent (e.g. in the summary)**.

    You should have a prominent section titled "**Consent and opt-in or opt-out**" – perhaps also in the Summary. Also you must stress that it is easy to withdraw consent with respect to Online advertising and new technologies (**as often this does not happen**).

    Similarly the provision "*You must make it as easy to withdraw consent to direct marketing as it was to give it*" (page 33) is very important and **should not be buried in the text**. Many sites that get consent for cookies do not easily allow withdrawal of consent. So if there is a website where people sign up to marketing, that part of the website should also allow people to stop marketing. **This message should also appear on page 85 re cookies**.

    In general, the ICO should consider enforcing this requirement (i.e. from the data subject's perspective, it is easy to give consent as to withdraw it) as it avoids **any debate as to what consent means in practice** (for example, how many websites requires consent to get on the website (it is easy to consent) but at the same time makes it difficult to withdraw consent).

11. Page 34: the statement under "Specific and informed" that refers to "third party **controllers**" has an **error**; the third party does not need to be a controller – so "controllers" needs to be removed.

12. Page 34: *How does legitimate interests apply to direct marketing*?. I think you can explain that legitimate interest for marketing can apply when obtaining consent for direct marketing is impracticable (e.g. controller transfers from the public sector to the private sector) as per British Gas Trading Tribunal under the 1984 Act. Can you consider the arguments about legitimate interest half way through my blog on: https://amberhawk.typepad.com/amberhawk/2016/05/marketing-by-opt-in-opt-out-consent-or-legitimate-interest-consider-your-abc.html).

    The text here under legitimate interests conflates PECR with the GDPR. Do you mean this? For instance an email address is personal data. Are you saying that if a controller uses the "soft-opt in" to obtain an email address (PECR), that controller can rely on "legitimate interests" under the GDPR?

This is important because your ICO documentation on https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/02/dma-data-protection-2018/ quotes the Commissioner saying the opposite: *"Detail of the e-privacy regulation is still being debated, but a default for all consumer marketing to be opt-in is in the current draft.* ***Until the e-privacy regulation comes into force, PECR will sit along side the GDPR. That means electronic marketing will require consent".***

If you have changed your mind, you should state this clearly

You should add that the text omits the argument that the "*legitimate interest of the data subject*" arises as there is an ***absolute*** right to object to the processing of personal data for a marketing purpose. Marketeers who rely on "*legitimate interests*" should be able to justify marketing under this lawful basis (e.g. may need to demonstrate why data subject consent was inappropriate and how they provided information about exercising the right to object to marketing at the time of collection).

13. Page 38 text "*In practice the only condition available for processing special category data for direct marketing* purposes *is 'explicit consent'*. First, can you use the correct term "special category of personal data" for "special category data". As you state that explicit consent is the ONLY option**, you need to debunk the argument that the special category of personal data was not "*manifestly made public by the data subject***" (e.g. a woman who announces that she has the flu on Facebook and this is scraped up by marketeers). The Glossary should also have the correct term (special category of personal data).

14. Page 39: The explicit consent text (top of page) omits the fact that it has to be as easy to withdraw consent as to give it. Also, on page 39, are you correct to state that a collection of personal data cannot be special category of personal data? Suppose I have a list of email addresses of HIV patients; these are **not** special category of personal data according to your text. Yet, under the DPA1998, the ICO fined health bodies for using an email list CC: rather than BCC: (see https://www.bbc.co.uk/news/technology-36247186 and https://www.theregister.co.uk/2016/05/09/london_nhs_trust_fined_180000_by_ico_over_hiv_newsletter_breach/). **You need to be clear if there has been a change of policy, as your statements here may be used to state that the ICO has provided conflicting guidance on the issue.**

15. Page 52: use of public information. You need to cover off the collection of special category of personal data in the public domain (see comments on page 38; para 13 above).

16. Page 56 etc. **The text focuses on A.22 (e.g. bottom of page 58) and not A.21 (which is better for you).** In addition, although you infer that explicit consent is only needed for special category of personal data (middle p57) mainly because direct marketing is assumed not to have a significant impact on the data subject, I would not be so absolute. I would argue that to the use of confidential personal data for a marketing purpose requires consent to make it lawful under Principle in A.5(1)(a). ("*However, processing may also be unlawful if it results in: a breach of a duty of confidence*") https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/.

