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:

This version has lots of useful clarification, particularly on the definition of direct marketing purposes and contains helpful cross-referencing to PECR.

Would it be possible to have some sections and numbers in this document? It would be helpful to also have references to articles or recitals where appropriate.

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?

There is plenty of detail in this draft code, but there are instances of conflict and ambiguity. We have referenced these instances in Q6 and provided some suggestions which may help with this.

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:

Would it be possible to have some sections and numbers in this document? It would also be helpful to have references to the specific GDPR articles or recitals where appropriate.

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 :

1. Page 35-37, How does legitimate interests apply to direct marketing?

This section gives the impression that whilst there is no hierarchy of legal basis, the ICO is not keen on LI.

We think the relationship point in particular needs more clarity. This guide suggests that LI may be appropriate if there is a relationship in place however industry best practice (where the ICO has included a foreword in the guide) states that a relationship is not necessary, which is confusing. See DMA guide "GDPR for Marketers: Consent and legitimate interests" for more information.

And now the definition of direct marketing has been widened to include all elements of the campaign process, we think it would be beneficial to marketers to understand how legitimate interests can be used for those other parts of the process.

We think this section could take some examples from the DMA guide "GDPR for Marketers: Consent and legitimate interests".
https://dma.org.uk/uploads/misc/5ae1fbf5c60fd-gdpr-for-marketers---consent-and-legitimate-interest_5ae1fbf5c6066.pdf

It would also be helpful to include some examples of where LI could be used. There are some examples in the DMA advice: Using third party data under the GDPR, pages 11-13. https://dma.org.uk/uploads/misc/third-party-data-guide-1.0.pdf

Suggested List DM Example
A life insurance company sends direct mail to people about its products and services. It uses legitimate interests as its legal basis as there is a underinsurance problem in the market (which meets the necessary test) and direct mail is the most cost effective way to reach people and is permissible under ***Recital 47***. In order to ensure their activity is conduced within the requirements of GDPR, the insurance company makes sure

- the data processed is ***minimised*** and only the necessary data points are used,
- the data subject was aware that the processing could happen and who will be using their data at the point they provided the data through a compliant ***privacy policy***,
- the data provider has an ***audit trail*** of permissions given,
- the data subject can ***opt out*** at any time
- the age of the data (both of when it is first collected and recently verified) is within an acceptable time period (it would be great if the ICO could provide some guidance here – we understand best practice to be collected within 5 years and verified within 2 but would appreciate some guidance here)
- and the necessary data protection documents (DPIA, RPA and LIA) and completed and held on file.

2. Publically sourced data – Page 53

The new guidance suggests that if we wanted to use publically available data such as

the electoral role for cleansing a gone away file or for verifying addresses, we would need to send a privacy policy out to everyone who's record we check within one month of using it. We understand that the data market makes widespread use of publically available data to verify and cleanse records to ensure the data is up to date and accurate, just before the campaign goes live. For these reasons, we feel that the draft guidance would have some unintended consequences:-

1) It would be impractical and costly for organisations to send a copy of their privacy policy every time they use publically sourced data such as the EER to cleanse data or validate an address
2) It is not a great experience for customers generally as they could receive thousands of privacy policies and not understand why
3) It could cause unnecessary worry to vulnerable customers
4) If we stopped cleansing data by using these sources then there is a risk that direct mail could be sent to people at the wrong address, which could cause harm or distress.

Our recommendation would be for the ICO to provide greater guidance on how publically sourced data could be used more responsibly and in line with the GDPR. For example:-

- More detail on how its use could be included in the electoral roll forms (ie at source of data collection) and on local authority websites
- Organisations could include details in their privacy policies about what publically sourced data they use and what they use it for
- We couldn't see where this interpretation is grounded in the GDPR so it would be good to understand how other countries have approached this.

3. Recommend a friend – page 55

This section suggests that recommend a friend is no longer permissible but it only talks about one method of how this can work. We agree with the example, but there are other ways Recommend a Friend can work, so would suggest it might be helpful to clarify that in the code. For example a person could give their friend a code to quote when applying that could give them the discount.

Suggested Example: Taylor Wimpey.

They provide all new home owners with a book of vouchers. The home owner is incentivized to give a voucher to a friend, and the friend hands it in to Taylor Wimpey for redemption if they buy a new house too. At no point is Pii disclosed unlawfully as the new home owner completes the voucher themselves, and provides it to their friend for the purpose of benefitting from the recommend a friend scheme.

