Submission to ICO Consultation on draft Code of Practice for Direct Marketing

Privacy international

4 March 2020

Questions

Q2 Does the draft code contain the right level of detail? (When answering please remember that the code does not seek to duplicate all our existing data protection and e-privacy guidance)

☐ **Yes**

☒ **No**

If no please explain what changes or improvements you would like to see?

The draft Code is already extensive in its length. However, too often space is taken up explaining the provisions of the law as opposed to guidance on its practical application in the context of direct marketing. In our view some more detail and examples (as set out in our response to Q6) are needed in order to promote good practice.

Areas of the code which could benefit from some further detail/ clarification are:

- **PECR & GDPR, especially re Soft Opt-in** (p31 & 72)

In our view further clarification is needed in the Code on the interaction between PECR and GDPR in particular when it comes to what the ICO describes as the 'soft opt-in.' Whilst the table on p31 is helpful and this type of presentation can provide welcome clarity, more context is needed. For example, the box stating that there is no requirement under PECR to obtain consent for "Emails/texts/in app/in-platform direct messaging to individuals – obtained using 'soft opt-in", would benefit from further context. Context is not provided until pages 72 and 74, which then point to further sections on online advertising and there is a risk of confusion in terms of the need for a legal basis under GDPR for such direct messaging. That a soft opt-in is not the equivalent to valid consent as a legal basis under GDPR should be made clear and explicit.

- **How long should we keep personal data for direct marketing purposes** (p41)

We note the statement, "If you no longer need the personal data for your direct marketing purposes you should erase (delete) or anonymise it (i.e. so it is no longer in a form that allows the individual to be identified)." We recommend adding further detail and at the very least signposting to what anonymisation means and how this may be done. As the ICO is aware, anonymisation is an extremely complex process.

- **Publicly available data** (p51)

It is important to underline, as the draft Code does, that such data is not 'fair game'. We also question the inclusion of social media in this section. The scope for abuse is vast, from Cambridge Analytica to the recent Clearview scandal, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement More detail should be added here to underly the need for a legal basis.

- **Profiling** (p56 on)

It is essential to further highlight the role of third parties in profiling, including for the sourcing and analysis of data. In the examples of profiling on page 57, a number will undoubtedly involve third parties. For example, predicting what products an individual might buy based on their online browsing history - how is the controller getting access to this history, on what basis, and with what data is it being combined, again on what basis?

In our view, there is a need to caveat the following statement on page 58 further "You can profile aspects of an individual's personality, behaviour, interests or habits in order to use this for direct marketing purposes, but you must still comply with the direct marketing rules and where applicable the rules on automated decision-making." The Code should be careful not to endorse this practice and also repeatedly make clear, as it seeks to do, that any such profiling would need to be transparent, fair, lawful and comply with the other principles, such as purpose limitation and data minimisation, and all further requirements of GDPR.

Further detail and examples on what constitute a 'similarly significant effect' would be helpful, including for example inferences about special category personal data.

- **Enrichment** (p59)

In this section, we recommend that it is made clear that such enrichment is unlikely to be permissible, even if notified in a privacy policy. Too often, such activities are buried deep in privacy policies or other notices. Furthermore, adding that even notified, you need a legal basis and to ensure fairness.

- **Online advertising and new technologies** (p85 on)

Given the changes in technology and advertising and marketing, this section is key to the Code and will be the most important in guiding compliance on the practical application of the law and encouraging good practice. However, it currently lacks sufficient detail together with examples about what is acceptable and importantly what is not.

This section is essential as across the board in online advertising and use of new advertising technologies (https://privacyinternational.org/topics/adtech) - whether tracking (https://privacyinternational.org/explainer/2976/how-do-tracking-companies-know-what-you-did-last-summer), cookie banners, (https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent) or Real Time Bidding (https://privacyinternational.org/explainer/2974/why-am-i-really-seeing-ad-answer-might-be-real-time-bidding-rtb) we see blatant disregard for the provisions of both GDPR and PECR. This is why Privacy International complained about AdTech and Data Broker companies https://privacyinternational.org/legal-action/challenge-hidden-data-ecosystem and are waiting for the ICO to take action as part of its ongoing investigations into data brokers, credit reference agencies and AdTech.

