Call for Views: Code of Practice for the use of personal information in political campaigns

The ICO's new Code of Practice for the use of personal information in political campaigns will draw from our current Guidance on Political Campaigning, but will be fully updated to ensure it reflects the current Data Protection Act 2018 and GDPR requirements. It will also be widened to cover areas where our investigation found significant concerns or misunderstandings of the law. In addition, it will provide guidance and good practice recommendations to aid compliance.

You can read the full background and legal basis for the production of this code on our website.

Responses to this call for views must be received by **11.59pm on Friday 21 December 2018**

If you would like further information on the call for views please telephone 0303 123 1113 and ask to speak to the Parliament and Government Affairs Department about the call for views on a new Code of Practice for the use of personal information in political campaigns or email politicalcampaigning@ico.org.uk.

Privacy statement
For this call for views we will publish responses received from organisations but will remove any personal data before publication. We will not publish responses from individuals. For more information about what we do with personal data please see our privacy notice.

Call for Views: Code of Practice for the use of personal information in political campaigns

Q1 Do you agree with our understanding of 'political campaigning' and what processing should be covered by the code?

□ Yes
■ No

Please explain further:

Privacy International considers that the ICO's understanding of the term 'political campaigning' and the processing that should be covered by this code requires further consideration in order to ensure it is sufficiently clear and broad. The ways that data is used in elections are constantly evolving and thus the Code must also offer a certain level of flexibility to respond effectively.

From the introduction of the consultation we understand that the ICO anticipates that the code will apply to: "*all data controllers who process personal data for the purpose of political campaigning." And that by 'political campaigning' the ICO means activity, "which relates to elections or referenda, in support of, or against, a political party, a referendum campaign or a candidate standing for election. This includes but is not limited to processing by registered political parties, electoral candidates, referendum permitted participants and third party campaigners, as defined in Political Parties and Referendums Act 2000.*"

Both when the Code applies and to who must be clear. We would welcome the opportunity to comment further on a draft Code.

We consider the following requires further consideration as to the scope of the Code:

Data Controllers

The limitation of the Code to data controllers makes sense given the ICO's role and the requirements of the GDPR and the Data Protection Act 2018. However, consideration must be given to how to avoid this term being interpreted too narrowly in the implementation of the Code. Whilst the term 'data controller' has repeatedly been given a broad interpretation by the European Court of Justice and it is clear such a role cannot merely be assigned via a contract, there is the risk that some actors may try to shift responsibility by seeking to assume data processor roles. Therefore, the Code must be clear that the concept of data controller is broad and can be shared by joint controllers. Furthermore, consideration should be given to whether data processors have any specific responsibilities in this context, including how this relates to their existing obligations under GDPR such as Article 28. For example, in its report Democracy Disrupted, the ICO flagged platform Nationbuilder, commonly used by political parties, as being a data processor – this and any similar platforms should not be outside the scope of the Code.

Personal data

As with the above limitation, we appreciate why the Code will be limited to the processing of personal data given the scope of the GDPR and the Data Protection Act 2018. However, again care should be taken in the Code to emphasise that this definition is to be interpreted broadly and includes personal data from which individuals are not directly identifiable. Furthermore, it should explicitly cover personal data that is derived, inferred and predicted (profiling) (https://privacyinternational.org/blog/742/hiding-plain-sight-political-profiling-voters).

Data can be used to develop profiles of both individuals and groups. The data that feeds into such profiles is bought, amassed and shared from and between multiple actors (https://privacyinternational.org/feature/1721/snapshot-corporate-profiling and https://privacyinternational.org/advocacy-briefing/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad) without individuals having ever known that they were profiled (https://consoc.org.uk/wp-content/uploads/2018/07/Stephanie-Hankey-Julianne-Kerr-Morrison-Ravi-Naik-Data-and-Democracy-in-the-Digital-Age.pdf). Profiles can be cross-correlated and used to infer data not just about an individual but others ‘like them’, for example through ‘lookalike audiences’(see, e.g., ICO Democracy Disrupted Report at page 36). Furthermore, data brokers and AdTech companies often offer probabilistic solutions i.e. they will establish “a match between sets of data leveraging inferred, modelled or proxy assumptions”. (Winterberry Group Report: “Know Your Audience: The Evolution of Identity in a Consumer-Centric Marketplace”, August 2018 https://www.winterberrygroup.com/our-insights/know-your-audience-evolution-identity-consumer-centric-marketplace).There is a risk that some of the processing of data used in political campaigning will seek to circumvent the definition of personal data, through for example, claiming profiles or segments are created from aggregated data or that they apply to groups/ households as opposed to individuals - no matter how granular they then are or that the profiles are in the end associated with individuals or where the use of a platform’s tool has enables political actors to reach individuals without actually having their data. The Code should seek to mitigate this.