4. Definition of Marketing and Servicing Communications – page 19

This section contains much needed detail about the difference between marketing and services communications.

There were some areas which we felt were confusing and ambiguous:

Page 19 details that we can no longer encourage customers to make use of a particular product as a service message. We would request more clarity here. Our regulator – the FCA – encourages us to ensure that our customers know about the products they have with us and are making good use of the benefits that they are paying for. We have a regulatory requirement under FG16/8 to talk to our long

standing customers regularly to ensure they have an opportunity to review their cover and ensure the product still meets their needs. To do this in the right possible way, we have designed letters that meet the DMA and DPN's guidance on service messages and we have conducted research with customers who received the mailings to get their feedback. Those customers have all told us they appreciated getting the mailing as it gave them an opportunity to check their cover and then not worry about it. We are not encouraging them to change or upgrade their cover. We are concerned that the current wording in the draft code would make it difficult for us to deliver on this FCA requirement.

Furthermore, we also have vital benefits within our product range such as Employee Assistance Helpline available through our workplace income protection product that we need to be able to tell employees it's there so that they can use it (free of charge) if they should ever need it. It comprises of counselling and mental health services, legal advice, financial advice and rehabilitation services such as physiotherapy. We do not make any money from employees using this service so they would be at a disadvantage if we couldn't tell them about it as we do not collect marketing permissions in a workplace arrangement (as the contract is between us – the insurer and the employer).

"We stock carrots example" on page 20. We believe the purpose of this example might be to highlight intent / motivation as key to determining whether a message is marketing or servicing. But this wasn't clear in the document. The DPN produced a blog last year that provided some greater clarity on what would fall in the marketing definition and what would fall in the servicing definition and covers the subject of intent as follows:

"As a rule of thumb, if the aim of your communication is to try to generate more business it will be deemed to be a marketing message. If the intention is to sell services/products, cross-sell, up-sell or generate leads, it will fall under the definition of direct marketing"

Our recommendation is for the ICO to use the DPN blog and incorporate some of their guidance as we have found it to be very clear and valuable.
https://dpnetwork.org.uk/marketing-message-service-message-where-to-draw-the-line/?utm_source=Data+Protection+Network&utm_campaign=1cf13970a2-EMAIL_CAMPAIGN_October_Update_2019&utm_medium=email&utm_term=0_294c5d36b6-1cf13970a2-514991265

The clarification of what is a service message is helpful. We have provided greater detail to our business which could also be helpful to include here as follows:

- Formal looking
- Content is factual and information based – only contains what is necessary
- No promoting of organisations ideals
- No persuasive language – "**Great**", "**only**", "**just**", "**limited time**", "**remember**..", "**don't forget**", "**simply**", "**special offer**", "**exclusive**" etc
- Performance monitoring is purely to provide a baseline to measure effectiveness of the marketing version against – no sales objective or targets assigned to this activity
- Uses performance of contract legal basis

We do think it would be useful to include in this guide what would be permissible under a "servicing message" in the right circumstances (for example where customer detriment becomes a risk). For example

- The EE example in the text could stray into a conduct issue if customers aren't

presented with an option to get more data when they run out as it could leave them in a vulnerable position with no options to fix it.

- If a proposition contains an incentive, then all components of the proposition should be included in a quote confirmation so that the customer can compare others and make an informed decision – without it, the customer could suffer a detriment of losing out if they don't have all the facts to compare.
- Some of the examples on pages 22 and 23 could also carry a customer detriment risk. Our view would be that in the case of a healthy eating event or a flu vaccine, if the service is free and helpful to customers with no money to be made or purpose to be gained for the organization, then this would not constitute direct marketing. We believe Direct Marketing is about Sales/generating income, hitting targets and generating brand awareness.

5. Regulatory communications – page 21

We didn't understand the section that talks about:

is against your interests and your only motivation is to comply with a regulatory requirement (eg the regulator is requiring you to tell people that they should consider using your competitors' services).

We don't understand what would be against our interests as we believe delivering regulatory communications are in our interests to do. Could this either be explained or reworded?

6. Re-permissioning / changing marketing preference – Page 15

We noticed that clause 194 from the original code has been removed from this draft.