In this section it is important to be clear that the issue is not just people not understanding the use of such technologies but that this is also a result of the design and implementation

of many of them. They are hidden by design and default and raise fundamental questions in terms of compatibility with data protection principles, including transparency, fairness, lawfulness, purpose limitation, data minimisation, accuracy, storage limitation and integrity and confidentiality.

- When mentioning consent in this section (p88) it is important to emphasise the right to retract consent at any time. This is particularly important given the way that consent is being implemented in practice.

- In the third example on social media (p89) in direct marketing, we suggest separating it into two points: data observed through the use of the platform and data observed outside of the platform, collected through tracking techniques or technical tools such as an SDK for an app.

- In the section on targeting users on social media (p90), we recommend making clear the risks of how data collected on your site might not only be used by a controller but also by the third parties they rely on and the need to assess the impact of such data sharing.

- In the section covering targeting people similar to customers/ supporters, (p91) we suggest making clear that it is very difficult to see how such processing is evet going to be fair/ transparent/ have a legal basis. There are also issues from the perspective of purpose limitation.

- The section on facial recognition or detection (p93) needs further elaboration including in relation to fairness, legal basis and more. There should also be a section on the application of emotion recognition technologies for direct marketing and the resulting myriad of issues in terms of compliance with the frameworks.

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:

Please see our response to Q2. In particular we consider that further elaboration on online advertising and new technologies, with examples, as well as the role and risks of third parties, as data sources and recipients, would be beneficial.

We also recommend that the Code address the data sharing role that companies endorse when implementing third party tracking methods as part of their direct marketing. It should be made clear that the use of third-party technologies for programmatic advertising may result in undesired data sharing with third parties, and the risks of infringing the provisions of GDPR and PECR.

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:

In our view more examples should be added throughout, in particular examples using 'new technology' should be used throughout the Code and not only limited to the final section. This is essential to bring the Code to life and make clear what practices are not acceptable.

Our suggestions of where examples should be added are as following:

- **What does 'directed to' mean?** (p16)
    - Add examples re targeted advertising/ messaging e.g. smart TVs, geotargeting, use of FB or publishers.

- **What is 'solicited' and 'unsolicited' marketing?** (p17)
    - Add example re use of cookies or other tracking tech - and clarify that 'accepting', does not mean behavioural advertising (as a result) is solicited.

- **What is sugging** (p18)
    - Add example, such as Vote Leave's use of a football competition as a data gathering exercise: https://www.theguardian.com/politics/2018/may/20/vote-leave-scrutiny-

facebook-data-football-contest-brexit

- **Buying/ selling lists** (p52)
    - Add an example that illustrates the difficulty of compliance in this industry, we have set these out in detail in our complaints against data brokers, Acxiom, Oracle, Experian, Equifax and others: https://privacyinternational.org/legal-action/challenge-hidden-data-ecosystem

- **Customer family/ friend contacts** (p54)
    - Add an example, this could be an app which by default has permission or seeks permission to access contacts, or the use of networks on social media and the controversy around the Facebook 'People You May Know Feature': https://gizmodo.com/people-you-may-know-a-controversial-facebook-features-1827981959

- **Article 22** (p58)
    - Add more examples, this is particularly important in order to illustrate what is not permitted and also what may constitute a similarly significant effect.

- **Enrichment** (p59)
    - Add example, see for reference our complaints on data brokers and ad tech companies: https://privacyinternational.org/legal-action/challenge-hidden-data-ecosystem

- **How does GDPR apply to online advertising** (p88)
    - Add more examples, including in relation to data that reveals special category personal data. See for example, mental health website practices on tracking and consent: https://privacyinternational.org/long-read/3194/privacy-international-study-shows-your-mental-health-sale This further example regarding the sharing of depression test results: https://privacyinternational.org/news-analysis/3188/taking-depression-test-online-go-ahead-theyre-listening
    - Add example to warn against bundled consent.