Political Campaigning

This definition should be broad to reflect the wide and varied nature of political campaigning. This is achieved to an extent through the ICO’s proposed definition with the use of the term ‘relates to’. However, the Code should be clear as to whether it is limited to campaigns related to elections or referenda rather than political campaigning in a broader sense. If the definition and thus the Code is meant to be exclusive to elections and referenda, consideration should be given to whether this poses any timing restrictions as to when the Code applies, and if so what this is and whether there are risks in excluding political campaigning falling outside this scope. It is important to note that political campaigning with the potential for exploitation of people’s data is not limited to the run up to elections or referenda.

In Privacy International’s view, the Code must apply to political campaigning beyond the strict electoral cycle. The misuse of personal data for political manipulation and misinformation happens at all times, and not just around elections. Focusing only on the election phase and on the political parties or official candidates will miss a significant and growing phenomenon, which directly influences democracy and public discourse. (See recent article on UK https://www.politico.eu/article/britain-nationalist-dark-web-populism-tommy-robinson). The Code needs to contemplate that data can be used for political campaigning and elections outside the electoral context (e.g. UAE and Saudi Arabia’s use of ads/social media campaigns to influence US policy on Quatar (https://www.pri.org/stories/2018-07-24/how-diplomatic-crisis-among-gulf-nations-led-fake-news-campaign-united-states) or the use of spyware on supporters of a sugar tax in Mexico (https://www.nytimes.com/2017/02/11/technology/hack-mexico-soda-tax-advocates.html)).

Furthermore, clarification is required as to how “support for or against” in the proposed definition be measured, bearing in mind that there might not be obvious links between the way that data is used politically, for example in an effort to influence or create division, and a political party manifesto commitment or support or opposition in a referendum. As an example, a recent report prepared for the US Senate on Russian disinformation provides details on how Americans were categorised into key interest groups for targeted messaging, including through IRA controlled Facebook pages such as "Being Patriotic", "Heart of Texas", "Blacktivist" and "Army of Jesus". Furthermore "The Russians operated 133 accounts on Instagram, a photo-sharing subsidiary of Facebook, that focused mainly on race, ethnicity or other forms of personal identity. The most successful Instagram posts targeted African American cultural issues and black pride and were not explicitly political." (https://www.washingtonpost.com/technology/2018/12/16/new-report-russian-disinformation-prepared-senate-shows-operations-scale-sweep/?utm_term=.12b0a47d7c1f)

We welcome the clarification that the actors "include but are not limited to" as we consider that the Code should apply more broadly as set out in response to the next question.

Finally, whilst we welcome this important step by the ICO in developing the Code and we note that it is just one of the steps the ICO plans to take, it must be part of a wider multi-regulatory approach to this issue. This has already been acknowledged by the European Data Protection Supervisor (https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf) and the ICO. This is extremely important given the breadth of the challenges and issues faced and also because of the detail of how the law and the proposed Code apply and interlink with other legislative frameworks. For instance, as can be seen with this first question, the proposed Code is reliant on definitions in electoral legislation from 2000.

Call for Views: Code of Practice for the use of personal information in political campaigns

Q2 Should the code apply to other data controllers in the political campaigning process, beyond registered political parties, electoral candidates, referendum permitted participants and third party campaigners? Eg data controllers processing personal data on behalf of political campaigns, parties or candidates.

■ Yes
□ No

Please explain further:

As demonstrated in the ICO's recent investigations into data and elections and report 'Democracy Disrupted', the way that political parties and others have used data gives rise to grave concerns. This is in spite of the ICO's existing guidance on political campaigning, which has either been disregarded or has not stretched to the forms of processing we are now seeing. Therefore, the introduction of the Code is welcome, as a regulatory 'bigger stick' as opposed to voluntary compliance.

For the Code to be relevant and effective it must apply to other data controllers in the political campaigning process and should definitely include data controllers processing personal data on behalf of or jointly with political campaigns, parties or candidates. However, it should go even further to acknowledge that there are other actors that play a role (whether intentional or unintentional) in political campaigning (including through influencing and nudging) but do not have a direct relationship with/ are not affiliated with a particular party, candidate or third party (under the Political Parties and Referendums Act 2000).