We believe it is responsible to ensure customers know how to update or change their preferences at any time and would ask the ICO to consider putting it back in:-

194. However, we recognise that people can change their minds and that marketing strategies also change. There is some merit in making sure that the information about people's preferences is accurate and up to date. We consider that it can be acceptable to send a message immediately after someone has opted out confirming they have unsubscribed and providing information about how to re-subscribe, or to remind individuals that they can opt back in to marketing if the reminder forms a minor and incidental addition to a message being sent anyway for another purpose. However, organisations must do this sensitively, must not include marketing material in the message, and must never require an individual to take action to confirm their opt-out.

Suggested Example (from the previous code)
A bank sends out annual statements to its customers detailing transactions on their deposit accounts during the previous year. A message is printed at the bottom of each statement to remind customers that they may wish to review their marketing preferences and telling them how to update them.

7. **Privacy Policy Content – page 51**

The draft code suggests that companies should incorporate additional clarity in their privacy policies to call out all of the granular activity that is currently captured by the term 'marketing'. Whilst we appreciate the need for increased transparency, there is a risk that the inclusion of this much detail would make the privacy policy long and

cumbersome and would effectively deter customers from reading it, and those who take the time to read it may not understand this level of detail which could have unintended consequences for the customer, such as unnecessary concerns. A further issue with this requirement for increased granularity is that organisations would find themselves having to update their privacy policies more frequently to reflect each and every change within marketing.

8. Profiling, Segmentation and Analysis

Some of the definitions in here are different to what we use in our industry. We have produced detailed guidance for our policy that could provide this guide with more detail, see an extract below

Our view is that Profiling involves a number of types of processing of personal information:

- Obtaining personal information from various sources (including potentially public sources)
- Analysing or assessing that information
- Creating new data in the form of the profile
- Storing both the base data and the new data
- Sharing the base data or the new data

All of these processes must comply with the GDPR principles and have a lawful basis. Individuals have the right to object to profiling, and specifically profiling for marketing purposes, under Article 21. See the "”Right to Object to Processing Policy”

Profiling without using PII for Marketing Effectiveness

Profiling can be used to support **marketing planning and effectiveness activity** without using PII:-

The purpose is to build up a picture of the existing customer base across products and channels, to further our understanding of what types of customer (in terms of demographic, behaviours, journeys and purchase preferences) apply, complete and retain certain types of policy.

To do this we look at significant patterns emerging from defined groups within the customer base

- For example, if we look at 2 different distribution channels' customer cohorts we can test for significant differences in the two populations on variables such as average annual premium, gender, area location, cover type, payment methods, etc

- In order to test for significant differences, we need samples of sufficient size for our conclusions to be valid. The minimum sample size we can work with is 30 customers.

- Given this output, we can identify customer characteristics (from large samples) that, at scale, can be used to describe customers in a certain group and how they differ from other groups.

- Further analysis of these characteristics can show which variables are most important in driving the significant difference, at a sample wide level

As such, personally identifiable data is not needed for profile analysis. Even variables like postcode will be too specific to use as location proxy as these will likely limit sample size too much to make conclusions viable; in this example the wider "postal area" code could be captured.

This work can (and has) operated independently of marketing and marketing campaigns, simply serving to further the understanding of different groups of customers.

The following checklist for best practice has been developed:

- ✓ Profiling will be done at a group level, not an individual level
- ✓ No individual decisions will be made on profiling data
- ✓ The data we use for profiling is anonymous and doesn't contain PII.
- ✓ We will anonymise the data by doing the following:-
  - Remove last 2 digitals of the postcode
  - Remove house number from the address
  - Remove day and date of birth
  - Remove name

Automated Profiling

Profiling can also be done as a form of automated processing that is commonly used to evaluate the personal attributes of an individual for direct marketing purposes. It is used to predict an individual's personal preferences, behaviour and economic situation in order to provide them with marketing information that is relevant to them. This is not something we do, but we have included it as we know others do. Those that do may be able to provide greater detail on how to do it responsibly.

Profiling for Personalised Online Communications

Automated Profiling activities require a legal basis for processing. It is a requirement of this policy that consent is used as the legal basis for marketing profiling activities that use PII data for "personalised online communications". This means that the legal basis for profiling can be easily and unequivocally evidenced when consent is obtained for direct marketing purposes.