- **Custom audience** (p90)
    - Add example to illustrate problems further and these kinds of features are currently problematic. For example, we set out in this piece problems with current use and practices related to Facebook transparency: https://privacyinternational.org/long-read/3372/no-facebook-not-telling-you-everything

- **Direct Marketing on TV** (p92)
    - Add examples, see for reference our explainer: https://privacyinternational.org/explainer/3358/your-tv-also-watching-you and piece on the use of TV in political advertising https://privacyinternational.org/long-read/3355/smart-tvs-and-political-ads

- **In App advertising** (p95)
    - Add examples, see for reference Privacy International's work illustrating problems with app data sharing and GDPR / PECR infringements.
        - Technical analysis of apps using the Facebook SDK and leaking data to Facebook: https://privacyinternational.org/appdata
        - Cheap phones embedding trackers: https://privacyinternational.org/long-read/3226/buying-smart-phone-cheap-privacy-might-be-price-you-have-pay
        - Menstruation apps sharing personal data: https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruation-apps-are-sharing-your-data

- **Data Broking service** (p102)
    - Add examples to illustrate the difficulty of using such services and complying with the law. For reference, see our submissions on various companies: https://privacyinternational.org/legal-action/challenge-hidden-data-ecosystem

- **Individual Rights**
    - Individual rights are a core part of GDPR; however, we have concerns about the ability to exercise these rights, in particular as regards online advertising and use of new technologies. We have observed numerous challenges, as illustrated:
        - in our submissions on data brokers, credit reference agencies and AdTech companies re access and right to object: https://privacyinternational.org/legal-action/challenge-hidden-data-ecosystem as well as right to erasure: https://privacyinternational.org/news-analysis/2549/have-companies-deleted-your-data
        - in our piece describing difficulties with access to information and data on Facebook: https://privacyinternational.org/long-read/3372/no-facebook-not-telling-you-everything
        - in other research by civil society, for example in the political sphere: https://www.openrightsgroup.org/press/releases/2019/campaigners-demand-answers-over-parties-use-of-personal-data-in-general-

election

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

In addition to the above we consider that the Code should indicate that the default position be that the Data Protection Impact Assessments (DPIAs) be made public, unless there is a strong justification for not doing so and as a minimum recommend it be done as best practice.

In this regard, we note the Article 29 Working Party Guidelines on DPIAs, endorsed by the EDPB, state in relation to DPIAs that "…controllers should consider publishing at least parts, such as a summary or conclusion of their DPIA. The purpose of such a process would be to foster trust in the controller's processing operations and demonstrate accountability and transparency. It is particularly good practice to publish a DPIA where members of the public are affected by the processing operation." The lack of transparency and accountability has undermined trust in political campaigning and given, as the draft Code points out, many campaigning activities require a DPIA, the Code is an opportunity to advocate for publication of them.

Linked to this, but more specifically 'lawful basis' and any reliance on 'legitimate interest' under Article 6(1)(f) of GDPR, we consider that Legitimate Interest Assessments ("LIA") should not only be encouraged but also be published. The current section on lawful basis in the draft Code does not do this. This is necessary as our experience to date is that even where organisations, for example data brokers, claim to have carried out an "LIA" they refuse to publish or provide them, including in response to subject access requests.

Finally, our submission to the ICO on the draft Code of Practice for use of data in political campaigning makes points relevant to this Code:
https://privacyinternational.org/advocacy/3267/submission-ico-code-practice-use-personal-data-political-campaigning

About you

Q8 Are you answering as:

- ☐ An individual acting in a private capacity (e.g. 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:

Privacy International

If other please specify:

Q9 How did you find out about this survey?

- ☐ ICO Twitter account
- ☐ ICO Facebook account
- ☐ ICO Linkedln account
- ☒ ICO website
- ☐ ICO newsletter
- ☐ ICO staff member
- ☐ Colleague
- ☐ Personal/work Twitter account
- ☐ Personal/work Facebook account
- ☐ Personal/work Linkedln account
- ☐ Other

If other please specify:

Thank you for taking the time to complete the survey