The concerns flagged by the ICO around various actors, including data brokers, and the online advertising ecosystem in the recent data and election reports are reflected in investigations and actions by civil society. For example, in November 2018, Privacy International called on the ICO, together with the Irish and French data protection authorities, to investigate seven data broker and advertising technology companies, that are illustrative of more systemic problems (https://privacyinternational.org/advocacy-briefing/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad). Earlier, in September 2018, complaints were also submitted to the ICO and the Irish Data Protection Commissioner concerning online behavioural advertising (https://brave.com/adtech-data-breach-complaint). Whilst these complaints do not focus on political campaigning, they focus on actors that rely, thrive and profit from personal data. The techniques and data intensive ecosystem used in commercial advertising are also deployed in the political context with various actors advertising specific offerings for this context (e.g. Oracle http://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf and Experian https://www.experian.co.uk/assets/marketing-services/brochures/experian-marketing-services-brochure.pdf; see Audience IQ which provides political segments https://www.experian.com/assets/marketing- services/product-sheets/das-political-data-sheet.pdf; as explained here: https://ourdataourselves.tacticaltech.org/posts/psychometric-profiling/). Civil society advocacy, documented abuse of data in elections around the world , and the ICO's own work highlight that action is required not just to safeguard personal data but safeguard the democratic process.

Advertising and political campaigning have become intertwined and inextricable, as the founder of one political campaigning company put it: “There are tons and tons of consumer data on the ad exchanges that we built […] you have registrations that are publicly available information. You can take those voter rolls and match those to our online profiles and serve those people ads individually online." (https://ourdataourselves.tacticaltech.org/posts/the-new-disruptors/)

The code should aim to provide clarity on the legal obligations of the various actors, including those mentioned above and below, as well as the application to data processors. For example, it should clarify that the exemptions for processing for political purposes permitted in paragraph 22 of Schedule 1 of the Data Protection Act 2018 should apply strictly and cannot be invoked by entities which are not registered political parties.

Q3 Who should the code also be aimed at ie data brokers, analytical companies, online platforms? (List as many as you think are applicable)

- Data Brokers

- Credit Reference Agencies

- Analytical companies

- Campaigning platforms (e.g. Nationbuilder)

- Online platforms providing advertising (e.g. Facebook, Google etc) and other companies that facilitate the behavioural and micro-targeted advertising ecosystem (AdTech companies).

- Social Media and Messaging applications (e.g. WhatsApp, see report on data and elections in Brazil https://www.codingrights.org/wp-content/uploads/2018/11/Report_DataElections_PT_EN.pdf)

We recommend consideration of the research by Tactical Tech, in particular the lists of 100s of companies operating in this sphere. The Code should be clear as to how it applies to these broader range of actors and identify their responsibilities to ensure that those actors involved in political campaigning do not abuse personal data.

Tactical Tech have divided the organisations’ roles into: Data as influence: Campaigning; Data as influence: Communications; Data as an asset; and Data as intelligence. Many of the companies fall into multiple categories (https://ourdataourselves.tacticaltech.org/posts/whos-working-for-vote/ and https://ourdataourselves.tacticaltech.org/media/data-companies-and-digital-consultants-long-list_updated-28th-Nov-2018.pdf)

Call for Views: Code of Practice for the use of personal information in political campaigns

We propose the code will include the following broad topic areas:
- The role of data controllers in the political campaigning ecosystem;
- Transparency requirements in practice;
- Accountability, security and data minimisation requirements;
- Lawful bases including the new 'democratic engagement' aspect of the 'public interest'
basis in the Data Protection Act 2018;
- Using special category data;
- The use of personal data from the Electoral Register;
- Data collection directly from individuals;
- Using personal data collected by third parties;
- Personal data analytics;
- Direct marketing including the application of the Privacy and Electronic Communications
Regulations;
- Online advertising and the use of social media;
- Post political campaign/election considerations.

Q4 Do you agree with the proposed topics?

■ Yes
□ No

Please explain further:

We agree with the proposed list of topics. We welcome the inclusion of transparency and consider that, within the broad topic, it should be broken down to cover transparency in practice, including in the context of the different actors – such as political parties, candidates, the platforms and tools used to convey political messages.

We consider the Code should also be expanded to include at least the topic areas listed in response to the next question.

Call for Views: Code of Practice for the use of personal information in political campaigns

Q4c Is there anything we have not listed that ought to be included?

