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:

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?

The fact that the Code identifies and separates what is best practice from what is a general requirement is helpful.

There is, however, scope for the Code to provide better examples of how consent UXs should be presented in practice. To take an example, few organizations use only one form of marketing tool. The Code identifies numerous marketing practices for which consent is required. However, there is no example in the Code of how a consent UX could be structured for an organization that is using many of these tools and consequently is requesting numerous consents in the same UX.

The Code could also do significantly more to separate out B2B from B2C activities. To give one example to illustrate the point, the comments about buying in email marketing lists are premised on consent being required for email marketing. However. in the UK B2B email marketing does not, in contrast to B2C emails, require consent This section of the guide is therefore overly strict (and legally incorrect) as regards B2B emails. Not all organizations have the resources to seek advice from external counsel and by not separating out B2B from B2C examples the Code will mislead readers.

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:

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

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?

Yes, Bird & Bird LLP held a roundtable discussion on the Code on the 11 February. The event was well attended by clients as well as non-client stakeholders from various sectors including but not limited to: financial services, retail, healthcare, gaming and the charity sector. The feedback below is based on the aspects of the Code that we found to be most concerning to attendees at this event:

i. custom audience initiatives (in response to *'Can we target our customers or supporters on social media*?');
ii. consent requirements for in-app messages (in response to *'Direct marketing by electronic mail (including emails and texts)*');
iii. pixel tagging in email (in response to *'Direct marketing by electronic mail (including emails and texts*)');
iv. 'tell a friend' schemes (in response to *'Can we ask individuals to send our direct marketing*?'); and
v. joint marketing activities (in response to *'Can we use third parties to send our direct marketing*?').
vi. legitimate interests for updating customer details (response to '*Can we use data cleansing and tracing services*?')

i. Custom audience initiatives

In the Code, under the heading *'Can we target our customers or supporters on social media*?' on page 90, consent is noted as the likely lawful basis for custom audience initiatives, as ICO states that it considers it is difficult to envisage how such processing would otherwise satisfy the three-part legitimate interest test.

No reasons are given for this position. As a matter of law, we see no reason as to why legitimate interest would not apply in this context. Recital 47 GDPR notes that: '*The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest'.*

The Privacy and Electronic Communications (EC Directive) Regulations 2003 ('PECR') do not provide more specific rules requiring consent for standard custom audience tools (as they do for example for undertaking direct marketing by emails, cookies etc.). Similarly these tools prohibit, via their terms and conditions, the special category information being uploaded to the platform, meaning consent would also not be required pursuant to Article 9 GDPR.

While the Article 29 Working Party's Opinion 06/2014 on legitimate interest notes that it is unlikely that controllers will be able to rely on legitimate interests to collect vast amounts of data to monitor the online and offline activities of data subjects without their knowledge or a mechanism to object - standard custom audience tools work very differently. These tools neither depend on building large profiles nor surreptitious data collection; rather they just allow a company to reach a customer they already know via a different marketing platform.

Recital 47 GDPR states that legitimate interest may provide a legal basis for

processing provided that the interests or the fundamental rights and freedoms of the data subject are not overridden taking into account the reasonable expectations of data subjects based on their relationship with the controller. Those attending our workshop felt that this test is met based on the following factors:

(a) *Relationship with the data subject:* Standard custom audience tools let companies reach and engage with their existing customers, using information that their customers have shared with them. It is based on there being an existing first party relationship.

(b) *Reasonable expectations of the data subject:* The processing of personal data in custom audience tools is within the reasonable expectations of the data subject. The terms and conditions of these tools require that the advertiser gives notice of the custom audience activity in their Privacy Notice. In addition, the social network gives notice of the processing to the data subject via their own notices.

(c) *Opt-out:* Given the processing for standard custom audience tools is based on an existing customer relationship and notice is given; the processing is unlikely to take individuals by surprise, but if a data subject does not want to receive advertising on other platforms via customer matching techniques, he or she has the ability to opt-out at any time pursuant to Article 21 GDPR.

Accordingly, there is no reason why standard custom audience tools that are based on a first party relationship could not rely on legitimate interest. This also reflects the position adopted in the majority of countries across Europe, where custom audience tools can be based on legitimate interest rather than consent.

ii. Consent requirements for in-app messages

The Code, under the heading *'Direct marketing by electronic mail (including emails and texts)*' on page 72, states that in-app messages and direct messages in social media *'are electronically stored messages',* therefore requiring consent under Regulation 22 PECR.

