Data & Marketing Association

DMA Response to ICO Direct Marketing Code of Practice

About the Data & Marketing Association (DMA)

The DMA is Europe's largest trade body in the data and marketing industry, representing over 1,000 data-driven companies across the UK.

The DMA played a major role in the shaping of the GDPR data protection laws in the UK and EU and led the implementation in our industry as the trusted source for industry advice and guidance.

The DMA continues a leading role in discussions around data, tech and AI, ethics, marketing and beyond. Our Value of Data campaign—led in partnership with Edinburgh University's Design Informatics Department and the Bayes Centre—is leading the way in providing a place for discussions about the ethical use of data.

General Comments

The DMA welcomes the direct marketing draft code of practice.

The DMA understands the need for the ICO Code on Direct Marketing to be comprehensive and protect the consumer. Nonetheless, we feel the drafted document has a general negative bias against marketing as if it is a nefarious activity.

The document often refers to consumer expectations but provides no evidence for what people expect or approve of. It is more often than not assumed the consumer is not happy to have data used and that they do not want businesses to access information that will tailor advertising to their preferences. This is not borne out by the evidence. On the contrary, research reports that consumers prefer advertising that is targeted to them, insofar it is clear where the data is coming from and how it is used. While it is up to businesses to provide the means by which consumers access this information, the law encourages a baseline of transparency and accountability that we believe will satisfy most consumers.

The document generally favours consent and suggests that LI is always the more difficult option. Previous advice from the ICO stated that there was no hierarchy and consent was not always the best option.

Indeed, some areas such as the requirement for consent for social audiences seem overly strict for no real reason, there is no harmful impact and yet there is no option for LI to be used.

Legitimate interest is an instrument that allows GDPR to strike the balance between Article 1 (2) "This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data." and (3) "The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.", which reflects

EU Charta of Fundamental Rights Articles 8 “protection of personal data” and 16 “Freedom to conduct a business”. By more or less denying legitimate interest for marketing purposes, ICO is ignoring the fundamental premise of the GDPR and the EU Charta of Fundamental Rights.

The outcome of businesses complying fully with the ICO’s consent-favoured interpretation would create an uncompetitive environment. Smaller businesses and new entrants would have almost no options for doing independent marketing and would be forced to use the services of existing tech giants such as Google and Facebook.

Ultimately, modern consumers are well-aware that ‘free’ online services are nearly always funded by advertising based on their internet use. The provisions in direct marketing are to ensure unsolicited communication are blocked, not that advertisements that may be relevant to consumers and that they expect to see. These ought not to be regulated in the same fashion as unsolicited communications unwelcomed by consumers.

Furthermore, while this is a ‘direct marketing code’ there is a need to put greater distinction between the processing covered by GDPR and that covered by PECR. Currently, it may be unclear to many when the document is relying on GDPR or PECR to give its advice. As much explicit information on this would aid businesses—particularly smaller organisations without large legal and compliance teams—to understand the law and act appropriately. The guide ought to be educational as well as practical.

On this note, the document would benefit from more examples (or a follow-up guidance document of a comprehensive set of examples). Where an example of bad practice was provided a separate example or description of how it could have been properly should be given.

In the past the ICO has made good use of visual guides, tables, diagrams, infographics to explain complex subjects, these seem to be lacking in the draft code.

Many members have taken the trouble to explain the far-reaching and possibly unforeseen negative consequences of the law being interpreted as described by the draft code:

- Damage to brands as their marketing communications deteriorate due to lack of data for verification, general intelligence and targeting appropriate messages.
- Almost complete removal of third-party data, products, services
- Less analytic data available, unable to personalise marketing or make marketing relevant.
- Impact on brand return on marketing investment
- Huge negative impact of user experience as they were presented with more and more consent options and more poorly targeted and less relevant advertising
- Fewer marketing opportunities, especially for small and new businesses
- Increased cost to business to update systems and databases to accommodate new requirements.
- Hugely increased complexity of data systems and new options and consent preferences are added and managed
- Reduction in data quality as opportunities for updated data and data matching is removed

- Financial impact on industry and loss of jobs if third party data and related products have to be removed.

Specific comments

In consultation with our members, the DMA has identified a number of issues that we feel could be examined further.

