Information Commissioner's Office

Consultation:

Direct Marketing Code

Start date: 8 January 2020

End date: 4 March 2020

Introduction

The Information Commissioner is producing a direct marketing code of practice, as required by the Data Protection Act 2018. A draft of the code is now out for public consultation.

The draft code of practice aims to provide practical guidance and promote good practice in regard to processing for direct marketing purposes in compliance with data protection and e-privacy rules. The draft code takes a life-cycle approach to direct marketing. It starts with a section looking at the definition of direct marketing to help you decide if the code applies to you, before moving on to cover areas such as planning your marketing, collecting data, delivering your marketing messages and individuals rights.

The public consultation on the draft code will remain open until **4 March 2020**.The Information Commissioner welcomes feedback on the specific questions set out below.

You can email your response to directmarketingcode@ico.org.uk

Or print and post to:

Direct Marketing Code Consultation Team
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

If you would like further information on the consultation, please email the Direct Marketing Code team.

Privacy statement

For this consultation we will publish all responses received from organisations except for those where the response indicates that they are an individual acting in a private capacity (eg a member of the public). All responses from organisations and individuals acting in a professional capacity (eg sole traders, academics etc) will be published but any personal data will be removed before publication (including email addresses and telephone numbers).

For more information about what we do with personal data please see our privacy notice

Q1 Is the draft code clear and easy to understand?

☐ Yes

☒ No

If no please explain why and how we could improve this:

1. **Extension of the 'electronic mail' definition under PECR to include in-app and direct social media messaging**

- Under this draft Code, there is clearly an extension from what was classed as 'electronic mail' under current ICO guidance (please see extracts below) to now include direct social media messages and in-app marketing messages.
- Whilst it is appreciated that the growth in social media and in-app messaging is something that is not currently directly regulated, it is not clear how the definition of 'electronic mail' can be extended to include these two channels without the definition itself being amended under the legislation.
- Under Regulation 22 PECR *"'electronic mail' means any text, voice, sound or image message sent over a public electronic communications network which can be* ***stored in the network or in the recipient's terminal equipment*** *until it is collected by the recipient and includes messages sent using a short message service"* [emphasis added]
- We understand 'the network' (not defined under PECR) to mean the general internet network.
- Direct messages via social media platforms and in-app ads are not *"stored in the network or in the recipient's terminal equipment".* Both ad channels work by the sending of a message to the ad server (such as Facebook/LinkedIn) and an ad capture being sent back and displayed either on the social media platform or in the app.
- We feel it would be beneficial to instead distinguish 'in-app ads' from '**push notifications'**. The latter are sent to someone's device, so are *"stored…on the recipient's terminal equipment*", thereby meeting the definition of 'electronic mail'. Yet, they are not included by the ICO as 'electronic mail' (see page 95 of the Draft Direct Marketing Code) or otherwise captured under the draft Code.
- We also feel the draft Code should be clear as to who would be responsible for meeting the requirements – the social media platform which delivers the ad or the publisher, and if the latter, how they would go about obtaining the 'soft opt-in' or consent given they do not hold the direct relationship with the individual.

Extracts from the ICO's Guide to the Privacy and Electronic Communications Regulations (as updated May 2018): https://ico.org.uk/media/for-organisations/guide-to-pecr-2-4.pdf

What kinds of electronic marketing are covered?
PECR cover marketing by phone, fax, email, text or any other type of 'electronic mail'.
There are different rules for live calls, automated calls, faxes, and electronic mail (this includes emails or texts).

PECR marketing provisions do not apply to other types of marketing, such as mailshots or online advertising. However, you must always still comply with the Data Protection Act and the GDPR; and if your online advertising uses cookies or similar technologies, the provisions about cookies may apply. [Page 14. Note: current guidance expressly excludes online targeted ads].

How do these rules affect apps?

Apps store information on smart devices, and some apps may also access information on the device (eg contacts or photos). App developers should therefore provide clear information to users about what the app does, and exactly how it uses their information, before users click to install the app. It is also important to consider user privacy controls and avoid switching optional features on by default. This ties in closely with the requirements of the Data Protection Act and the GDPR. [Page 33, Note: current guidance leaves it to the app developer to determine how the rules apply in line with how they deliver the app and use information taken from/delivered to it.]