Where this type of profiling is used for personalised online communications purposes, the privacy policy and marketing consent wording must include a clear description of the profiling activities to enable customers to make an informed choice whether they are comfortable to consent to this use case for marketing profiling activities.

Marketing profiling activities which use PII for personalised online communications may only be performed on customers who have provided consent. This requires business areas to have appropriate controls to record that the customer has also consented to marketing profiling activities.

The right to object to direct marketing (including profiling) is an unconditional right and there are no exemptions or grounds to refuse. The use of a single **marketing consent** indicator means that customers can be easily opted out of personalised online communications and related profiling activities at the same time.

Profiling for Active Segmentation

Automated decision-making and profiling is the ability to make a decision without the opinion or consideration of a person. For example, a model or algorithms that calculates and assigns prospects to a segment to determine marketing activity, frequency and content of communications. Because little or no human oversight is involved, this type of marketing is classified as automated decision-making.

By creating profiles of similar people, marketers can more accurately target the right individuals with offers they may be interested in. This also helps to reduce waste, with communications presented to consumers who might be genuinely keen to buy a product or service. There is no significant customer detriment or legal impact. They won't be declined for a product or blocked or be adversely impacted by pricing using this type of Active Segmentation.

This does not mean using a customer's PII to target them as individuals, or to tailor the communication content to them as individuals, as per "Personalised Online Communications", where consent is always required. Active Segmentation enables us to create experiences for segments or groups of customers with similar attributes, behaviours and predicted needs - adapting the experience to be more relevant and thus improving customer outcomes in line with the FCAs guidance on using segmentation and evidencing our target market and value for money requirements.

- In certain contexts profiling for marketing purposes can have a legal or significant effect. This is important for marketers as Article 22(1) acts as a prohibition on solely automated individual decision-making, including profiling with legal or similarly significant effects without consent. However, when a business area can demonstrate there is no legal or significant effect, automated decision making and profiling can be completed under a separate Legitimate Interests Assessment (LIA). This must be performed before any legitimate interests processing activities take place.

- The legitimate interests profiling activities must be recorded separately to direct marketing activities on the business area's record of processing activities. This additional record keeping requirement is caused by the use of a different legal basis than consent.

- Marketing profiling activities must always be explained clearly and adequately in our privacy policy, regardless of the legal basis for the profiling activities.

Profiling for Research & Statistical Analysis (Segmentation)

It is essential for businesses to be able to conduct analysis in order to minimise costs and continue to offer competitive products to customers.

It is also essential that we are able to use techniques as segmentation as it is recommended by our regulator (the FCA who also uses it) in order to understand consumer behavior and ensure products and services are designed to meet those consumer needs: https://www.professionaladviser.com/news/2390837/fca-reveals-types-consumer-bid-drive-product-design and https://www.fca.org.uk/publications/research/understanding-financial-lives-uk-adults

- Internal research and statistical analysis to produce a set of anonymous characteristics (or segments) for customers who are more likely to purchase particular products.

- In the unlikely event that this research and statistical activity involves profiling, the purpose is to produce a set of anonymous segments – it is not used to produce a legal or similarly significant effect on the individuals so the right not to be subject to profiling does not apply.

- The anonymous segments are applied to existing customers on the marketing databases based on their known attributes (e.g. age, postcode or policy type). There is no correlation between the customers used in the research and statistical activities and the customers to whom anonymous segments are applied.

Analysis and Optimisation activities

Customer data can be used for internal analysis to determine the efficiency of direct marketing campaigns. Knowing which types of direct marketing campaigns have worked well is essential to:

- Maintain control over marketing spend
- Optimise marketing investment

This type of processing is a research and statistical activity and does not relate to direct marketing activities.

We are permitted to perform these activities irrespective of the customer's direct marketing consent preference but the activities must not be used to support measures or decisions against our customers.