Dual brand promotions by email, both parties need to comply with PECR
Page 27 - Are we responsible for compliance? If you are planning electronic communications as dual branding promotion with a third party, you still need to comply with PECR even if you do not have access to the data that is used. Both you and the third party are responsible for complying with PECR. The example in the draft code is about a supermarket promoting the work of a charity. "...it still needs to ensure there is appropriate consent from its customers to receive direct marketing promoting the charity." Does the supermarket need to get consent to send messages including information about the charity? Including offers from partner organisations in marketing communications is common. E.g. Airlines offer hotel deals. Consumers have come to expect this type of advertising and it is often welcomed if consumers can save money on deals with partners. In order for this to continue, it should be made clear where consent is necessary.

If consent required by PECR then consent must be used for GDPR

Page 30 – How do we decide what our lawful basis is for direct marketing

"PECR requires consent for some methods of sending direct marketing. 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 legitimise processing that is unlawful under other legislation."

This would suggest that if you gather consent to send marketing emails to customers you would also need consent for any other processing related to marketing such as profiling or segmentation of data leading up to the sending of an email.
The DMA does not agree that only one legal basis can be used.

This would mean that if you need consent to send an email (PECR), you must also obtain consent to do any profiling/segmentation of the same data (GDPR) or any other processing purpose.

This requirement is copied directly from the ICO legitimate interest guidance that was published soon after the implementation of GDPR. However, the meaning of direct marketing 'purposes' was not defined at that time and therefore this requirement was not interpreted in this way.

It also makes things very unsatisfactory for consumers and difficult to manage and maintain for marketers.

It appears that, as well as an opt-in box to send emails, you would also need a separate opt-in box for profiling/segmentation.

Including this box would undoubtedly reduce the amount of customer data a company will be able to access in spite of there being little evidence to suggest consumers do not want businesses to have such data. Indeed, studies show that consumers prefer seeing advertising that is relevant to them. This change would reduce business' ability to provide such targeted advertising by limiting the amount of profiling data they can collect.

In addition, GDPR accepts more than one legal ground to process data. For instance, article 17 (1) b "*…and where there is no other legal ground for the processing*" implying just that. EDPB in its guidance on consent states " *As a general rule, if consent is withdrawn, all data processing operations that were based on consent and took place before the withdrawal of consent - and in accordance with the GDPR - remain lawful, however, the controller must stop the processing actions concerned. If there is no other lawful basis justifying the processing (e.g. further storage) of the data, they should be deleted by the controller.*" Supporting the point that more than one legal ground can be present for a processing.

Good practise recommendations
Page 31 – Good practice recommendation The ICO 'recommend' consent for all direct marketing activities. The DMA does not agree with this recommendation, and back in 2017 it appeared to be the case that the ICO did not agree with it either. Blog: Consent is not the 'silver bullet' for GDPR compliance https://ico.org.uk/about-the-ico/news-and-events/blog-consent-is-not-the-silver-bullet-for-gdpr-compliance/ The ICO also recommends that "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." A specific time is not mentioned in the GDPR or PECR. There are many examples where a company might want to delay the sending of marketing communications until the most relevant time, e.g. insurance. More importantly, we think that because the code is written by the regulator and has legal status, it should focus on interpreting the law and not overstep its remit by suggesting best practice which is historically the role of industry associations – often with input from the ICO at this point. Section 122 (1)(b) DPA 2018 the commissioner must prepare a code of practice which contains … such other guidance as the Commissioner considers appropriate to promote good practice in direct marketing. If the ICO must provide best practice, they could use this opportunity to suggest things that they have seen the industry struggling with and subjects in which they have superior knowledge such as completing a DPIA or LIA, or suggestions on how to present complex information simply to consumers. The regulators 'suggestions' blur the line between legal interpretation and what the regulator finds acceptable. The DMA does not think it is the job of the regulator to offer best practice suggestions on industry matters; this is clearly the role of industry associations.

Article 14 notification

Page 48 – What do we need to tell people if we collect their data from other sources?

Article 14 of GDPR says that if one obtains personal data from somewhere other than directly from the data subject, one is obliged to provide privacy information to that person within a month.

For companies that collect data from such sources as Companies House, Edited Electoral Roll or third-party data providers, this will have a major impact.

Until now these companies have been relying on the 'disproportionate effort' exemption. However, the draft code says:

"You are unlikely to be able to rely on disproportionate effort in situations where you are collecting personal data from various sources to build an extensive profile of an individual's interests and characteristics for direct marketing purposes. Individuals will not reasonably expect organisations to collect and use large volumes of data in this way, especially if they do not have any direct relationship with them. If individuals do not know about such extensive processing of their data they are unable to exercise their rights over it."