2. The requirement to comply with Regulation 6 PECR when using cookies/similar technologies as part of in-app and email marketing

- It is not clear from the draft Code as to when and how the ICO anticipates consent to cookies and similar technologies, when used within in-app or email marketing, should be obtained.
- Pages 74 and 95 of the draft Code detail the requirement with reference to Regulation 6 PECR.
- Whilst it is appreciated that consent is needed where such cookies/similar tech meet the requirement under Reg 6, it is operationally impossible to collect such consent **before** the message is delivered containing the relevant cookies/similar tech.
- A solution could be to recognize that there are two types of cookies used in emails/SMS: a) include in the email/app ad such due notice and acknowledgement that by clicking on the hyperlink within the message the user is agreeing to the use of such cookies/similar tech in line with Reg 6; and b) recognize that analytics cookies (which measure open rates etc) could be deemed as 'strictly necessary', not require consent under Reg 6 PECR, and arguably be within the 'legitimate interests' under GDPR of the sender, much like the ICO view first party analytics cookies under their cookie guidance issued July 2019 (https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf).
- Practical examples demonstrating how consent could be obtained would be helpful additions to the draft Code to aid the practical implementation of what the ICO have in mind with this new requirement.

3. The ICO's position that data tracing activities are unfair unless the individual has expressly said it is ok (page 61 of the draft Code)

- Whilst we agree with the need to seek consent or other appropriate permission for the use of certain contact details for direct marketing purposes, in line with legislation, we believe this does not preclude us from proactively keeping those contact details up to date.
- The proactive updating of individual's contact details, for instance where they have moved house, is: (a) in the individual's interests (we cease sending them information to an old address); (b) in line with the 'accuracy' principle (i.e. *"every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay");* and (c) that the personal data is kept *adequate* and *relevant* in line with the 'minimisation' principle under Article 5 GDPR.
- The individual has the means to ask us to cease using their personal data for marketing purposes at any time, so the protection and control over their personal data is not diminished.
- We ask that this point is reconsidered in the context of maintaining up to date records.

4. The ICO's position that if direct marketing is not necessary for the performance of a service or contract then consent to such marketing activity will be invalid as it is not freely given (page 37 of the draft Code)

The draft Code gives the examples of a retail loyalty scheme as being likely to be able to show that direct marketing is necessary for that service, but that a points-based loyalty scheme would not. There is also an example of free wifi being available on a train, where the rationale for any marketing consent being mandatory when signing up for the free wifi is that *"it is not necessary for the train company to collect these details for direct marketing purposes in order to provide the wifi, therefore the consent is not valid"* (page 37 of the draft Code).

a) The distinction between retail loyalty schemes and points-based loyalty schemes

- This appears to overlook the fact that the underlying principle for both is the same – which is: a data exchange happens, regardless of the service, to allow for direct marketing activity.
- It also appears to contradict the position taken further on in the draft Code given a retail loyalty scheme would inevitably bundle the consent as it is part-and-parcel of signing up to their service. *"It is also important to remember that consent must be separate and cannot be bundled into your terms and conditions for the use of your mobile app, unless you can demonstrate that consent for marketing is necessary for the provision of your service."* (page 95 of the draft Code)
- There is also confusion when comparing the draft Code with the ICO's Consent Guidance (9 May 2018). In the Consent Guidance, the description of a retail loyalty scheme allows for money-off vouchers to be acceptable: *"The ICO's view is that it may still be possible to incentivise consent to some extent. There will usually be some benefit to consenting to processing. For example, if joining the retailer's loyalty scheme comes with access to money-off vouchers, there is clearly some incentive to consent to marketing. The fact that this benefit is unavailable to those who don't sign up does not amount to a detriment for refusal. However, you must be careful not to cross the line and unfairly penalise those who refuse consent."* Whereas in the draft Code, the retail loyalty scheme has to be one that is *"operated purely for the purposes of sending people marketing offers."* (page 38 of the draft Code).
- It would be helpful and consistent to align the draft Code with the Consent Guidance.