PECR defines the term 'electronic mail' as: *'any text, voice, sound or image message sent over a public 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'.*
The Code needs to provide more clarity on this issue:

- 'In-app message' is a broad term which is left undefined in the Code meaning it is unclear to organisations which messages require consent and which do not.

- Under PECR an 'electronic mail' is one stored in the network or the recipient's terminal equipment *until* it is 'collected' by the recipient. The Code does not explain why 'in-app messages' or push notifications constitute 'electronic mail' under PECR, i.e. whether this is because, in

ICO's view, the message is stored in the individual's device or because the message is stored in the network.

This level of imprecision makes it difficult for controllers to understand which messages require consent and why.

Furthermore, not all types of notification within mobile operating systems involve the transmission of information over a public electronic communications network, as some notifications can be generated by the app itself.

Without prejudice to the foregoing, if direct in-app messages and direct messages in social media are 'electronic mail' for the purposes of PECR, then it is important that the Code, preferably through the provision of examples, makes clearer that the soft opt-in exemption may also apply to these messaging channels. The Code currently states at page 31, under the heading *'How do we decide what our lawful basis is for direct marketing?*' that *'in-app/in platform direct messaging to individuals'* requires consent - *'without the 'soft opt-in'*. While controllers are familiar with the application of the soft opt-in to email and SMS, the Code should provide more guidance as to how this exemption will apply to in-app messaging.

To take an example, if an individual downloads an app, the app developer should be able to rely on the soft opt-in exemption for sending the user in-app messages containing the developer's own tips, offers and features - assuming that opt-outs were provided on download and in each message. In this case, the downloading of the app should be capable of satisfying the first condition of the soft opt-in exemption i.e. that the data subject's contact details were obtained in the course of a sale (or negotiation for a sale) of a product or service to the individual. Therefore, the ICO should provide further clarity on the application of the soft opt-in exemption in this context.

iii. Pixel tagging in emails

In the Code, under the heading *'Direct marketing by electronic mail (including emails and texts*)' on page 74, ICO states that if pixels or similar devices are being placed in email marketing messages so as to measure open rates or similar metrics, then consent will be required under Regulation 6 PECR. This is in addition to the consent mandated under Regulation 22 PECR for sending the email marketing message itself.
This is very challenging and raises practical difficulties around how consent can be obtained. Controllers generally obtain consent for cookie type technologies via a cookie banner in-desktop or equivalent in the app environment . However this will not cover the use of pixels employed in emails. While the draft Code mandates consent for pixels, it does not describe how consent should be obtained for this processing in practice.

The only feasible option would seem to be to get consent at the time opt-in to sending the email marketing is sought. This, however, raises further practical challenges:

- *Soft opt-in exemption:* where the soft opt-in exemption applies, opt-in consent is not obtained for the sending of the email. In this regard, requiring controllers to obtain consent for measuring open rates of an

email, when consent to sending the marketing email is, itself, exempted at law, greatly undermines the value of the soft opt-in exemption.

- *Service Messages:* Similarly, in the context of service messages where, again, the law does not require consent for sending the email, but where pixels are often employed by the sending controller to ensure that important service messages are delivered and read.

More generally, the fact the Code mandates such a challenging consent standard for pixels in emails is at odds with ICO's recent guidance on cookies which states first party analytics - which is essentially what pixels measuring email open rates amount to - is unlikely to be a regulatory priority for the ICO. That being the case in desktop and apps, it is unclear why the ICO is pushing such a demanding consent standard for analytic pixels in emails given the even lower level of intrusiveness and risk of harm to the individual overall. It also reflects a move in the opposite direction of travel with the rest of Europe given that the proposal for a new e-privacy regulation, in the Commission, Parliament and Council drafts to date, includes an exemption in the regulation for first party audience measurement.

iv. 'Tell a Friend' Schemes

The Code, under the heading *'Can we ask individuals to send our direct marketing*?' on page 83, notes that it is likely that 'tell a friend' campaigns by electronic mail would breach PECR. This is a restrictive position meaning 'tell a friend' schemes - tools widely used by advertisers and greatly valued by consumers - would no longer be permitted in the United Kingdom.

