The ICO's new Direct Marketing Code

Nick Graham, Partner, and Monika Sobiecki, Senior Associate, with Dentons, examine the changes introduced in the ICO's new draft Code of Practice on Direct Marketing

On 8th January 2020, the UK Information Commissioner's Office ('ICO') began consulting on a new draft Direct Marketing Code of Practice ('the Code'). The draft Code is both clear and practical in its approach, clarifying direct marketing rules for a General Data Protection Regulation ('GDPR') world, and introducing guidance on new technology such as custom audiences and 'lookalike' audiences.

This article focusses on the significant changes as set out in the new draft Code.

Significance, scope and structure of the Code

The ICO is under a statutory obligation to publish this Code and to take it into account when enforcing the GDPR and the Privacy and Electronic Communications (EC Directive) Regulations 2003 ('PECR'). Therefore, the Code should be treated as significant in terms of establishing legal compliance and not merely as a question of good practice. Further, the Code's enforcement section states that the ICO may ask for details of policies, procedures and the relevant Data Protection Impact Assessment ('DPIA') in the event of complaints and investigations. It's therefore important to ensure that such policies, procedures and documentation are available and reflect the requirements of the Code.

The Code adopts a new structure based on a marketing life cycle. So it walks sequentially through guidance applicable to design, data capture, profiling, campaigns, online advertising and selling data.

The Code is for anyone who intends to conduct direct marketing directed to particular individuals or those operating in the broader marketing eco-system. This covers commercial organisations, but also charities and third sector organisations, political parties, public authorities and those involved in buying, selling, profiling or enriching personal data for direct marketing purposes.

Direct marketing rules are primarily set out in PECR or the equivalent law for EU Member States. These rules fit together with the general GDPR rules.

A copy of the draft Code is available at: www.pdpjournals.com/docs/888020

The ICO's consultation closes on 8th March 2020.

Content of the Code

Direct marketing definition: The term 'direct marketing', defined in the UK in Section 122(5) of the Data Protection Act 2018 ('DPA'), means 'the communication (by whatever means) of advertising or marketing material which is directed to particular individuals'. This is the same definition as that under the old rules. Crucially, the new Code states that the definition applies beyond the simple sending of direct marketing communications — it includes all processing activities leading up to, enabling or supporting the relevant campaign. This would encompass the collection of personal data and building up a profile with the intention of using it for targeted advertising.

Disclosing data to third parties for them to use for their direct marketing also constitutes direct marketing purposes.

'Solicited' and 'unsolicited' marketing: As per the previous position, there are no PECR restrictions on sending 'solicited' direct marketing. This refers to situations where the recipient has specifically requested the particular marketing material to be sent (for example, an individual asks a double glazing company for a quote, and the company sends the quote to the individual).

Market research: There is no major change on this in the new Code. In order for market research to not constitute direct marketing, it needs to be genuine 'market research'. However if, in practice, an organisation is generating leads or collecting data that would later be used for marketing, it cannot argue that it is outside PECR rules.

'Service messages': Organisations often attempt to justify campaigns on the basis that they are really administrative or customer service messages. The term 'service message' is not used in the GDPR or PECR so this requires an assessment of the substance of the message. Phrasing, tone and context will be key factors. Informing credit card customers who have variable balance transfer rates that the rates are changing for a limited period would, according to the Code, be necessary to do. However, if the message actively encourages the individual to make use of the rate change offer, then this is likely to be direct marketing as it is about promoting the rate in

(Continued on page 8)

order to gain further business. Needless to say, these fine distinctions are not easy to make and careful judgement will be needed.

Data protection by design: In line with GDPR accountability requirements, the draft Code states that organisations need to plan properly to avoid the risk of infringing the direct marketing rules. It's also highly likely that they will need to perform a DPIA. This is particularly true for large scale profiling, data matching, online tracking/ advertising, cross-device tracking and targeting children or other vulnerable people.

GDPR lawful basis for direct marketing: In general, the Code questions the possibility of relying on the ground of 'legitimate interests' for direct marketing purposes. For example, if a controller has obtained consent for compliance with PECR (which must be to the GDPR standard) then, in practice, consent is also the appropriate lawful basis under the GDPR. In our view, however, this is open to debate. The PECR consent requirement and the options for choosing a legal basis under GDPR are two separate matters. Pages 30/31 of the draft Code includes a table that is intended to help organisations to know whether or not PECR consent is required for different marketing channels (for example, telephone, email, post). On this, there has been no change to the current position.

The Code states that as a matter of good practice, organisations should get consent for all direct marketing regardless of whether PECR requires it or not. Nevertheless, the legal position is that consent is not always required — in some cases, a 'soft opt-in' for e-marketing will suffice.

If consent under PECR is not needed, then organisations would most likely rely on legitimate interests (for example, for B2B marketing).

"The Code states that as a matter of good practice, organisations should get consent for all direct marketing regardless of whether PECR requires it or not. Nevertheless, the legal position is that consent is not always required — in some cases, a 'soft opt-in' for e-marketing will suffice."