b) Consent for the use of personal data for direct marketing purposes in exchange for a free service, such as access to free wifi, cannot be considered valid consent

- The GDPR requires that for consent to be valid, it must be freely given (amongst other things). To obtain a free product/service or money off a service/product, in return for providing a consent to direct marketing (provided it does not prevent those not willing to agree to the data exchange still being able to pay or pay full price for the same product/service) does not make the consent unfairly given. The choice and control is still in the hands of the individual and is therefore given 'freely'.
- In fact, by not making this option available, the individual is prevented from commoditizing / monetising their own data.
- This principle applies to a huge number of what we all consider 'free' services today – from online services such as Google search and social media platforms (all of which are not cost-free to the supplier to provide, enhance and maintain), to airmiles and points-based voucher schemes. If you collect points with a retailer, how can they tell you how to redeem them if they cannot send you direct marketing communications?

- We have sought QC advice on this point, extracts of which we share, in strictest confidence but in the interests of transparency and to contribute fully to the consultation, under Annex A to this response.

We welcome a clearer, consistent and practical solution here from the ICO, which empowers the individual to use their data to obtain free/money off products and services. Money-off vouchers, free service access and regular freebies such as a free downloadable film each month, should be considered valid incentives for providing a marketing consent. Individuals should not be denied from being able to commoditize their personal data.

The point of contention should be whether, by saying 'no' to marketing consent, the individual is prevented from accessing the service altogether, i.e. they suffer a detriment - as per the principled approach taken by the ICO in their Consent Guidance.

5. Conflating the legal basis for processing personal data such as consent or 'legitimate interests' under the GDPR with the instances where you need to obtain consent under PECR

- PECR does not account for the concept of having a 'legal basis' for processing personal data. For example, the requirement for consent under Regulation 6 PECR is to *"store information, or gain access to information stored"* (Reg 6(1)) which can include storing or access to non-personal data/information, subject to the exclusions which then follow.
- Therefore the statement at page 31 of the draft Code is not correct – *"If PECR requires consent, then processing personal data for electronic direct marketing purposes is unlawful under the GDPR without consent. If you have not got the necessary consent, you cannot rely on legitimate interests instead. You are not able to use legitimate interests to legitimize processing that is unlawful under other legislation."*
- A context-led approach would be helpful to apply here, as there are instances where PECR consent would apply, for example, which would not automatically mean consent should be sought under GDPR.
- Examples include fraud purposes, and some direct marketing activity, provided the legitimate interests assessment can be met.

6. The [potential] requirement to seek consent specifically for the use of personal data for list-based social media advertising.

- Highlighted as a potential requirement as we acknowledge that the ICO points to the potential to rely on legitimate interests still.
- We feel it is firstly important to distinguish between the different types of list-based advertising when considering the legal basis that should apply. On the Facebook platform these are referred to as Custom Audience versus Lookalike Audience.
- The difference is important. For the Custom Audience version the actual contact data of the individuals is uploaded by the advertiser to be matched on the social media platform – whereby allowing the advertiser to only upload those contacts it has a marketing permission to use that data for, e.g. an email address – the individual to whom the data relates will therefore know the advertiser is using their email address for marketing purposes, an expectation that can be further informed through privacy notices.
- Whereas for the Lookalike Audience option, the advertiser does not have any contact details to upload; they provide a criteria for those individuals they would like the social media platform to target for them. So the advertiser may have no previous contact with the individuals that then receive the ads.

