Experian's response to

"ICO consultation on the draft direct marketing code of practice"

Response sent 4 March 2020

For any queries please contact:

[redacted]
Experian
Riverleen House
Electric Avenue
Nottingham NG80 1RH
Email: [redacted]@uk.experian.com

Introductory

Experian welcomes the opportunity to respond to the ICO's consultation on the draft Code. We support the broad aims of the Code and the ICO's desire to provide further clarity and interpretation of the relevant data protection laws as they relate to the activities of marketers.

However, we have reservations that this Code will undermine the organisations that the ICO regulates and restrict their ability to grow[1] at a time when the UK needs its businesses to flourish more than ever. As drafted, the Code would go beyond what is required under the current data protection framework and our concern is this would create an uneven playing field for businesses operating in the UK compared with their non-UK based partners and competitors. We also have concerns the Code does not adequately support the delicate balance between the privacy rights of individuals and realising the opportunities that using data for the benefit of individuals and society more broadly can bring.

We perceive a significant shift in the ICO's approach to legitimate interests as a lawful processing ground compared to both its previous public statements and the dialogue that we had with the ICO before the GDPR came into force. This shift does not appear to be justified under GDPR nor is it clear to us how the ICO have considered the costs and benefits of establishing a Code that establishes a new approach over what is required by GDPR[2]. There is nothing in the GDPR to suggest that consent is the preferred basis for processing or that a hierarchy exists for the available grounds and this is echoed in public statements made previously by the ICO[3].

Throughout the Code, by setting out a view that the ICO prefers consent over legitimate interests, the Code appears unbalanced. It conveys throughout an assumption that all data broking and related activities lead to bad outcomes for data subjects.

Unintended consequences

Our concern is that should the ICO maintain this position in the final code, then there will be a range of consequences unlikely to have been intended. The effect of creating an environment where a consent-based model is the only viable compliance model for the marketing industry would be likely to mean:

- An unnecessary burden for the use of public record data that would be particularly heavy or impractical for smaller organisations and result in a deluge of unwanted of notifications to households all over the UK. We can imagine "*GDPR gone mad*" newspaper headlines. We cannot believe that any data subject would welcome this, particularly when practical alternatives exist;
- Building on the above point, a requirement to obtain consent for all processing for marketing purposes could inadvertently work in opposition to the intended aims and objectives of obtaining consent. Individuals could be faced with endless requests for their

[1] See section 1 of: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/300126/14-705-regulators-code.pdf

[2] See Recital 47 of GDPR.

[3] See https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/05/blog-raising-the-bar-consent-under-gdpr/

consent to the point where they become blind and immune to them, resulting in a lack of engagement and clear understanding of what they are providing their consent for;

- A distortion of competition in the market that will favour the major, non-UK online players and disadvantage the many, much smaller, micro or SME businesses in the UK[4]. This is because it is comparatively easy and cost-effective for the vertically integrated, large online platforms to obtain consent compared to almost all UK businesses;
- The knock-on effect is likely to be that data analysis that has a low level of intrusiveness and that helps UK organisations understand their customers better and to find new ones will be driven out; the only useful data analysis that is likely to be left in the marketing world will then be the considerably more intrusive profiling undertaken by the major, non-UK online platforms. Surely, this cannot have been the EU's intention, or that of the ICO now?
- A comparatively harder environment for UK businesses to achieve the innovation, growth and prosperity necessary for the UK to succeed in a post-Brexit world. This will be because it will be harder for businesses to understand the people who make up their customer base; that will mean it will be harder to meet their needs and find more customers like them;
- Using useful insights from data for businesses will be less possible, because the quality and depth of data that marketers will be able to access or use is likely to be severely impacted;
- The legitimate right of businesses to market will become more costly because it will, inevitably, be aimed at much wider audiences decreasing the value per pound that businesses spend. New market entrants will find it even harder to compete with large established competitors;
- Direct mail marketing may well see a return to "Dear householder" mailings, over which data subjects have no right of objection. This could mean individuals actually receive more, but less relevant, marketing communications.