You could say "usually there is no significant legal impact" from direct marketing so there is no prohibition in A.22 but then add the requirement in A.21(2) includes the right to object to profiling for a marketing purpose and this in turn means that the profiling has to be fully explained to the data subject (and consent usually obtained).

Data enrichment could involve confidential personal data could also require consent**. In general, the use or disclosure of confidential personal data does not appear in the Code; this is important, as in the absence of consent, the use or disclosure of confidential personal data can breach that confidence and constitute unlawful processing (according to your general guidance quoted above). You should state that marketing based on "legitimate interest" using confidential personal data is unreliable.**

17. Page 59: linking statistical data with personal data can be an offence under S.171 of the DPA2018. **Can the Code alert readers to the need to check whether they can re-link statistical data with personal data.**

18. Page 67: The "**must**" in the following statement is wrong: "*If you want to call a number registered with the TPS or CTPS you must have the subscriber's consent in order to override their general objection to direct marketing calls*." The rule in PECR is an "unsolicited marketing" rule which is not a consent rule. Change "you must" to "it is best practice".

19. Page 74: I would replace the text "….*describe the exception to the consent requirement of Regulation 22*" with "….*describes an alternative to the consent requirement of Regulation 22*".

20. Page 73: Can you add to the jeans example (top of page) that would correct the example. Something on the lines of: "*if you ask a customer, when they pay for a product 'would you like a copy of your invoice emailed to you?'*" you should also ask at the same time "*do you want your email address to be part of our marketing lists so you can receive details of our own similar products*" and establish a procedure to store the emails of objectors on a suppression list.

21. Page 82: "*Can we use third parties to send our direct marketing*?.

    As Third Party is a GDPR defined term, I think you need to make sure that the text specifically states that it **does not apply to use of "processors" as defined by the GDPR**. You could explain that in data protection terms a "Third Party Supplier" (e.g. someone who manipulates a list for you) is often parlance for "a processor".

    For example, the text you use on p82 ("you provide a third party with the contact details of your customers and ask them to do it on your behalf") is a "processor" relationship and not a "third party" (if the processing is on behalf of the controller).

    Similarly on page 26: "Are we responsible for compliance? , you use the text "third party" the draft code states "However it is common in the direct marketing context to work with third parties and this can be beneficial to you – but you do need to ensure that your collaboration with others is compliant with the GDPR and PECR". This is followed by several paragraphs of text that relates to processors (and not Third Parties as defined in the GDPR).

In general, there is likely to be confusion between third party supplier (processor) and GDPR Third Party (the Third Party definition is missing in the glossary).

The problem you have is that if you enforce Third Party Marketing (which requires consent) the defence may point to the above confusion in your Code (i.e. "*if the ICO cannot get it right, what hope does a normal controller have?*")

22. Page 88-89: "What do we need to know if we use cookies and similar technologies for direct marketing purposes?" **Can you remind the readers: "*Marketing organisations have to provide for the right to object to direct marketing*" and "*they have to make it as easy to give consent as to withdraw it*"**. And provide meaningful, accessible and clear information as to how to exercise these rights (as per A.12).

23. Page 90; "*Can we target our customers or supporters on social media*?" Can you add a reminder about the use of special category of personal data requires "explicit consent" and make reference to debunking the "*manifestly made public by the data subject*"? point (see para 13 above).

24. Page 113: suppression list. Could add (to the fact that a controller can retain the personal data for a legal obligation in a suppression list) that it is also in the legitimate interest of the controller to comply with the right to object to marketing.

25. Editorial comment re definitions: Can you check on the use of "data" and whether it should be replaced by "personal data" (i.e. check whether the word "data" could carry the inference that the information is NOT personal data and not subject to the GDPR). Also there are a few (about 6) references to "data controller" in the text. Special category of personal data – use the correct term. Conflation of processor and third party – please resolve