MACMILLAN
CANCER SUPPORT

ICO Direct Marketing Code of Practice Consultation – Draft Response

Q1: Is the draft code clear and easy to understand?

Overall, the Code is clear and easy to follow. However, there are several points where we feel greater clarity would be useful:

a) Status of the Code

Page 3 of the Code states that:

"This is a statutory code of practice prepared under section 122 of the Data Protection Act 2018".

Pages 6 and 119 of the Code states that:

"If you do not follow this code, you will find it difficult to demonstrate that your processing complies with the GDPR or PECR"

However, on **page 10** it says

"The code contains practical guidance on how to carry out direct marketing fairly and lawfully and how to meet your accountability obligations". It does not impose any additional legal obligations that go beyond the requirements of the GDPR or PECR but following the code will ensure you comply with those obligations. It also contains some optional good practice recommendations which do not have the status of legal requirements but aim to help you adopt an effective approach to data protection compliance".

It is our understanding that if, while conducting direct marketing, organisations can identify alternative ways of complying with the GDPR and PECR to the practical guidance set out in the Code then this would be acceptable. Can you please confirm if that understanding is correct?

It would be helpful to know if a) it is mandatory to comply with the practical guidance set out in the Code or b) the Code is instead a set of best practice guidelines with which organisations OUGHT to comply.

b) Online advertising and new technologies

Page 5 of the Code says that:

"Individuals are unlikely to understand how you target them with marketing on social media so you must be upfront about targeting individuals in this way".

However, there is no further clarity provided on what would constitute "upfront" in the eyes of the ICO so some practical examples would be helpful.

c) How do we decide what our lawful basis is for direct marketing?

In the table on **pages 30 - 31** the Code states that, under PECR, organisations do not need to get consent for *"emails/texts/in app/in-platform direct messaging to individuals - obtained using soft opt in"*. However, it is not made clear that this soft opt in rule does not apply to fundraising-related direct marketing until later in the Code.

It is therefore possible that a charity could unintentionally overlook the different soft opt in rules for corporations and charities, so it would be beneficial to make those differences clearer in the table itself in the interests of consistency.

d) How does consent apply to direct marketing?

Page 33 of the Code outlines what is required to secure specific and informed consent. It says that, "where possible" consent requests need to cover the purposes as well as the types of processing activity for which you need to provide "granular consent options for each separate type of processing".

However, the Code does not clarify what the difference is between "purpose" and "type" – it would be useful if clearer definitions perhaps with an example that would be clear and easy for the average person to understand could be provided. Also, are there circumstances where an organisation could make a case that is was not possible to provide granular consent options? e.g. where there are IT limitations?

e) Can we use profiling to better target our direct marketing?

Page 58 of the Code says:

"It is unlikely that you will be able to apply legitimate interests for intrusive profiling for direct marketing purposes. This type of profiling is not generally in an individual's reasonable expectations and is rarely transparent enough".

However, it is not made clear what the ICO would consider to constitute "intrusive" profiling and a more detailed definition is needed. It would also be helpful to be given examples of what the ICO considers to be "unintrusive profiling".

f) Direct marketing by post

On **page 66**, the ICO makes the following good practice recommendation about screening data against the Mailing Preference Service (MPS):

"However, we recommend that you screen individual's names and addresses against the mail preference service (MPS) prior to sending out the direct marketing".

The ICO however does not confirm whether this applies to warm (i.e. existing contacts) or cold (i.e. new contacts) lists. The MPS website says *"you can expect to continue to receive mailings from companies with whom you have done business in the past"* which suggests that the service does not apply to marketing lists compromised of existing customers.

It would be helpful if the Code could provide more clarity on this point.

g) How does direct marketing using social media work?

Page 90 of the Code says that:

"...targeted advertising on social media does not fall within the definition of electronic mail in PECR".

However, the Code does not clarify whether social media platforms can rely on consent or legitimate interests to target their users with direct marketing appearing, for example, in newsfeeds. It would be helpful if the Code could provide more clarity on this point.

Q2: Does the draft code contain the right level of detail? (When answering, please remember that the code does not seek to duplicate all our existing data protection and e-privacy guidance)?

Overall, we feel that the Code is detailed and thorough, providing the right amount of information required to comply with the ICO's requirements. However, we also think that more detail could be provided in the following areas:

a) Sending direct marketing messages

Page 5 of the Code says:

"The electronic mail "soft opt in" only applies to the commercial marketing of products and services, it does not apply to the promotion of aims and ideals".