The Code's position is potentially confusing for marketers, many of whom process personal data under legitimate interests for direct marketing purposes where this is allowed, and who have invested considerable time and resources into supporting the legitimate interest model within their businesses. We do not believe the industry is at odds with the overall goal of ensuring individuals have control of their data and that there is transparency around its use, and we assume this is an important goal for the ICO. However, simply moving to a consent based model does not truly provide consumers with the knowledge and understanding of what data does for them, the economy and in many instances the entities they are likely to work for. We are as committed as any business to improving data knowledge within the population, but we do not believe the ICO's approach proposed in the Code will deliver that understanding, instead harming businesses, the economy and innovation.

Best practice

We are supportive of the ICO calling out examples of best practice. However, we think care needs to be taken in the ICO itself recommending such best practices, particularly in areas upon which GDPR is silent. We also believe there is the potential to confuse organisations as it is unclear in the Code where the distinction between best practice and minimum standards for compliance is, appearing to set best practice more as minimum standards. This needs to be addressed if the ICO continues to expect firms to go beyond 'mere compliance'.

[4] See the Competition & Markets Authority interim report at https://www.gov.uk/government/news/cma-lifts-the-lid-on-digital-giants

Our view is that if the Code is to recommend best practice then this should be for the next iteration and the ICO should identify the practices in association and consultation with the marketing industry and its trade associations so that the Code reflects the context of the particular activity, is workable and set at a level that organisations will be able to achieve.

Attitudes of data subjects

We are concerned that the ICO thinks that the understanding of data subjects about how organisations use data about them is much lower than reality. Sweeping generalisations on the issue accordingly influence the Code's view of "reasonable expectations" and fairness.

We believe that most people understand that data is an important part of the modern economy and have a degree of tolerance for marketing where it is relevant to them and that they can control (e.g. by exercising the right to opt-out). Many people expect that organisations they deal with have an understanding of their circumstances and requirements and, as a result, trust them to send communications that are relevant to those circumstances and in their best interests (e.g. customers of a bank would not expect to receive offers for lending products if those products aren't suitable for them). Whilst we do not believe most people understand the inner workings of a model, we do think that most people understand the logic behind why they might be seeing a certain type of advertisement or receiving a certain type of communication. And we have seen no evidence to the contrary from the ICO or elsewhere.

Code structure

We think that the lifecycle approach that the ICO has adopted in structuring the Code is well thought through. It should help marketers follow the guidance in a logical way, reflective of the process flow that they undertake internally when carrying out their direct marketing activity.

Transparency

We welcome and support a Code that encourages organisations to continuously review and adapt their approach to transparency. However, there can be no 'one-size-fits-all' approach.

About Experian

Experian is a credit reference and data analytics business, providing services direct to consumers and to businesses across a number of sectors. We provide credit data services to lenders and operate in the price comparison website market.

Experian's data and analytics help people, businesses and organisations protect, manage and make the most of their data, creating better business and consumer outcomes and building stronger customer relationships.

Experian helps people, businesses and organisations to:

- **Lend and borrow responsibly:** by gathering information on past and present credit commitments, such as loans, mortgages and credit cards, Experian helps lenders to understand whether people and businesses can manage their debt repayments affordably, so they can borrow and lend responsibly.

- **Treat people and businesses fairly:** because Experian helps organisations make decisions based on facts, they can treat people and businesses fairly and consistently, which in turn helps people to access credit.
- **Access vital information more easily:** easily available and understandable information allows people and businesses to prove their financial track record to organisations, so they can get the best deals.
- **Make better, more efficient decisions to create better business outcomes:** by gathering and analysing information supplied by people and businesses, organisations can make quicker decisions, now taking seconds and minutes instead of days. Organisations need to make fewer manual checks which means less administration and fewer bad debts. This means the cost of extending credit is lower.

Experian responses to the ICO Consultation questions

Q1 Is the draft code clear and easy to understand?

☐ Yes – in many places

☒ No – but not clear in others

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

Many parts of the code are very clear and provide welcome further guidance and detail on key topics. However, there are sections of the code where we would welcome further clarification and consideration. We set out our comments below.

1. Definition and scope of direct marketing

The detail provided by the Code around the definition and scope of direct marketing (starting on page 14) is useful, particularly as the concept of processing activities for "direct marketing purposes" is not well defined in either GDPR or PECR.