For some reason, the draft code omits the other exemptions 14 (5)(a) and 14 (5)(c) both of which are very relevant to data collected for marketing purposes.

This was identified as a risk when it was first spotted in the EDPB's guidance on transparency, at which point companies who relied on collecting data indirectly decided that the disproportionate effort exception would be appropriate. If the 'disproportionate effort' exemption is not considered acceptable for companies that collect and aggregate data for re-sale and the development of additional data services, it could put the data business units at many of the UK's big data companies out of business. It is the view of the DMA that if the effects of complying with a requirement were to bankrupt a business, it would be disproportionate.

Example from DMA member:
"Here at [redacted], we base our business on the provision of data to our clients for use with postal DM only. Strictly postal, no email, telephone or social marketing, and indeed do not gather, store or process data relating to those methods.

We gather data from a number of sources, including a couple of well-known and larger well-established UK data providers - as well as our own gathering from open source. Do we profile? Yes, of course - it's the whole point of this particular genre of marketing. Whether the market be utilities, travel, retail, whatever it is and wherever our client resides, we use our personal data to analyse their existing clients, and then locate new potential clients who match - straightforward and fundamental.

So, considering we deal with many millions of records (data on some 50+ million individuals and some 29+ million properties) - the option to inform them all that we have gained their data from another source is simply a non-starter. I would hope disproportionate effort in posting notice to 50m individuals might count.

From our perspective - we conduct a DPIA for each market in which we operate, and a LIA for each client in each market, and if necessary an additional LIA for any postal DM campaign we feel needs it - we are very thorough. We police every item of DM, literally every single item, and ensure nothing leaves us that will have a negative impact on the recipient audience. We offer opt-outs that are clear on every single item with which we are involved."

Example from DMA member:
"As most marketing campaigns take longer than a month, this seems to state that we should contact the data subject twice, once with the privacy information and then following up with the marketing. This would have significant resource implication (both time and financial) but also would increase the number of mailings received by the consumer, which seems to defeat the purpose of this clause. It also raises the problem that we would have to mail people with privacy information who might not actually be sent any marketing as they were suppressed or de-selected as the offer might be inappropriate.

The ICO should provide examples of what it believes a proportionate effort would involve for those B2B companies with no direct relation with individuals. Sending a letter to millions of people just for the purposes of the A14 information would for example clearly involve a disproportionate effort."

Overall, this has a potentially huge impact on data services companies that aggregate data from various, including public sources and then resell this data (data enrichment, appending profiling, developing data products).

If this is no longer a viable business, it would also have a knock-on effect to all the organisations that use this data for customer acquisition campaigns or use the various data products.

The DMA believes that the disproportionate effort exception should be available. Consumers do not want to be contacted multiple times to be informed that companies hold their data. The impact on the individual is negligible until the data is used for marketing at which point, they become informed and can choose to opt-out.

Disproportionate efforts has no effect on reasonable expectations, i.e. someone (assuming they had knowledge of the law) would not reasonably expect to be contacted about unobtrusive use cases if that contact would involve disproportionate efforts and would therefore reasonably expect certain "behind the scenes" processing to take place.

Colleagues at FEDMA came to the view that the UK translation of the EDPB guidance may be incorrect, and it should say 'privacy information should be supplied within one month **or** at the point of first communication'. I have previously raised this with the ICO but have not had a response.

There are still compelling reasons that data companies need not inform consumers that they have gained data from another source. Companies collecting data inform consumers about the companies they intend to share their data with at the point of collection, creating a layered policy approach Article 15(5)(a) (the data subject already has the information). Article 14 (5) (c) (*"obtaining or disclosure is expressly laid down by Union or Member State*

law") clearly addresses the use of electoral roll data which is covered in the Representation of the People Act:

This data is then used for more accurate and relevant communications and better business decisions. As long as any communication to prospects or customers communicates the original data sources within the email, this should be sufficient. Similarly, If the data is used for internal processes only such as data hygiene, and not as a mailing list, it should be appropriate to use legitimate interest.

After all, third party data helps business and customers improve relevance and productivity. It is the DMA's view that it is a legitimate interest to understand audiences for your customers and to be able to understand them better, to serve them better and develop new products.

Ultimately, any issue of notification should be restricted to the use of contact data for specific communications rather than profiling and analysis, and the notification can take place within the message, provided there is some way to object.

The DMA believes this to be a primary risk of the draft code and the ICO should consider the impact more broadly.