How legitimate interests applies to direct marketing: According to the Code, in order to rely on legitimate interests for direct marketing, organisations need to be able to demonstrate that data use is proportionate, has minimal privacy impact and individuals are unlikely to object.

The Code repeats the standard three part test in assessing legitimate interests:

- purpose test — is there a legitimate interest;
- necessity test — is the processing necessary for that purpose; and
- balancing test — is the legitimate interest overridden by the individual's interests rights or freedoms.

This is what the ICO refers to as the Legitimate Interest Assessment.

The Code states that legitimate interests may not apply where individuals are not given a clear option to opt out of direct marketing when their data are initially collected; where processing for direct marketing is not what the individuals would expect because they haven't been told about it (i.e. invisible processing); and where it is possible to collect or combine vast amounts of personal data from different sources to create personality profiles. In short, anything that stretches the boundaries of reasonableness may also stretch the ability to rely on legitimate interests as a lawful basis.

Data retention: There has been much discussion, but very little guidance, on how long to keep data for direct marketing purposes. The Code states that 'consent does not last forever', whilst the ICO has repeated its position that the duration of consent will depend on circumstances including the context in which it was given, the nature of the individual's relationship with the organisation and the individual's expectations. In our view, this equates to a 'reasonableness test'. This is borne out by some of the examples given in the Code, such as where a retailer collects email addresses for customers who have asked to be kept updated on a new product launch as opposed to subsequent use of that mailing list to promote other products in general.

There is also a useful 'good practice recommendation' in the Code that when sending direct marketing to new customers on the basis of consent collected by a third party, organisations do not rely on consent given more than six months ago.

Generating leads and collecting contact details: The Code explains that there are a number of ways that organisations may decide to generate leads and seek contact details. This might be from individuals who buy their products, third parties who sell leads, rent lists or publicly available sources. Clearly, depending on whether details are collected direct from the data subject or not, there will be associated transparency obligations under Article 13 and/or 14 of the GDPR.

Informing people: As we know, the GDPR requires privacy notices and disclosures to be concise, intelligible, in clear and plain language and easily accessible. The Code also criticises vague terms such as 'marketing purposes' or similar. However, the challenge, particularly with new technology such as social media and use of cookies, is as to how to best explain those processes clearly and simply. The sub-text is that organisations should place themselves in the shoes of the individual and ask themselves whether they would have properly understood how your data were going to be used for direct marketing.

Use of publicly available personal data for direct marketing purposes: Organisations should never assume that publicly available data are 'fair game'. The Code specifically states that an individual may want as many people as possible to read their social media posts, but that 'does not mean they are agreeing to have their data collected and analysed to profile them to target… direct marketing campaigns'. Companies that use public source data should review these processes carefully against GDPR requirements and record this in a DPIA.

Buying or renting direct marketing lists: Organisations should undertake proportionate due diligence and provide a list of the required components including who compiled the data, where they came from, what information has been provided to the individuals and what consents/opt-outs are in place.

In addition, they would need to screen new lists against their own suppression lists.

Asking existing customers to provide contact details of their friends and family: The old Code was somewhat critical of this practice. Under the new draft Code, the ICO repeats that it is difficult to comply with the GDPR in this kind of case when collecting details for direct marketing or to demonstrate accountability. The Code says, for example, that organisations 'have no idea what the individual has told their friends and family about them processing their data, and you would not be able to verify whether these contacts actually gave a valid consent for you to collect their data.' This is a steer to avoid viral marketing of this type. The ICO goes further and says that if contact details collected in this manner are used for e-marketing, this will 'likely breach the PECR'.

"Organisations should never assume that publicly available data are 'fair game'. The Code specifically states that an individual may want as many people as possible to read their social media posts, but that 'does not mean they are agreeing to have their data collected and analysed to profile them to target… direct marketing campaigns'."

Profiling and data enrichment: Profiling is where behavioural characteristics of individuals are analysed to find out about their preferences, predict their behaviour, make decisions about them or classify them in different groups or sectors. Data enrichment is where organisations find out more data on individuals to add to the profile already generated. This includes sourcing additional data on contacts and customers from third party sources (public or otherwise).

There are a whole host of issues resulting from such practices. We want to flag specifically that the ICO effectively states that the scope of legitimate interests is unlikely to cover intrusive profiling, as this is not generally in an individual's reasonable expectations and is rarely transparent enough. This poses a challenge for the direct marketing sector, in particular in relation to new technology and social media.

The Code also discusses Article 22 and automated decision-making, including profiling. Article 22 only applies to solely automated decision-making which has legal or similar significant effects on individuals. Helpfully, the Code confirms that the majority of direct marketing of this type is unlikely to trigger Article 22, but states that there are circumstances where it might do just that. For example, profiling to target vulnerable groups or children might be caught, as would targeting individuals known to be in financial difficulty with marketing about high interest loans, targeting known problem gamblers with adverts for betting websites, or using profiling to effectively 'price-out' individuals of owning a particular product by giving them a much higher price than other people.