We welcome the clarity around direct marketing being defined as wider than just sending direct marketing communications, to also include all processing activities that lead up to, enable or support sending those communications. This will particularly help organisations in appreciating that data subject rights like the right to object extend not only to the sending of a marketing communication but also to any associated profiling of the data subject to support direct marketing.

The section on what constitutes a service message is important as many organisations struggle to draw the line between a "marketing communication" and a "service communication" (page 19). The Code usefully expands on this, but it takes a strict yet inconsistent approach. In particular, the Code says that when determining whether a communication is service or marketing in nature, "*a key factor is likely to be the phrasing, tone and context*". A message that actively promotes a product or service will be marketing in nature, but a message that takes a "*neutral tone*" and is informative is more likely to be viewed as a service message. However, the Code goes on to say that brands cannot "*avoid the direct marketing rules by simply using a neutral tone*". The extent to which tone is relevant is therefore unclear and worthy of further clarity in the final guidance.

The Code needs to carefully consider the practical realities in the examples it uses to illustrate the differences between a marketing message and a service message. For example, on page 20, the Code discusses the example of a mobile phone operator who can notify individuals that they are reaching their monthly limit but can't, in the same communication, then provide them with a special offer to buy more data because this then tips it over to a direct marketing message. Whilst we can understand how the ICO would conduct such a legalistic analysis, from a data subject's (that is, customer's) perspective it makes no sense that they aren't offered more data in the same communication about approaching a limit. Surely a data subject, a customer, would expect to see this in communications because, after all, existing customers are not going to get this additional data from anywhere other than their own mobile operator.

Similarly, the Code suggests that a GP can send an SMS stating that their flu clinic is now open, but they then can't then in the same service message provide the contact details of the surgery if

individuals would like a vaccination (page 22). In our view, most data subjects, patients, would actually expect and want to see these two pieces of information together and think that their GP was providing a useful service in doing so. Notwithstanding, we would ask the ICO to consider this example and the logic it is applying in light of the current health threat we are facing globally. Would anyone really interpret the law such that it would be illegal for a GP to tell people about how to receive a vaccine for Coronavirus should one be made available? We think not and therefore we believe the interpretation being made – and certainly the example given – is erroneous.

The Code also discusses whether regulatory communications are "direct marketing" (page 20). Notification correspondence to individuals to inform under article 14 GDPR falls under this category and the Code says that such a communication needs to be:

- neutral in tone (without encouragement or promotion);
- sent solely for the benefit of the data subject;
- is against the organisation's interests; and
- the only motivation is to comply with a regulatory requirement.

We do not understand the basis upon which the ICO has decided that these are the requirements. Not only does this appear to be an unobtainably-high threshold to achieve, the requirements are contradictory. The last 2 requirements are particularly difficult to understand and contradict each other, as an organisations regulatory obligations often align to the interests of that organisation (e.g. although a bank has a regulatory obligation to not lend irresponsibly, it is also in the interests of the bank that customers do not miss payments). We would like greater clarification about the ICO's view on what such a notification would look like?

Lastly in this section, we note on pages 13 and 14 of the Code that:

> "*GDPR and PECR do not define the term 'direct marketing purposes', but clearly it is intended to be wider than simply sending direct marketing communications. The focus is on the purpose of the processing, not the activity. Therefore, if the ultimate aim is to send direct marketing communications, then all processing activities which lead up to, enable or support sending those communications is processing for direct marketing purposes, not just the communication itself.*
>
> *Therefore, if you are processing personal data with the intention that it is used for communicating direct marketing by you or a third party you are processing for direct marketing purposes. For example, if you are collecting personal data from various sources in order to build up a profile on an individual – such as the products they buy, the services they like to use, or the causes they are likely to support – with the intention that this is used to target advertising at them, whether by you or by a third party*" (emphasis added).