- To introduce a requirement to seek consent for Custom Audience list-based advertising would mean: a) introducing another marketing permission box on sign up, rather than making the consent/permission channel-led (i.e. use of email for direct marketing *per se*), and b) further consideration and clarity in the guidance would be needed as to how that permission would be worded to adequately capture the potential use given the vast number of social media platforms offering such a list-based ad service – e.g. would it be necessary to name the platforms (LinkedIn, Facebook etc) and if so could the permission be 'bundled', or would it be sufficient to just reference 'social media', and what if an individual is a member of one platform but not all (if they were to be listed)?
- We believe the direct marketing rules for social media list-based advertising should be split in approach. For the Custom Audience method, the advertiser should be able to apply the current permission for the contact data 'matched' on the platform, and for the Lookalike method, the social media platform should be responsible for managing the permission of the individual user.
- For the Lookalike method, we can see that Facebook have relatively recently updated their ad transparency (Why Am I Seeing this Ad?) and controls – if these became the norm on social media platforms then arguably this does/could afford the data subject adequate rights and control to block targeted ads from receiving direct marketing from unwanted parties. This could enable the legitimate interests test to be met on a social media-specific basis, which reflects how individuals interact with such platforms (i.e. being a member of one, several or many of them) rather than the publisher being responsible when they don't own the direct relationship in this scenario.

7. If an organization encourages an individual to share details of a promotion or campaign with a friend, the organization is responsible for the processing of the personal data and the sharing of a marketing communication by that individual (page 85 of the draft Code)

- If an individual is encouraged to share-on a message to their friends, the party doing the encouraging does not actually process the friend's personal data in order for the message to be sent.
- The individual, in sending the message to their friend, arguably falls under the 'domestic use' exemption under GDPR.
- It is entirely in the control of the friend to then provide their contact details or otherwise act on the promotion with the organization sending the original message. No action, no personal data about the friend is passed to the organization. So, how can they be responsible for it?

8. Referencing a third party in your marketing activity equates to joint marketing activity (page 28 of the draft Code)

- It is our understanding, that if you obtain consent for marketing activity (in accordance with the standard of consent under the GDPR), then you are not restricted by what you promote, as the consent is specific to the party identified and the data used to conduct the promotion. There is no reference under the Articles and Recitals on consent under the GDPR to the content of the promotional activity.
- However, the example given in the draft Code of a supermarket promoting a charity states: *"Although the supermarket is not passing the contact details of its customers to the charity it still needs to ensure there is appropriate consent from its customers to receive direct marketing promoting the charity. Where possible it would be good practice for the supermarket to screen against the charity's suppression list."*
- We believe this is stretching the rules on consent for marketing beyond what is in scope of the legislation.

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)

☐ Yes

☒ No

If no please explain what changes or improvements you would like to see?

Please see answers to question 1.

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

☐ Yes

☒ No

If no please outline what additional areas you would like to see covered:

Please see answers to question 1.

Q4 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?

☒ Yes

☐ No

If no please outline what additional areas you would like to see covered

We note that there is no reference to the need for all app-related messages to be considered marketing messages – something that was included as a secondary comment in an enforcement action against EE Ltd in June 2019 (paragraph 42 of that enforcement report). Therefore, we take this to mean that we should not consider all app-related messages as marketing messages, as in fact they can be purely service messages.

It is our understanding that linking from a service message to a customer service app or website where the landing page does not include promotional or marketing material is acceptable as a service message. The fact that the website or customer service app more generally includes products / services that a customer can purchase would not breach direct marketing rules provided the customer is not linked or sent directly to that page (i.e. they would need to navigate themselves from the landing page with no promotional material to a sales page).

The ICO also received a letter from Mobile UK on this point (December 2019).

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

- ☒ Yes
- ☐ No

If no, please provide your suggestions on how the structure could be improved:

Q6 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

- ☐ Yes
- ☒ No

If yes, please provide your direct marketing examples:

Q7 Do you have any other suggestions for the direct marketing code?

All covered under the response to question 1.

About you

Q8 Are you answering as:

- ☐ An individual acting in a private capacity (eg someone providing their views as a member of the public)
- ☐ An individual acting in a professional capacity
- ☒ On behalf of an organisation
- ☐ Other

Please specify the name of your organisation:

British Telecommunications plc

If other please specify:

Q9 How did you find out about this survey?

- ☒ ICO Twitter account
- ☐ ICO Facebook account
- ☐ ICO LinkedIn account
- ☐ ICO website
- ☐ ICO newsletter
- ☐ ICO staff member
- ☐ Colleague
- ☐ Personal/work Twitter account
- ☐ Personal/work Facebook account
- ☐ Personal/work LinkedIn account
- ☐ Other

If other please specify:

Thank you for taking the time to complete the survey