We are concerned that there is a not a level playing field between commercial enterprises and charities within the context of the soft opt in rule and would welcome some more information in the Code for the reasons why such a distinction has been made. Although we note that the soft opt distinctions are not new, guidance on the ICO website does not explain why they exist in the first place.

b) Direct marketing of "similar products and services"

Page 75 of the code states this requirement for use of the "soft opt-in" for marketing similar products and services.

"In the course of a sale or negotiation of a sale of a product or service"

Page 78 of the code states that "soft opt-in" only applies to when an organisation is marketing similar "products and services". In the context of the charity sector, it provides an example of someone buying tea through a charity's online shop. It says that because the individual has not opted out of further shop-related marketing during that transaction, the charity can send them future marketing emails about products in the shop.

However, the code does not provide any guidance about whether it would be possible to promote specific charity shop products which are directly related to, for example, a fundraising event that someone has signed up to. Would such a promotion within that context count as a service message?

Further clarity about the status of shop-related marketing in the context of fundraising event-related stewardship communications would be welcomed.

c) What type of "communications" are covered?

Page 16 of the Code says:

"Online behavioural advertising and some types of social media marketing are not classed as electronic mail under PECR but these are still direct marketing messages".

Some examples of what type of social media marketing are not classified as electronic mail would be useful.

d) What are service messages?

On **page 19** of the Code, the ICO provides an example of what would constitute a service message from a credit card provider which is useful for the commercial sector. However, many charities send thank you correspondence to supporters for donations setting out how their donation has helped – it would therefore be helpful if the ICO could also provide an example of what would constitute a service message from a charity or not-for-profit and what would cross the line into direct marketing.

For example, would providing the following examples constitute services messaging?

- letting a supporter know that they can gift aid their donation in an acknowledgement letter

- mentioning in a services email about an event that there's a free cancer support line available to members of the public. This is an obvious benefit to anyone affected by cancer and we consider it would be potentially detrimental if a charity could not highlight the existence of a free support line that might be able to help with their situation.

- sending an email with hints and tips for raising more money to someone taking part in a fundraising event

We are sure that additional clarity on this subject would be welcomed by many charities and not-for-profits.

e) How do we tell people that we want to use their data for direct marketing?

Pages 50 -51 of the Code provides an example of a charity providing inadequate information about its use of wealth screening in its privacy information. It would be helpful if the ICO could provide another example of what it would consider to be sufficiently transparent information so that charities who do conduct wealth screening can ensure that they are providing the right level of detail to their supporters.

f) Direct marketing by electronic mail (including emails and texts)

Page 74 of the Code says:

"If you use "tracking pixels" within your direct marketing emails, then you need to be aware that:

- *regulation 22 applies to the email itself; and*
- *If the pixel involves storing information, or accessing information stored, on the device used to read the email – such as its location, operating system etc – then PECR's rules on cookies and similar technologies (Regulation 6) will also apply".*

We understand this to mean that organisations will need to have consent for email pixel tracking. There are obvious impracticalities involved in securing consent within this context because, as far as we are aware, no email service providers offer that functionality. In addition, the ICO appears to be relying on legitimate interests to track user interactions with its own enewsletter.

With that in mind, it would be helpful if the Code could provide an example or some guidance on how organisations can practically secure consent for email pixel tracking.

g) Business to business marketing

Page 81 of the Code says:

"Assuming PECR does not require consent, in many cases it's likely that legitimate interests will be the appropriate lawful basis for processing individuals' personal data in their business capacity for direct marketing purposes".

It would be useful if the Code could provide some specific examples for when PECR does not require consent. It is our understanding that, except for sole traders, legitimate interests can be relied upon to send business contacts direct marketing emails.

Q3: Does the draft code cover the right issues about direct marketing?

We are satisfied that the draft Code covers the right issues about direct marketing, however (as outlined in answers to previous questions), we believe that more detailed information could be provided about profiling, service messages and digital advertising.

Q4: <u>Does the draft code address the areas of data protection and e-privacy that are having an impact on your organisation's direct marketing practices?</u>

Yes

Q5: Is it easy to find information in the draft code?

Yes

Q6: <u>Do you have any examples of direct marketing in practice, good or bad, that you think it would be useful to include in the code?</u>

Yes, although as outlined in answers to previous questions, we believe that there should be more examples of good practice to help organisations to comply with the Code's requirements.