Notwithstanding our earlier comments, this is a very broad definition. Related to this is the Code's stance on "suppression lists" – it states (at page 111):

> *"You should not confuse direct marketing suppression lists which are used to record an individual's direct marketing objection with a screening list that you have decided to use to*

screen out certain people because they do not fit the particular direct marketing campaign that you or a third party are running"

Taken together, the Code suggests that some products designed for lenders might be for "direct marketing purposes". The Code provides the following example:

> "*A lender decides they only want to send direct marketing to customers who have balances above a certain level. It screens out anyone with a balance that does not meet that threshold and creates a list of those people above it so it can use this again in future. This is not a direct marketing suppression list because it is unrelated to an individual's wishes*"

However, the Codes fails to acknowledge that the purpose of a such a product might be to prevent over-commitment/promote responsible lending and assist lenders in meeting other regulatory requirements laid down by the FCA or in statute.

The position of the Code here is inconsistent with the ICO's comments on page 35 of the Code, which recognises that:

> *"direct marketing has the potential to have a significant negative effect on the individual, depending on their personal circumstances. For example, someone known or likely to be in financial difficulties who is regularly targeted with direct marketing for high interest loans may sign up for these offers and potentially incur further debt"*

The whole point of such a product is to ensure that this doesn't happen, and as such we would ask that the ICO spends time with Experian and other data providers to truly understand how such data is used, the role it plays and the actual impact on consumers.

2. Data protection by design, accountability and DPIAs

Article 35 GDPR makes it clear that a DPIA is a requirement for processing that is "*likely to result in a high risk to the rights and freedoms of natural persons*", which appears contradictory to the Code which establishes a much broader application of the DPIA requirements for organisations involved in direct marketing activities. The Code suggests instead that all key activities of data brokers will require a DPIA and as such, establishes a much higher requirement for those firms. Indeed, the Code recommends (page 29) that it's good practice that all direct marketers will need to carry out a DPIA on their activities.

The purpose of conducting a DPIA is to ensure risks are identified and mitigated, and therefore it follows that processing which could have a significant effect on the lives of individuals is more appropriate for a DPIA than processing that does not have such an impact. As written, the Code could drive organisations to complete DPIAs for processing activity that is benign to individuals just because it has a link to direct marketing (e.g. marketing analysis tools using very little personal data, which is clearly at a different end of the scale to facial recognition tools for spotting criminals in football crowds). DPIAs must be targeted at processing activity that is likely to have a high impact on individuals and should not arbitrarily be required just because a processing activity is part of a broader purpose which the ICO considers to be high risk. Had either the EU or Parliament intended an effect that all processing needed a DPIA then it would have made this clear in the legislation.

Further clarity on this point would be appreciated as if DPIAs are required for all direct marketing activities using personal data, this could be a real burden for smaller organisations. This might be regarded as "excessive" and risks producing a counter-productive, box ticking culture.

3. Lawful grounds for processing and legitimate interest

Overall, the tone of the parts of the draft which discuss processing grounds and the viability of legitimate interest in a direct marketing context do not strike the right balance in recognising that legitimate interest can work well in many direct marketing contexts – and in certain circumstances be more meaningful and give greater control to data subjects.

Where consent is not required under PECR, the Code clarifies that legitimate interests may be able to be relied on to process personal data for direct marketing activities. However, the Code then goes on to include a contradictory good practice recommendation around consent at page 31:

> *"Get consent for all your direct marketing regardless of whether PECR requires it or not."*

In the run up to the GDPR the ICO encouraged organisations to look at all potential lawful grounds. For example, the Information Commissioner made this clear in a blog post in August 2107 entitled "*Consent is not the "silver bullet" for GDPR compliance"* when she said:

> *"So, let's be clear. Consent is one way to comply with the GDPR, but it's not the only way."*
>
> *"Headlines about consent often lack context or understanding about all the difference lawful bases businesses & organisations will have for processing personal information under the GDPR"*

The Code is seeking to create a preference for a consent-based model over any other lawful basis and such a preference is only suitable for Parliament to establish.

Whilst the Code does acknowledge legitimate interests may be appropriate, the Code goes further and determines several areas where the ICO considers that legitimate interests may be difficult to rely on in practice, that the legitimate interests test will rarely be met and consent will therefore be required. These examples include "intrusive profiling" (on pages 4 and 56), tracing (page 62), the use of social media "list-based targeting" tools, location based direct marketing and selling or sharing data. A move to consent as the only viable compliance model may prove impossible to achieve.

