

ICO consultation on the draft framework code of practice for the use of personal data in political campaigning

It is vital in any democratic society that political parties, candidates and campaigners are able to communicate effectively with voters. But it is equally vital that all organisations involved in political campaigning use personal data in a way that is transparent, understood by people and lawful.

Our current guidance on political campaigning is outdated. It has not been updated since the introduction of the GDPR and does not reflect modern campaigning practices. We have therefore drafted and are now consulting on a new framework code of practice for the use of personal data in political campaigning. This will serve both as helpful guidance in its own right as well as having the potential to become a statutory code of practice if the relevant legislation is introduced.

The framework code of practice does not introduce new requirements for campaigners but seeks to explain and clarify data protection and electronic marketing laws as they already stand. It also seeks to provide practical guidance and useful examples on ways campaigners could comply with their obligations whilst carrying out common political campaigning activities.

Before drafting the framework code of practice, the ICO launched a call for views in October 2018. You can view a summary of the responses and some of the individual responses on our website. The responses have helped inform the content of the draft framework code.

We welcome views on the draft framework code of practice. Please send us your responses by **Friday 4 October 2019**.

Privacy Statement

For this consultation, we will publish all responses except for those where the respondent indicates that they are an individual acting in a private capacity (e.g. a member of the public). All responses from organisations and individuals responding in a professional capacity will be published. We will remove email addresses and telephone numbers from these responses; but apart from this, we will publish them in full.

For more information about what we do with personal data please see our [privacy notice](#).

Questions

Q1 Does the draft framework code adequately explain and advise on the aspects of data protection and electronic marketing laws which are relevant to political campaigning?

☐ Yes

☒ No

Q2 If not, please specify where improvements could be made.

Bundling consent – GDPR and PECR

Open Rights Group (ORG) is concerned that the ICO's Draft Framework Code of Practice for the Use of Personal Data in Political Campaigning ('the guidance') does not sufficiently address the issue of bundled consent. The General Data Protection Regulation (GDPR) is explicit that consent should not be bundled up as a condition of providing a service, unless it is absolutely necessary for that service.

It is difficult to see how targeted political advertising is a necessary condition of most online services. Whilst sites such as Facebook may rely on advertising for revenue, the relationship between this and targeted political advertising is unclear. If this is the case, then the guidance should spell this out. Online services ought to request a specific opt in from citizens if they wish to receive targeted political adverts as part of their use of a service. The assumption that they would want to do so is likely to be unlawful.

Furthermore, it would be useful for the guidance to better explore the relationship of custom audiences to the Privacy and Electronic Communications Regulations (PECR) and GDPR. The Information Commissioner's Office clearly had concerns about the development of micro-targeting.

Micro-targeting clearly engages PECR and GDPR as direct marketing. Under the guidance the only lawful basis is consent. However, the question is whether the consent model currently in operation is sufficient for processing special category data. There is no distinction between the commercial custom audience and the political custom audience. Combine this with the guidance at page 42 where the guidance states that in most circumstances that special category data can only be processed with the explicit consent of the individual.

We would like to see the ICO explain in no uncertain terms whether they consider the use of certain targeting techniques in political campaigns, to require explicit consent separate to that of commercial direct marketing. Those practices are:

- Custom audiences.
- Lookalike audiences.
- Other micro-targeting techniques, cross-device tracking.

Currently while there is some discussion pp. 90 – 93 it is not stated whether current consent mechanisms are enough for this practice.

Further practical information on Data Protection Act 2018 Schedule 1 paragraph 22

One of the more controversial areas of the Data Protection Act 2018 was the inclusion of a special condition for political parties to process political opinions without relying on explicit consent if it is necessary for the purposes of the party's political activities.¹ This condition is discussed on page 45 and the terms of the condition are explained, including for example the inclusion of an 'appropriate policy document'. There is, however, no practical example of this condition in practice. Important questions remain unanswered, such as:

- What is an appropriate policy document as it relates to this processing?
- What are activities "necessary" for the purposes of the party's political activities?

Further detail on these areas would improve the relevance of this guidance to issues that are unique to the political campaigning context.

Q3 Does the draft framework code contain the right level of detail?

- ☐ Yes
☒ No

¹ The Data Protection Act 2018, *Schedule 1, Paragraph 22*.

<<http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted>>

Q4 If no, in what areas should there be more detail within the draft framework code?

Although the guidance generally offers a good level of detail, there are specific instances where it does not. As the guidance is titled a code of *practice*, it should aim to give clear, detailed, worked out examples of recommended practice and implementation where possible.

ORG does recognise however the tension inherent in the investigative role of the regulator, and the expectation that those covered under the regulation should take a proactive approach to meeting the guidance.

Profiling:

The guidance states that if Article 22 of the GDPR (automated processing and legal or similarly significant effect) applies, then organisations must “provide meaningful information about the logic involved and what the likely consequences are for individuals”.² It does not, however, give an example of what this should look like. ORG considers it within the scope of the guidance for the ICO to provide examples of what constitutes meaningful information and likely consequences, how it should be formatted, and how this information should be served to individuals. For example, profiling often takes the form of percentage scores or demographic descriptors, of which the ultimate meaning and data sources are opaque.