Publicly available personal data for direct marketing purposes
Page 52 – Can we use publicly available personal data for direct marketing purposes? This section starts by listed public sources including the EER, but only provides an example for social media. A position on the use of EER would be helpful. Many organisations use the EER or data based on the EER, the use of this data is explained at the point of registration and people can opt-out. Examples of acceptable use of EER would be useful. Article 14(5)(c) of the GDPR states that where 'obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests' Article 14 transparency requirements do not apply. This needs consideration / explanation in the CoP.

Using MPS
Page 53 – What do we need to consider when buying or renting direct marketing lists? The guide recommends using TPS and CTPS, we would also like it to include reference to MPS. Although no specific law mentions MPS, GPDR does say that opt-out requests must be honoured. MPS is a well-known industry opt-out request and should be listed in this document. This would give a more effective suppression of direct mail.

Profiling
Page 58 – Can we use profiling to better target our direct marketing? "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." A number of DMA members are concerned that the ICO appears to prize consent as a legal ground over legitimate interest in spite of the law describing all legal grounds as adequate. As discussed earlier, the DMA believes legitimate interest can be a valid option for profiling given the benefit to customers from improved business performance. The DMA believes the ICO should clarify that by "intrusive" profiling, it means profiling that produces legal or similar effects. In addition, DMA is concerned that the ICO may be generalising profiling that is used in the context of direct marketing. ICO may be assuming that there are only two types of profiling, namely profiling based on factual behaviour that can be carried out in a walled garden context by global social media and online service providers, and, profiles that are developed using cookies. However, there are much less intrusive profiling which most members of the DMA and their client marketers have been using for over 50 years. Traditional profiling, or conscientious profiling, are created using data sources such as the census, survey, and market research. The key difference between this raw data and online behaviour-based data is that data collected this way is self-declarative in nature. Some of the lifestyle data are even aggregated and averaged out onto anonymous geographic level. Marketers then use addresses to match such data to their CRM file to, for instance, generate a report what the socio demographic characteristics are or what hobbies they are likely to have. Similarly, differentiation should be made for cases where technical and organisational measures are taken where profiling is conducted. Pseudonymisation, for instance, helps marketers gain insights into their client base while the identities of the data subjects are protected.

Sending emails using a third party

Page 82 – Can we use third parties to send our direct marketing?

Page 82 of the Code suggests that the sending of emails using a 3rd party technology provider such as any of the marketing cloud providers or specialist ESPs would require both parties to have consent for the activity. This must surely be a mistake in drafting as the brand who has the consent to send emails to customers is acting as the data controller and the martech provider is clearly acting as a data processor under contract. There is no aspect of the relationship that would imply the tech provider is a joint controller.

This section suggests that both parties need consent. Currently, the wording includes ESP's as they are the 'sender' of the email.

If the definition of sender or instigator includes email service providers, then a company could not use Mailchimp, Dotmailer etc and would only be able to send emails from their own organisation. Could the ICO clarify if this a mistake in drafting? If not, it would be an extraordinarily limiting move that would prevent the use of ESPs. It is difficult to imagine this is the intention.

Refer a Friend

Page 83 - Can we use third parties to send our direct marketing?

According to the draft code 'Refer a Friend' campaigns breach PECR.
The DMA has a member whose business is all about referral marketing. They provide codes for customers to pass on to their friends – Would this also breach PECR?

"The term 'instigator' is not defined in PECR; however, you are likely to be instigating if you encourage, incite, or ask someone else to send your direct marketing message." This definition is incredibly broad.

There is an entire section of the industry dedicated to referral marketing 23% of all brands use some kind of referral marketing:

https://dma.org.uk/research/referral-marketing-are-you-creating-customer-advocates

Clarity is required here. The example given of a brand generating emails to for existing clients to send to their friends can clearly be seen as instigating the sending of an email. But many organisations merely give a code to customers for their friends to use at sign up, would the sharing of this code also be considered instigation of marketing?

It should be clarified in the guidance that "it is not active encouragement or instigation by an organisation if an individual has control over the message being sent to a friend and how the message is sent. However, there should be a message instructing individuals only to send a refer a friend message to a friend who would be interested in this message rather than to all friends in their network.

Referral marketing is based on trust. Firstly, the trust between a customer and a brand and secondly, the trust between that customer and any friends they choose to share the brand with. In the context of a referral, this means that a customer will consider how their message will be received before referring a brand to a friend. They will filter for relevance and for trust.