A particular area identified by the Code here includes, on page 36:

> *"collecting and combining vast amounts of personal data from various different sources to create personality profiles on individuals to use for direct marketing purposes"*

Further on page 58, the Code says:

> *"If explicit consent is not required and you are considering using legitimate interests as your lawful basis, you need to give careful consideration to the three-part test. 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"*

The ICO needs to provide much greater clarity on what it means by "personality profiles" and "intrusive". Does this mean the types of profile that an online platform might build up about a person based upon their friends, location, "likes" and real-time activity? Does it include, at the other end of the scale, socio-demographic segmentations that are built largely from aggregated, geographic and/or census data?

The above would also imply there are instances where transparency is achieved and the ICO have such examples the rest of the industry could follow. Could these be shared with us and others?

We are concerned that the ICO's view about where the bar sits as to "intrusiveness" or "profiling" may be so low as to bring in virtually any sort of processing activity. The danger with setting the bar too low is apparent from the work that the FCA has conducted in the field of behavioural economics. For example, in its article[5] entitled, *"Don't look here. Do risk warnings really work?",* there is a clear read-across.

In our opinion, the ICO needs to consider the wider implications for organisations in applying the ICO's proposals and how to strike a reasonable balance.

4. Switching lawful processing grounds

On page 30 the Code addresses sharing data and switching legal basis and states that:

> *"if PECR requires consent, then processing personal data for electronic direct marketing purposes is unlawful under the GDPR without consent"*

It continues to suggest that an organisation cannot use legitimate interests to further process data if unlawful under other legislation. This suggests that if you gather consent to send electronic marketing to customers, you would also need consent for any other processing activities that are related to electronic marketing, including any subsequent profiling or segmentation to select the individuals for marketing.

The PECR consent requirement and the options for choosing a legal basis under GDPR are separate matters. It is our view that that there is no reason why different activities at different stages of a process cannot be based on different processing grounds, particularly where the switch of processing grounds has no impact on the rights and protections afforded to individuals. For example, when using profiling for the selection of individuals for marketing, consent is not required if the profiling does not have a legal or similarly significant impact, which most profiling for marketing purposes does not have (and which the Code itself acknowledges).

Is this the ICO's intention that this logic applies outside of electronic marketing? Why should one company's legal basis influence another? How could the recipient of the consented contact data for postal marketing undertake any further processing of the data once they receive it, including any profiling or do any suppression matching prior to our sending a communication if Legitimate Interests can't be used for this further processing?

The Code states that "*This misrepresentation and the impact on the effectiveness of consent withdrawal mechanisms would cause a problem with the balancing test*" but it is not upon what

[5] https://www.fca.org.uk/insight/dont-look-here-do-risk-warnings-really-work

basis the ICO has drawn this conclusion. Under a well thought through legitimate interests framework, data subjects can object to direct marketing at any time either with the organisation or with the third party and it would be effective within a reasonable time frame.

5. Public data & Article 14 requirements

As you know, Experian is supportive of the requirement for organisations to make their personal data processing activities transparent to data subjects. In this context, the Code suggests that once an organisation has collected publicly available personal data, it will be a controller of that data and must comply with GDPR by, for example, disclosing its processing (including the source of the data) in its privacy notice and identifying a lawful basis (page 51). If the ICO believes greater transparency is required, we would strongly encourage them to work with their counterparts in the public sector to raise awareness about public registers and how they are used by organisations. It is our view that individuals do not consider data held on public registers to be private, they are by inference matters of public record.

If the ICO believes that notification of the use of public data to every individual is required by every organisation that uses that data, and the "disproportionate effort" exemption cannot be relied upon, then the implications are significant for both organisations and data subjects. This could put most businesses that process such data for direct marketing purposes out of business, or at the very least cause them to incur huge costs in executing on this requirement.

Until now, companies that collect data from public sources, such as Companies House or edited electoral roll, have often relied upon the exemption to help cope with the challenges to their business. If it is no longer applicable, it would have a knock-on effect to all the companies that use this data for customer acquisition campaigns or data products.

Again, we do not believe that this was an intended effect of GDPR. Recital 73 specifically envisages that requirements as to public registers could be subject to specific legislation of Member States. The UK has a long-established series of registers. It is our view that it was never the intention of a relevant legislature to restrict the established practices in Member States in relation to public registers or impose as mass notification requirement because:

- The EU did not enact any such provisions; and
- Given the particular context of Brexit, the UK enacted the Data Protection Act 2018, Parliament specifically considered many derogations and other provisions and yet it chose not to introduce any further particular requirements as to public registers.