This works in the following way:

- Equipped with the knowledge around the key characteristics of who has bought in the past, prospect consumers can be prioritised to receive marketing material according to how best they fit the profile of the existing customer base
- This helps to focus marketing activity on those prospects who are more likely to convert
- This can be done with internal data (for cross sell/servicing marketing) or from external data (for acquisition marketing) but both do not need personally identifiable data in order to drive value
- Again this work can operate independently of marketing and marketing campaigns, especially when, for example, estimating market sizes and marketing opportunities

The following best practice checklist has been developed
Anonymise the data by doing the following:-

- Remove last 2 digitals of the postcode
- Remove house number from the address
- Remove day and date of birth
- Remove name

9. Digital Marketing / Third party social platforms

Some of the definitions in here are different to what we use in our industry. We have produced detailed guidance for our internal policy that could provide this guide with

more detail:

Customer Match Profiling

Customer Match and Store Shopping (also sometimes called Similar Audience Profiling): gives advertisers the ability to create and target (or exclude) their very own user lists simply by uploading prospects' PII (typically Email, Telephone and/or Postcode). They can then apply these lists to things like Google Search, Gmail or YouTube, Bing Search, Facebook, Instagram and create customized experiences based on the users' attributes/stages in the purchase journey. These features require you to upload customer data into the 3rd Party Platform. If you enter user data without permission, you are likely to violate GDPR. Key definitions are:

SIMILAR AUDIENCES - Identifying "**lookalike**" customer profiles within the 3rd Parties Customer Accounts for identification for **inclusion or exclusion** from our marketing activity. They use data points from 3rd parties' platforms including contextual and audience signals, building a segmentation of their users who are like the ones that match our profiles. All data is anonymised, and never made available externally.

CUSTOMER MATCH - **Excluding** our customer profiles that match with the 3rd Parties Customer Accounts from marketing activity – to drive efficiencies and improve customer experience.

For targeting purposes

- Customer match involves taking personal user information from your database and giving it to a 3rd Party such as Google, Bing, Facebook, Instagram
- Google has mandated that advertisers **can only upload customer information that they've obtained in the "first party context."** This includes emails collected through website forms, apps, physical stores and in-person events; essentially, instances where the user has demonstrated interest in the advertisers' business
- Under GDPR you need to let your users know how you're going to use their data. And your users have to give you permission to use and transfer their data. Without consent from your users, data uploads to Google can put you at risk for a GDPR violation.
- If you want to use PII in your customer match process, to do it safely, there are the following options:

    i. **Exclude all you user addresses from your upload.** You can do this by deleting your user data from your customer match file before you upload it to the 3rd Party.
    ii. **Let your customers know, at the time of purchase or opt-in, that you're going to be using their data for matching in search campaigns**. Be explicit with this notification in your terms of use agreement. And leave the box unchecked on this notice, so your users can opt-in as required by GDPR.
    iii. **Do a risk/reward assessment** (LIA) if PII is included and consent has not been obtained

For Exclusion purposes

- This is where we would work with a company like Google initially then other 3rd Party platform owners (such as Bing, Facebook and Instagram) to identify our

customers who should be excluded from marketing, and also identify "lookalike" customer accounts that are similar to our customers that can be either included or excluded from marketing

- The 3rd party can also use our L&G customer profiles to identify "similar" customer profiles to those who hold a policy with us. This similarity check enables us to market to prospects who most resemble L&G customers
- The legal basis is legitimate interests and the purpose is limited to the purposes of ensuring that marketing activity designed for attracting prospects is not sent to existing customers. Once we have identified our customers, they will be removed from any marketing targeting
- To do it safely we would recommend:

    - We use anonymised data in our profiling activities
    - **Limited data use**. 3rd party won't use our data files for any purpose other than to create our Customer Match audiences and ensure compliance with policies. They won't use our data files to build or enhance profiles of our customers.
    - **Limited data access**. 3rd Party won't share our data files with other 3rd Party teams other than to create our Customer Match audiences and ensure compliance with policies. 3rd Party use employee access controls to protect our data files from unauthorized access.
    - **Limited data sharing**. 3rd Party won't share our data files with any third party, including other advertisers. They may share this data to meet any applicable law, regulation, legal process or enforceable governmental request.
    - **Limited data retention**. 3rd Party won't retain our data files for any longer than necessary to create our Customer Match audiences and ensure compliance with policies. Once those processes are complete, they'll promptly delete the data files we uploaded via the 3rd Party interface or the API.
    - We will create a **customer data file** based on PII data we hold on customers. All L&G data is hashed and sent securely to the 3rd Party in line with Information Security policies
        - Hashed: email, phone, salutation/ title, first name & last name
        - Data to be hashed using SHA256 algorithm which is the industry standard for one-way **hashing**.
        - The upload will be via the 3rd party API (Google, Bing, Facebook, Instagram)
        - The 3rd Parties are ISO 27001 compliant, and use Transport Layer Security (TLS 1.2) for the upload
        - Un-hashed (non PII): postcode (this is industry standard)
    - 3rd Party processes the data for the purpose of exclusion only and deletes immediately (within 48 hours max)
    - Complete a DPIA and LIA to ensure customers rights can be exercised and balanced.