Q7: <u>Do you have any other suggestions for the direct marketing code?</u>

There are some areas of the Code that we feel need to be reconsidered or, alternatively, additional clarity needs to be provided as follows:

a) How do we decide what our lawful basis is for direct marketing?

Page 4 of the Code states:

"If you are carrying out solely automated decision making, including profiling, that has legal or similarly significant effects on individuals then there are addition [sic] rules in the GDPR that you must comply with."

It would be helpful if the ICO could provide examples of what would constitute "significant effects" in the context of profiling and what would not.

Page 4 of the Code also states:

"If you use non-personal data such as assumptions about the type of people who live in a particular postcode to enrich the details you hold about an individual it will become personal data."

It would be useful if the ICO could provide some specific examples to help illustrate this point.

b) How do we decide what our lawful basis is for direct marketing?

Page 31 of the Code outlines the following "Good practice recommendation";

"Get consent for all your direct marketing regardless of whether PECR requires it or not".

In the past, the ICO has been careful to highlight that consent and legitimate interests are both equally valid legal bases to rely on for certain types of direct marketing.

We are concerned that this prescriptive good practice recommendation could lead to confusion and lead to organisations concluding that they <u>must</u> get consent for all types of direct marketing when legitimate interests is a valid alternative providing that appropriate due diligence (i.e. the three-part test) has been conducted and is met.

We consider that such a recommendation goes beyond what is required in law and should be removed.

c) Can we use special category data for direct marketing?

Page 39 of the Code says:

"If you are profiling for direct marketing purposes on the basis of special category data, you need explicit consent for that profiling – including drawing inferences about people's likely race, ethnicity, politics, beliefs, health or sexual orientation from other data".

It is our understanding that making **inferences** about someone's likely characteristics is not the same as processing data relating to people who **definitively** have those characteristics. It is our understanding that just because an individual, for example, looks at cancer-related information on a website (or indeed searches for cancer-related information through a search engine), does not mean they have cancer. To put this in another context, it would not be possible to definitively conclude that because someone visits a website about a specific religion, that they're a follower of that religion.

Health organisations cannot make inferences that ALL visitors to their website have a particular health condition because it will be evident that many people visiting health websites are friends and relatives of people who are unwell, medical professionals, people who are concerned that they might have a particular condition etc.

On that basis, there needs to be some recognition in the draft Code that the situation with online tracking is more nuanced than the current draft wording implies.

d) Online advertising and new technologies

The "At a glance" section on **page 85** says:

"Individuals are unlikely to understand how you target them with marketing on social media so you must be upfront about targeting individuals in this way".

This statement does not recognise that there are distinct differences between the purposes and uses of social media platforms which will inevitably impact on the expectations of their users. For example, LinkedIn is a professional networking platform so users would be more likely to expect information about their employment status and work experience to be scrutinised than, say, Facebook users which is predominantly more of a social platform.

The lack of acknowledgement of the nuances relating to different social media platforms has the potential to have a damaging impact on online fundraising appeals.

e) How does legitimate interests apply to direct marketing?

Page 36 of the Code states:

"Given that individuals have the absolute right to object to direct marketing, it is more difficult to pass the balancing test if you do not give individuals a clear option to opt out of direct marketing when you initially collect their details …"

This seems to imply that it would be impossible to pass the balancing test when using legitimate interests as a lawful bases for direct marketing by post and telephone unless organisations provide opt out tick boxes at the point of data collection. This has the potential to cause unnecessary confusion for members of the public and it is our understanding that when collecting personal details organisations can rely on legitimate interests as a lawful basis for direct marketing by post and phone so long as they provide information about how they can opt out.

f) How long should we keep personal data for direct marketing purposes?

Page 42 of the Code states:

"When sending direct marketing to new customers on the basis of consent collected by a third party we recommend that you do not rely on consent that was given more than six months ago."

We understand this requirement relates to data that are purchased from third-party **list brokers** as opposed to third party **agencies** (e.g. a telemarketing agency) acting on an organisation's behalf to collect consent for future direct marketing.

Because the agency is the representative of the organisation making the consent request and is therefore required to use that organisation's specific consent statement, we understand that consent secured through third-party agencies can be used for longer than six months.

g) Can we use profiling to better target our direct marketing?

Page 58 of the Code states that profiling poses "significant risks to the rights and freedoms of individuals because *"it might perpetuate stereotypes; or cause discrimination."* To help illustrate this point, it would be helpful if the Code could provide some specific examples about how profiling could lead to stereotypical or discriminatory decisions being made to help organisations avoid this.