From the perspective of the data subject, the impact would potentially be hundreds of direct notifications that it is hard to imagine doing anything other than creating mass annoyance. Of course, of a lesser concern would be the massively unnecessary waste of paper.

In addition, we do not agree that there is any requirement to provide direct notification to data subjects where they have already been provided with adequate notification.

The effectiveness of direct postal notifications of the type the Code suggests has repeatedly been found to be ineffective in bringing to the attention of individuals issues of which regulators consider they should be made aware[6].

We can write to you with our more detailed thoughts on, for example, Parliament's intention as to the electoral roll should you wish. In any event, article 14(5)(c) and recital 62 of GDPR explicitly state that notice is not necessary to data subjects "*insofar as . . . the recording or disclosure of the data is expressly laid down by law*", which is the case in respect of the EER and other public data sources where disclosure is mandated by law.

We strongly encourage the ICO to work with the marketing industry and others to find a solution that works for both data subjects and for organisations, whilst fulfilling the aims of transparency in the use of public sources of personal data.

Here are two simple examples, which we do not intent to an exhaustive list of alternatives:

- Local authorities have a statutory duty to send households an annual notice in connection with the electoral roll. With a few changes, an existing process could be adapted to provide greater transparency without the need for mass notification by many organisations to every individual;
- When an organisation starts Court proceedings against an individual, the Civil Procedure Rules specify the information that the Court must send to the Defendant. A few changes to that documentation and association pages on gov.uk could provide greater transparency to Defendants about the implications for them of the Court making a judgment against them.

Both of the above approaches would help the ICO in its's aims but in a way that also complies with its obligations under the Regulators Code, namely, in a way that does not impose unreasonable burdens on the organisations that the ICO regulates and, thereby, helps them to continue to grow.

6. Duration of consent

The Code reminds organisations that consent to marketing does not last forever. It goes on to say that the validity of consent depends on the particular circumstances of the case including:

1. the context in which it was given;
2. the nature of the individuals relationship with the organisation; and
3. the individual's expectations.

We do not understand upon what basis the ICO draws this conclusion. GDPR does not impose any duration requirement for consent in the marketing context and, logically, there is no reason to do so because data subjects have a right to object to processing of data for marketing purposes. What is the ICO's view as to the legal basis for suggesting in the Code at page 42 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."*

[6] See for example OFGEM's "Cheaper Market Offers Letter" trial involving 100,000 letters sent out to individuals about cheaper energy supply, resulting in less than 2% of individuals changing energy supplier, despite the potentially significant direct financial benefits of such a switch. See https://www.ofgem.gov.uk/publications-and-updates/results-cheaper-market-offers-lettertrial.

It is our belief that had either the EU or UK legislature intended consent to be time-limited in the context of marketing then it would have so provided. Had that been the intention, then one might have envisaged there to have been no need to include a right for data subjects to object to marketing processing.

Once again, we have real concerns that the Code's views are academic in nature rather than practical for organisations to implement. How can the Code suggest that the duration of marketing consent will be context-specific and yet set a time-limit? What about data collected for insurance renewals, holidays, replacing cars? There are many reasons why an organisation might delay communication until the most relevant time for the data subject. For example, what would be the point of an insurance company promoting its home insurance to a customer only a few months after that customer has taken out a new policy. The outcome here would be a lose-lose because a customer is likely to think the insurer inept and the insurer would view the timing of such a communication as a waste of time. The current Code accepts that there could be circumstances where consent can remain valid for longer periods, providing examples where marketing activity could be for seasonal products or insurance renewals. By setting a hard time-limit, the new Code appears to conflict with previous guidance from the ICO and we would like to understand the drivers for this change in approach – has the ICO seen evidence of harm to individuals or poor outcomes? It is also unclear what the ICO's basis is for assuming that placing an expiry date on consent is what individuals expect.

We believe that the ICO needs to engage in a much wider dialogue with industry and include that in a further iteration of the Code. Otherwise, the ICO is seeking to impose burdens on those it regulates that make it hard to comply and are likely to stifle growth.