In practice, organisations will want to avoid triggering Article 22, as doing so is likely to require explicit consent. The better approach is to stay outside its scope. In terms of enriching data already held, the Code takes the view that enrichment should not be unfair to individuals, but that it is unlikely individuals will anticipate such a use. Therefore organisations should inform individuals about this in advance.

Online advertising and new technologies: The Code repeats the current position on cookies and similar technologies, and that this requires provision of clear and comprehensive information (i.e. the cookie notice) and consent (i.e. the icon/checkbox to indicate agreement that is used on many websites). It also repeats the position that the notice and consent rule not only applies to cookies but also device fingerprinting, tracking pixels and plug-ins as well as other third party tracking technology.

Interestingly, the Code states that because consent cannot be bundled up as a condition for receipt of a service, in many circumstances, a cookie wall is unlikely to be appropriate. The optimal position is to offer website users a genuine choice as to whether or not to accept cookies without limiting their access to the website content. It should be noted, however, that there are significant philosophical debates going on about how this issue should be resolved without damaging the 'free web'.

The Code also deals with targeting customers or supporters on social media. It explains that social media platforms offer 'list-based' targeting tools that allow organisations to target direct marketing to users on their platform. In practice, the organisation uploads its customer list and the platform then matches this data to its own user base. These tools are generally known as 'audiences'. In

(Continued on page 10)

(Continued from page 9)

this case, organisations must be transparent and clearly inform individuals about this processing. The Code also states that organisations should be 'upfront' about this processing and that individuals are unlikely to expect that it will be taking place. Therefore, they should not 'bury information about any list-based tools...within your privacy information'. This suggests that a more prominent notice will be needed.

The Code also states that it is likely that consent is the appropriate lawful basis for this processing, as it is difficult to see how it would meet the three-part test of the legitimate interest basis. Clearly, if an individual gives consent and then revokes it, organisations cannot use their data to target them on social media including by using list-based tools. So the 'off-switch' needs to cover direct marketing campaigns, associated profiling and targeting on social media using the list-based tools.

The Code also discusses the targeting of people on social media who are similar to an organisation's customers or supporters. These are commonly known as 'look-a-like' audiences. In this case, the Code states that organisations need to inform individuals who have provided their information that you intend to process their data to create these audiences and ensure they have a valid lawful basis. There's nothing in the Code that says that legitimate interests would not be appropriate in this kind of case, so it appears that this is one available option.

Finally, the Code says that both the organisation and the platform are likely to be joint controllers for this activity. This is because while the social media platform does most of the work, the organisation instigates the processing and provides the platform with the initial data set (i.e. its original list-based audience).

Direct marketing using facial recognition or detection: For the first time, the Code discusses the use of facial recognition and detection for direct marketing purposes. Interestingly, both these technologies will involve processing biometric data. Facial recognition seeks to identify or verify a specific individual, whereas facial detection seeks to distinguish between different categories of individuals only. Biometric data are also special category data when they are processed specifically 'for the purpose uniquely identifying a natural person'. It is this end purpose of the processing which determines whether the data are special category data, not whether the deployment has the technical capability to uniquely identify an individual. This is an important distinction and one which will be helpful in analysing the scope of special category data in this context.

The ICO's position is that it is unlikely that organisations will be able to use facial recognition technology to display direct marketing to particular individuals. This is because it would be very difficult to comply with lawfulness, fairness and transparency requirements of the GDPR when using the technology for this purpose. In addition, this would constitute special category data which would likely trigger a requirement for explicit consent.

Interestingly, facial detection technology may not strictly speaking be special category data, as it is not about seeking to identify an individual, but rather segmenting the audience into categories (e.g. detecting someone's age, gender, facial attributes or mood and then showing them an advert based on those characteristics). Nevertheless, facial detection systems can still trigger Article 9 GDPR where they store a template to track the individual across an area covered by various screens and billboards (for example, in a shopping center).

Clearly, there's more thinking to be done on this, but the Code offers useful observations for what is potentially a high risk privacy area.

Use of advertising IDs: Device operating systems, such as Android or iOS, incorporate unique identifiers that can be used for marketing purposes. These are known as Google Advertising ID ('ADID') on Android, the 'Identifier for Advertising' (IDFA) on iOS and the 'Advertising ID' on Windows 10. The Code takes the view that these are examples of 'online identifiers' which Recital 30 of GDPR states can be personal data. These advertising IDs, when enabled, can allow the organisation's mobile App to assess and use them for personalised advertising similar to the way in which online services use unique identifiers stored in cookies. In addition, advertising IDs can also be used in other types of online behaviour advertising, such as real-time bidding. The Code indicates that due diligence would be needed, as well as a DPIA.

Conclusion

The draft Code updates the guidance for new tech and social media and represents a general push towards a permission-based model. Further thinking is needed on the practical application of some of these new technologies such as custom audiences and look-like lists. Now is the time to review the Code and start working on how it applies practically to your organisation.

Nick Graham and Monika Sobiecki
Dentons
nick.graham@dentons.com
Monika.Sobiecki@dentons.com