■ Yes

□ No

Please specify:

The following broad topics should also be dealt with (once a draft Code is published other gaps may be identified):

- Fairness

- Purpose Limitation

- Profiling in the political context

- Individual rights – guidance on respecting individuals' rights including to access, object, rectification, erasure etc., as well as the application of Article 22 of GDPR relating to automated decision-making in this context.

- Under 'using special category personal data' and 'lawful bases', the Code should specifically seek to tackle the condition for political parties contained in paragraph 22 of Schedule 1 to the Data Protection Act 2018. Privacy International is extremely concerned by this condition and raised this during the passage of the Bill. Despite these concerns being echoed by peers and MPs, the condition remains and thus the Code is a key opportunity to mitigate the abuse of this condition by political parties and those that work with them. (see https://privacyinternational.org/sites/default/files/2018-05/17%2012%2004%20Briefing%20DPB%20%5BHL%5D%20Report%20Stage_0.pdf paragraphs 5.15 – 5.35) Furthermore, clarity should be provided around the definition of special category personal data – Article 9 of GDPR defines it as the "Processing of personal data **revealing**…" the special categories. This should be interpreted as such with all categories, including political opinions, e.g. the data may not directly indicate a political opinion such as conservative, but may reveal it through other data and these are the categories or segments that can be used to target individuals.

- Under 'The use of personal data from the Electoral Register', the ICO should seek to address the use of this data in the Open and Full Register by third parties, including credit reference agencies who use this data (for example Equifax, Experian, Acxiom). The Code also provides an opportunity for reflection as to why inclusion in the Open Register, whereby people's personal data is for sale to anyone who wants to buy a copy, continues to be on the basis of Opt Out as opposed to Opt In (https://www.gov.uk/electoral-register/opt-out-of-the-open-register).

- The use of tools and techniques which facilitate data being used for micro-targeting in the political campaigning context, including cross-device targeting; programmatic advertising; lookalike modelling; geolocation targeting; online video advertising; targeted TV advertising; psychographic, neuromarketing and emotion based targeting (https://policyreview.info/articles/analysis/role-digital-marketing-political-campaigns). The Code should be flexible enough to respond to new techniques and experimentation with personal data for political influence.

- Sanctions and remedies, including how these apply prior to and post elections and referenda given the often unique and far reaching consequences in the electoral context. In terms of remedies, the development of the Code is a key opportunity to consider the benefits of implementing Article 80(2) of GDPR concerning collective redress, in preparation for the review in 2019 under section 189 of the Data Protection Act 2018.

- Extraterritorial application – to make it clear that actors that are not based in the EU may still fall within the scope of the Code.

- The role of joint controllers and data processors, as discussed in more detail in response to Q1.

Q4b What topic areas in particular ought to be covered in the most detail?

- **The use of platforms and tools that facilitate targeted political campaigning**. Political parties do not only target voters using data they either collected themselves or that they have obtained/ bought from a third party, they use tools that platforms provide to expand their reach and target other individuals, for instance through lookalike audiences. This was used by the far-right AfD in Germany (https://www.bloomberg.com/news/articles/2017-09-29/the-german-far-right-finds-friends-through-facebook) and is explained further here (https://policyreview.info/articles/analysis/role-digital-marketing-political-campaigns). This type of processing must not escape the application of the Code on the basis that the platform or tool provider is a data processor and that the political party or other actor that uses the tool did not process the personal data of the individuals reached via the platform or tool. Both the platform/ tool provider and the party using the platform/tool are together determining the purpose and means for which such data can be used, and the Code should be clear on the responsibility of each.

- **Online advertising**. Our concerns in this area are raised in response to Q2. Privacy International considers it imperative that the ICO investigate the AdTech industry more broadly. Most political actors use exactly the kinds of tools, platforms and even data that are used for marketing. As long as we're seeing blatantly non-compliant behaviour there, and as long as targeted advertising practices themselves don't meet the GDPR threshold (https://privacyinternational.org/campaigns/tell-companies-stop-exploiting-your-data), we will see political actors exploiting them, especially when there is lack of clarity around the definition of political actors.

- **Legal Bases** – including consent and legitimate interest, and for special category data (in particular the condition in paragraph 22 of Schedule 1 to the Data Protection Act 2018.)

Q5 What do you think should be covered in the new code of practice that isn't covered in current political campaigning guidance?

All the points listed by the ICO under Question 4 together with the points that Privacy International has listed above. The majority of these are not covered in the current guidance.