7. Incentivisation of consent

While the Code makes it clear that organisations should not coerce or unduly incentivise consent to marketing, the Code indicates that some element of incentivisation is permitted (page 33). The Code gives the example of joining a loyalty scheme, the whole purpose of which is to access money-off vouchers.

However, when it comes to incentives, the ICO warns organisations '*not to cross the line*' and unfairly penalise those who refuse to consent to direct marketing. The ICO needs to recognise the practical reality that if the ICO sets the bar inappropriately then organisations will simply stop providing loyalty schemes or reduce their value. That is likely to annoy data subjects and result in a poor outcome all round. Again, we could see "GDPR gone mad" newspaper headlines. We should also bear in mind a loyalty scheme is another form of marketing where the consumer is incentivised to buy from the vendor. To that end there is no difference to an offer providing a 10% discount for new customers, or 'buy one get one free' offers. They are all marketing vehicles and it would be odd to place one above another in terms of what it is seeking to achieve for the vendor making the offer. Additionally, the attractiveness of these programmes seems to confirm that individuals do expect this type of activity to happen and that they derive some value from the data exchange.

In our view, the Code needs to provide much greater clarity as to what this means in practice to avoid organisations getting their clarity ex post through enforcement action.

8. "Tracing" services

Similar to the examples that we criticise in connection with GPs and mobile communications operations in section 1 of this answer to Question, we believe that the Code fails to recognise the practical issues of the real world. The suggestion that organisations seek to "trace" individuals to bombard them with further marketing is an extreme interpretation.

The views expressed in the Code at page 60 relating to tracing to find new addresses of individuals who have moved, are extremely conservative and, again, seem to be contrary to the provisions of GDPR and as such, should be a matter of policy for Parliament if the requirements for organisations need to be changed. As we have already pointed out, GDPR provides a right for data subjects to object to processing for marketing purposes. It also imposes obligations on organisations to keep the data that they hold accurate and up-to-date and as drafted the Code undermines this core GDPR principle.

The Code suggests that irrespective of how clearly an organisation explains this activity in its privacy notice, or through other mechanisms, this will remain inherently "unfair" to the data subject. We do not understand upon what legal basis the ICO has drawn this conclusion.

Rather than a "blanket ban" on this kind of processing activity, surely if the individual has been told about this activity this ought to be a key consideration as to whether it is within their "reasonable expectations"? And therefore, if legitimate interest is the processing grounds this should be fully examined and documented in the appropriate Legitimate Interests Assessment, such that the balancing of the interests of the organisation with those of the data subject are properly examined.

9. Profiling

We have already touched upon profiling.

We suggest that there is a mechanism in place to assess the impact of "profiling", namely, through the requirement to undertake a Legitimate Interest Assessment (LIA) when undertaking such processing on the grounds of legitimate interests. This would need to include assessing whether such activities were in the reasonable expectations of the individual and that there was appropriate transparency in place. If the conclusion of the LIA was that it was not in the reasonable expectations of the individual and there was insufficient transparency, the assessment would fail, and the processing activity would need to find an alternative ground for lawful processing or cease that processing.

It is unclear to us whether the Code is seeking to reiterating the concept of a LIA (if so, it does not do so clearly enough) or suggesting that certain types of profiling would be, by their very nature, be more 'intrusive' than others? In our view, the ICO needs to consult widely in the industry and consider including details around this subject in a future iteration of the Code.

10. Using third parties to send direct marketing

At page 82, the Code states that if an organisation asks a third party to send marketing messages by email it is likely to be the instigator of this message and both it and the sender would require consent under PECR.

We understand that the ICO is setting the expectation that the organisation and the sender would be named at the point the data subject provides their consent.

However, some email mailing models work on the basis that the delivery of the email communication is made by the organisation from which the consumer originally gave their opt-in consent to receive relevant marketing communications. For example, in the context of a person signing up to a website offering money-off coupons, the website may do the mailing of coupons from third parties.

Following this example, the third party will provide their "content" with the discount website. The content will include the branding of the third party. However, the "From" line would make it clear that it is being sent from the discount website and the subject line will be descriptive and meaningful to the data subject. The website's contact details and opt-out mechanism would appear prominently in the footer of the email.