In coming to this conclusion the Code on page 83 takes an overly broad approach of what constitutes 'instigating' marketing: the Code states that '*actively encouraging the individual to forward… direct marketing messages to their friends without actually providing a reward or benefit still means…instigating the sending of the message'.*

Participants at our round-table event considered that, in the refer-a-friend context, the advertising controller should only be deemed to be 'instigating' the sending of marketing in circumstances where the advertising controller is overly incentivising its customers in a way that encourages excessive or viral marketing. By way of example, if the controller offered a reward or benefit based on the *number* of emails provided by an individual irrespective of whether the recipients of those emails subsequently sign up to controller's services, this would amount to misuse (spam) and should amount to instigating.

Save in such cases of abuse, refer-a-friend schemes would be better left to self-regulation vis-à-vis the recipient and their friend, not least because participant feedback was that consumers greatly value 'tell a friend' schemes and it is not an area which has typically generated many complaints to them. For example, if an individual is using a renewable energy provider and is happy with the service they should not be prevented from referring their friend. Participants thought that where a happy consumer recommends their service provider is To a contact who is likely to want to hear about this, there is no apparent harm to data subjects.

Accordingly participants felt that the ICO should endeavour to seek a more balanced approach to 'tell a friend' schemes focussed on regulating outlier bad actors rather than penalising the majority of controllers that sensibly use these tools.

v. Joint Marketing Activities

The Code, under the heading *'Can we use third parties to send our direct marketing*?' on pages 82 and 83 , states that electronic communications for joint marketing need to be based on consent for both parties and comply with PECR. ICO gives the example of a supermarket sending an e-mail promoting a supported charity's work on page 27 under the heading of *'Are we responsible for compliance*?'.

On this point, the Code confuses joint marketing with joint branding activities. In the example given on page 27 of the Code, the Code expects the charity '*to ensure there is appropriate consent'* in place from the supermarket's customers to receive messages promoting the charity. Requiring such a level of due diligence on the part of the charity is excessive in circumstances where the charity is not itself instigating the marketing nor receiving contact details of data subjects from the supermarket - in many cases the charity may not even be aware that the marketing is taking place.

Importantly the Code is also unclear as to whether the supermarket needs separate opt-in consent for the supermarket to reference the charity in the emails it sends (i.e. in addition to the primary consent the supermarket holds to send email marketing). It is submitted that such separate consent is not required by law.

If this were otherwise, it would mean, by way of example:

- that if an app store sent an email promoting '*This month's 15 most popular apps'* to data subjects who opted-in to receive that app store's updates by email, there would have to be fifteen separate opt-ins in the app store UX allowing the data subject to opt-in to receive email marketing relating to *each* app, i.e. in addition to the main opt-in to receive email marketing from the app store provider itself;

- if an individual has opted-in to receiving weekly offers from an online supermarket (e.g. 'this week's half-price offers'), the grocery store would have to obtain separate consent for every third party brand referenced in their marketing emails.

This is not mandated by PECR and would be excessive and unworkable in practice. Accordingly the Code should be updated to clarify the point.

vi. Legitimate interests for updating customer details

In the Code, under the heading *'Can we use data cleansing and tracing services?' on page 62*, the ICO notes, in an example, that a university cannot rely on its legitimate interest to obtain updated postal addresses of its alumni as it cannot '*outweigh the rights of the alumni to choose not to share their new address.'*

On this point, participants felt that the Code assumes too much pro-activeness on the part of data subjects to update *all* institutions they have ever had a relationship with after a change of address. Participants felt that it is also difficult to reconcile these comments with Article 5(d) GDPR which states that personal data shall be '*accurate and, where necessary, kept up to date; 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 ('accuracy')).'*

Without the institution updating postal address information, the personal data held in their systems would be inaccurate and would result in new occupiers of the properties receiving marketing communications not meant for them. Furthermore, so long as the controller entity provides notice of this activity and gives the data subject the right to opt-out at any time pursuant to Article 21 GDPR it is not clear why legitimate interest could not apply.

Participants asked that the ICO reconsider this issue and clarify how the section can be read consistently with Article 5(d) GDPR.

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:

Bird & Bird LLP (Contact People: [redacted]

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