Individual consumers should not be treated as advertising platforms, but discerning consumers who can make up their own minds about whether a particular offer is or isn't a good deal. While protections of vulnerable consumers are and should be in place to increase transparency and stop bombardment of deals, the ICO should not be in the business of telling individuals they cannot share what they perceive to be a good deal with a friend or relative, who, in turn, can decide whether the deal they have been offered is a good deal.

Improvements could be made in this field by marketers and clarity around rules can be issued by the ICO, but this practice of giving offers to customers and their friends and family ought to be protected.

Social audiences and 'lookalike' audiences
Page 90 - Is all online advertising covered by the direct marketing rules? The draft code makes it clear that data used for social audiences and 'lookalike' audiences requires consent. Also, as a joint controller, the marketer needs to undertake due diligence on the social media platform to ensure that the data being used has valid consent. This is a very popular form of marketing and an alternative to email where consent has not been provided. This could have a severe impact on many brands, particularly SME's. There are many different social platforms with different ways of presenting ads or identifying customers, treating the whole channel in the same way lacks the nuance needed for regulating a broad, innovative and multifaceted market. Given that the data subject has a first-party relationship with the brand and Facebook, is it justifiable to present consent as the only option for marketers? In addition, very often, look-alike audiences are being created using traditional conscientious profiling, making use of less intrusive self-declarative modelled data. This must be differentiated from other more intrusive form of look-alike audiences.

Switching legal basis
Page 102 – Can we offer data broking services? This section talks about sharing data and switching legal basis, it appears to be written because the ICO have seen this in practice and want to address it. For example, some brokers obtain data collected with consent and then share it under LI This has already been raised by two DMA members as contrary to their own legal advice. Switching legal grounds between controllers is a common practice, e.g. company (a) generating a lead could pass the lead information on the consent ground to another company (b) then that company (b) continues to process on the contract necessity ground. For example, data subjects who are provided information upfront as part of the consent mechanism that subsequent controllers will process on the legitimate interest ground are made aware of the "switch" and are free either to consent or not to that arrangement. On the other hand, processing done on the LI ground at all stages in the chain affords the individual slightly less control. Consent provides a stronger level of permission initially and acts as a "gateway" for subsequent LI use. Not allowing the switching of legal grounds both limits control of the customer (as they will be able to consent or not to the switching of and subsequent use of processing methods), and also limits the way businesses can best use data for improving customer experience. The key here is to provide transparency from the outset about what controller will process on which ground. In that sense, there is no switch of legal basis within a controller.

Consent required for tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering

Page 103 – Can we offer data broking services?

As noted in the text:
"…when an organisation specifically wants to analyse or predict the personal preferences, behaviour and attitudes of individual customers, which will subsequently inform 'measures or decisions' that are taken with regard to those customers... free, specific, informed and unambiguous ***'opt-in' consent would almost always be required****, otherwise further use cannot be considered compatible. Importantly,* ***such consent should be required, for example, for tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering,*** *location-based advertising or tracking-based digital market research."*

This reference contradicts previous advice in this document and says that consent should be used for all direct marketing, profiling, data broking etc.

DMA does not know why this has been included; it is old advice that contradicts previous advice that LI can be used.

It is dangerous to include pre-GDPR advice in a GDPR code. Why chose this piece of pre-GDPR advice and not another?

In addition, as mentioned in previous sections, the DMA is concerned that ICO is not differentiating profiles created through tracking and other traditional conscientious profiling and/or advertisement display triggered based on the context of website content. Similarly, the DMA feels that it is important to make a distinction between data-broking based on online behavioural tracking and that based on less intrusive for instance traditional data curation methods.

As noted in the text:
"If you are considering collecting and subsequently processing using legitimate interests as your lawful basis, you need to objectively work through the three-part test (the legitimate interest assessment) prior to the processing and record the outcome. A key part of the balancing test is the reasonable expectations of individuals, and transparency will be vital. It is unlikely to be in people's reasonable expectations that you will be building extensive profiles on them in order to sell these to lots of other organisations."

The use of the word "extensive" could also include unintrusive data points, i.e. those that would not produce legal or similar effects. It would be welcomed if the ICO would clarify that the use of the word "extensive" does not include unintrusive data points, i.e. those that would not produce legal or similar effects).

For instance, even when hundreds of characteristics are available (from hobbies to socio demographics), if the information is generalised on an anonymous neighbourhood level, it will still not identify the exact characteristics of the individual despite the profile being extensive.

Please do not hesitate to get in contact if the DMA can contribute further to the ICO's work in this area.

Kind regards,

[redacted]
[redacted]@dma.org.uk