We suggest that in such a model, data subjects will not be confused about such content. However, the Code fails to explore this model and the industry will welcome clarification.

11. Social Media Targeting

The Code includes guidance on commonly used methods for creating social media "audiences" - tools such as custom audience and lookalike targeting (page 89). The ICO stresses the importance of transparency and the need to be upfront about the processing.

However, the Code states that consent is likely to be the most appropriate legal basis for processing in this context, as it would be difficult to meet the three-part test for legitimate interests. It gives no basis for reaching this conclusion.

If an individual has a first party relationship with an organisation and a first party relationship with the social media platform, we do not understand why legitimate interests cannot be the basis for processing assuming this clearly explained in a privacy policy and taking into account the right to object.

As we have already said, we have genuine concerns that the impact of the ICO's view will be to reinforce the position of the global, non-UK online platforms since it will become, in practical, very difficult to create audiences from third party data compliantly.

Publishers will, therefore, will have fewer options for targeted advertising, and less third-party data to profile their customers. This will disproportionally affect smaller publishers.

Major brands are likely to spend more with the major online platforms, who will still have a continuously growing reach through the use of their extensive first party data.

There are a wide variety of services offered by social media platforms, but the Code addresses them together and directs that all need consent. For example, there are methods of creating audiences where the personal data can be pseudonymised for matching purposes and, therefore, where additional controls and mitigations could be referenced in any related Legitimate Interests Assessment as protections for the data subject. More granular examination in the Code of each tool available on the various social media platforms would be useful to indicate what processing grounds the ICO believes might be appropriate for each tool.

Given the ICO's concurrent work on real-time bidding, clarity around what, exactly, the Code is seeking to address in the context of social media platforms is essential.

12. Matching/appending

In relation to "matching/appending", at page 60, the Code says:

> *"In most instances, buying additional contact details for your existing customers or supporters is likely to be unfair, unless the individual has expressly agreed. This is likely to be true no matter how clearly you explain it in your privacy information that you might seek out further personal data about individuals from third parties. This is because it removes people's choice about what channels you can contact them on for direct marketing purposes"*

In this context, does the Code intend "expressly agree" to mean consent? This paragraph also assumes that acquiring additional contact details is merely about finding more channels through which to send marketing to data subjects. GDPR expressly provides that data subjects should have a right to object to processing in the context of direct marketing and so there is a legal presumption that such processing is permissible subject to the provisions of GDPR and the right to object. Had the EU intended that such processing was only possible with consent, then it would have so legislated.

The Code is seeking to extend the law considerably beyond the legislation.

13. Reliance upon consent to process special category data

The Code makes clear that organisations can only use special category data for marketing purposes (which includes profiling/drawing inferences about likely race, ethnicity, political beliefs, health or sexual orientation) if they have the individual's explicit consent (page 38).

The Code could benefit from a greater elaboration of how the exemptions in article 9 GDPR apply otherwise there is conflict between a generalised statement from the ICO and the law as set out in the GDPR and the Data Protection Act 2018.

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?

See our detailed comments in response to Question 1.

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

☒ Yes - to an extent

☐ No

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

We agree that the Code covers the significant issues relating to direct marketing. However, as we have mentioned in response to Question 1, there are numerous contradictions and other clarifications that would be welcome.

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

It is evident from the code that the ICO see the content of Legitimate Interest Assessments as being crucially important to support an organisation's legitimate interest basis. Whilst we appreciate that the ICO has issued guidance on legitimate interest, we believe that such guidance will need updating in the light of any final issued Code.

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:

The Code is well set out and the "lifecycle" approach to the topics discussed adds logic to the structure of the Code.

The "At a glance" summaries at the start of each section are useful in directing attention to the key points in each of the sections.

The signposts for further reading are helpful and direct readers to other ICO guidance 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 :

As the Code discusses "transparency" so much it would be useful to provide readers with some examples of "good" and "bad" transparency in the context of direct marketing. Particularly, more examples of how transparency requirements can be met in the eyes of the ICO would be helpful although we repeat our comments about the need for greater engagement around these issues with the wider industry.

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

No

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:

Experian Ltd

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