Q6 What factors ought to be taken into account regarding the particular circumstances of different types of election or referenda?

Privacy International suggests that a robust data protection framework should apply to all forms of political campaigning. We see little room for variation of the framework, at least to the extent any protections might be lessened, depending on the circumstances of the particular election or referenda.

Elections of all sorts can have significant impact – and therefore should be subject to similar high standards. For instance, as the ICO is well aware, recent referenda campaigns such as those surrounding Brexit (see the ICO's report "Investigation into the use of data analytics in political campaigns", 6 November 2018) and the Irish referendum on abortion (see, e.g., https://www.irishtimes.com/opinion/fintan-o-toole-abortion-fake-news-firestorm-heading-our-way-1.3440927) suffered from extensive potential abuse of personal information by the various parties involved. National elections in countries as diverse as the United States, France, Mexico, Brazil, and Kenya have also seen the manipulation of personal information. The EU is anticipating and attempting to prepare for potential manipulation in its upcoming elections (see https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf). Local elections, due to their smaller size, may be more easily influenced by the targeting made possible through the abuse of data. Those same local elections have formed core parts of the political strategy of certain political parties (see, e.g., https://www.washingtonpost.com/news/monkey-cage/wp/2017/05/11/what-can-or-should-activists-learn-from-the-tea-party/?noredirect=on&utm_term=.86917a6ad163). For all of these reasons, we do not see any room to vary a baseline, robust data protection framework for campaigning activities.

Call for Views: Code of Practice for the use of personal information in political campaigns

Q7 Please state any case studies or scenarios you would like to see included in the code?

The following would be useful case studies to explore in the Code:

(1) How the Code will apply to third parties such as data analytics companies, data brokers and social media companies. For instance, would it ever be possible for such third parties to obtain appropriate consent for direct marketing on behalf of a political campaign? What level of transparency must the third parties and the campaigns meet in order to fulfil their duties to operate in a fair, transparent and lawful manner?

(2) With campaigning increasingly becoming an activity that occurs throughout the election cycle, not only during purdah or immediately preceding an election, how should campaign activities that occur months or even years before an election be controlled? For instance, what are the rules surrounding communications from political parties that extend beyond being "in support of, or against, a political party, a referendum campaign or a candidate standing for election"? What if the communication is more generalised, such as regarding an issue that is part of the party's platform, but does not fit this narrow definition? Should the code apply in such a scenario, and if so, how? Privacy International believes the code should extend to the use of personal information to facilitate such communications.

(3) Relatively few resources are required to be able to significantly influence elections (and more broadly the electorate/political discourse). The Code should reflect on the role of social media platforms and other digital communications actors (e.g. Google) to address this.

(4) How will the political parties exemptions (clause 8(e) and Schedule 1, para 22) in the Data Protection Act 2018 interact with this Code?

Q8 Please state any examples of guidance, tools or good practice you have encountered that could aid compliance in this area, and could be included in the code.

An example of guidance elsewhere is the EU:

EU action plan, including Code of Practice on Online Disinformation and roadmap for implementation: http://europa.eu/rapid/press-release_IP-18-6647_en.htm

See also European Parliament decision on the use of Facebook users' data by Cambridge Analytica and the impact on data protection: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0433+0+DOC+PDF+V0//EN

In developing a Code of Practice, much can be learned from reports on past elections, these include:

Tactical Tech – Data and Politics Project with examples from a range of countries around the world https://ourdataourselves.tacticaltech.org/projects/data-and-politics/

Constitution Society Report https://consoc.org.uk/wp-content/uploads/2018/07/Stephanie-Hankey-Julianne-Kerr-Morrison-Ravi-Naik-Data-and-Democracy-in-the-Digital-Age.pdf

Call for Views: Code of Practice for the use of personal information in political campaigns

Q9 Name and contact details:

Caroline Wilson Palow, General Counsel and Ailidh Callander, Legal Officer

Privacy International

62 Britton Street

London, EC1M 5UY

Q10 Are you responding:

□ In your own capacity?

■ On behalf of an organisation

Please describe your role and your organisation:

Privacy International is a registered charity based in London that works at the intersection of modern technologies and rights. It envisions a world in which the right to privacy is protected, respected, and fulfilled.

Privacy is essential to the protection of autonomy and human dignity, serving as the foundation upon which other human rights are built. In order for individuals to fully participate in the modern world, developments in law and technologies must strengthen and not undermine the ability to freely enjoy this right.