Social Media

Furthermore, The Data Protection Network has provided industry guidance on legitimate interests and how it can be used as a legal basis for social media marketing which could also be included:

"Example 28 – PROFILING FOR SOCIAL MEDIA TARGETING (page 15)
As part of a multi-media marketing campaign, a furniture retailer wishes to use a social media platform to target advertising to existing customers whilst they engage with social media. They also wish to use an algorithm provided by the

social media provider to better target its advertising to 'lookalikes' - i.e. other individuals who have similar characteristics to that business' own customers that they wish to attract.

The business uploads the minimum required personal data on its customers to enable the social media targeting, but excludes those who have objected to marketing.

Profiling is conducted within the social media platform to enable the targeting, however it is purely for marketing purposes and the business has assessed that it does not result in any legal or similarly significant effects upon those individuals."

10. Joint Controllers for Online Advertising

When we brief our media planners/ buyers/agents with a target audience, we do not need nor want any pii. We simply want these agents to provide us with the greatest return on our media investment.

Please find below a very basic example of how we see this working in real life:
Let's imagine that we are targeting men 25-45, living in central London, who have at least one child. We would instruct our media buyers/planners/ agents to recommend the best combination of media to deliver our message to this audience over a given time period, with a set budget. As part of our brief, we may provide them with an anonymised sample of our audience to help them to create a similar audience. Let's imagine that the planners/buyers/agents come back with a combination of online and offline solutions, for example: Cross track posters in the underground, quarter page in the Evening Standard, banner campaign on the evening standard online, Facebook marketing, Twitter campaign and Sky Sports campaign. We would approve the media selection and then provide them with our ads, and expect them to be placed in the relevant places as per the media plan. At no point do we need to know who has seen the advert, or how many times, Facebook and Sky might need to know this in order to deliver the brief (e.g. to ensure sufficient targets have viewed it a sufficient number of times). This is very much their responsibility as a media buyer/ planner/agent in order to deliver our message to our audience most efficiently. We may need to know the total number of people who have viewed the ads, on each site, at specific points in the campaign, but there is absolutely no requirement for us to access their Pii.

For this reason, we contest your suggestion of a client being a joint controller for lookalike audiences. We do not understand why we would accept data controller responsibility of data for which we have zero control, governance or oversight.

We agree that we are independent controllers of our customers, and would take full GDPR responsibility in the processing of our customer data for the purposes of marketing, including suppression activities.

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

Yes

There are a few ambiguous terms in the code. We would appreciate more clarity on what the ICO's expectations are in relation to these terms:

- **Intrusive profiling** – what does the ICO define as intrusive? Is it using sensitive data like medical data, children's data, data on vulnerable customers,

gambling etc. Or it about the volume of data involved, or is it about where and how it was collected in relation to reasonable expectations? And does this definition consider the unintended consequence, that without some level of profiling there is a risk that consumers could receive marketing that is not targeted or relevant to them which could be a worse customer experience.

- **Vast amounts of data** – what does the ICO consider to be vast amounts of data?
- **Various sources** – what does the ICO mean by this? Could we have more context?
- **Disproportionate effect** – what does the ICO consider to be a good way to assess if something is disproportionate – could we have more detail and some examples?

With the definition of marketing now being expanded to include every aspect of a campaign, there are elements of the process where marketers pay third parties to do elements of the process. Some of the processing that this code now highlights is invisible to marketers and possibly not widely known or understood – for example a marketer could purchase data from data provider that has been modelled but they won't understand the technical way the model has been built. It would be helpful if this guide could provide more clarity on what is expected of a marketer to be responsible for in scenarios like this and if their responsibility needs to widen to be more aware of how suppliers build their models, is there any checklists or guidance the ICO can provide to help those marketer know what questions to ask.

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:

Legal & General

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