Additionally, this information ought to be *proactively* provided to individuals. Currently the only method that could provide this information would be a Data Subject Access Request, or the largely untested Data Portability Request.

For example, ORG believes that profiling is, de facto, often automated processing. As part of providing meaningful information to citizens, political campaigners should make this clear, and spell out their rights in relations to this.

² ICO, *Framework code of practice for the use of personal data in political campaigning*, 2019, page 71.
< <https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf>>

The prominent display of privacy information

The guidance notes that Article 13 of GDPR lays out a 'right to be informed' – that citizens must be alerted to when their personal data is being collected. Notably, it suggests that this information should be "prominently display" (ed) during various methods of personal data collection such as online surveys.³

Whilst it gives some collection method specific advice on what constitutes prominent display, the guidance should illustrate this more broadly. It should outline principles for what prominent display looks like in practice and give a detailed examples of best and worst practice.

Data controllership of electoral register data

The guidance suggests that political campaigners who receive electoral register data become data controllers for that data. Subsequently, it reminds them of their obligations under data protection law.⁴

The guidance does not, however, state who is the data controller for electoral register data before it is transferred to political campaigners. The European Commission's guidance on this suggests "national electoral authorities", such as the Electoral Commission, are generally data controllers for electoral registers.⁵ in UK electoral law, this is a decentralised responsibility and local Returning Officers are the data controllers.⁶

³ Ibid, page 53.

⁴ Ibid, pp 49-50.

⁵ European Commission, *Commission guidance on the application of Union data protection law in the electoral context*, 2018, page 4.

< https://webcache.googleusercontent.com/search?q=cache:eo-KAIZKvUYJ:https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf+&cd=1&hl=en&ct=clnk&gl=uk&client=firefox-b-d >

⁶ The legal basis for processing personal information relating to electoral administration is contained in the following legislation: Representation of the People Act 1983, Representation of the People Act 1985, Representation of the People Act 2000, European Parliamentary Elections (franchise of Relevant Citizens of the Union), Regulations 2001, Representation of the People (England and Wales) Regulations 2001 and Electoral Administration Act 2006.

< <https://hackney.gov.uk/privacy-notice-ro> >

There are two points of concern here. Although individuals are able to register to vote anonymously, if political campaigners become data controllers for the electoral register, there is no oversight mechanism to prevent campaigners from effectively de-anonymising anonymous entries on the register through inferential information.

The second point is that, whilst the guidance establishes the joint controllership relationship between political campaigners and other actors, it does not spell out whether Returning Officers share a joint controllership role with political campaigners. As it is arguable that Returning Officers play a role in determining the purpose and means of processing in this case, this relationship, and where controllership lies, should be fleshed out in detail.

Furthermore, ORG does not consider the democratic engagement opt out sufficient in light of the controllership role of local returning officers. As noted by the European Commission many other European countries, for example Germany, have centralised electoral registers with higher and more stringent conditions of access. It seems unlikely that access to electoral register data is 'necessary' for democratic engagement – although it may be 'necessary' for electioneering.

Q5 Does the draft framework code provide enough clarity on the law and good practice on the use of personal data for political campaigning?

☐ Yes

☒ No

Q6 If no, please indicate the section(s) of the draft framework code which could be improved, and what can be done to make the section(s) clearer.

ORG considers there to be several legal tests that are not clearly or tightly enough defined within the guidance.

Lawful, Fair and Transparent Profiling

'Necessary' test for democratic engagement:

The DPA Section 8 Specifies that a lawful basis for processing personal data is processing that is "necessary for ... (e) an activity that supports or promotes democratic engagement".⁷ The guidance clarifies that processing in this instance does not have to be "just useful or standard practice. It must be a targeted and proportionate way of achieving your specific purpose".⁸ Additionally, you cannot apply this if you can achieve this purpose by processing less personal data.

The operative tests for 'necessary' therefore are whether the processing of personal data is 'targeted' and 'proportionate', when weighed against the aim of achieving a 'specific purpose'. The application of these terms, however, are not clear. For example, for a political party, any activity may be considered proportionate when weighed against the specific purpose of electoral success in a ward or borough. The guidance should unpack these terms, and evidence their use and relationship to each other. Otherwise, political campaigners could legitimately operate within this loophole.

'Fairness' in political profiling

Fairness in processing is a cornerstone of data protection law. We welcome the guidance's call for an ethical pause before determining whether the utilisation of an innovative method of campaigning that uses personal data is fair or not⁹. This is particularly significant in relation to political profiling, as political profiling is often utilised as a

⁷ The Data Protection Act 2018, *Section 8, Lawfulness of processing*.
<<http://www.legislation.gov.uk/ukpga/2018/12/section/8/enacted>>

⁸ ICO, *Framework code of practice for the use of personal data in political campaigning*, 2019, page 38.
< <https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf>>

⁹ Ibid, page 35.

preamble to attempt to manipulate the political opinions of 'persuadables' in an emotive and underhand manner.¹⁰

ORG welcomes the guidance's emphasis on fairness in political profiling. It recognises that what should be examined in this element of political campaigning is the intent rather than the effect. There is little academic consensus on the effectiveness of political profiling to persuade and convince, and many prominent practitioners of this technique have been accused of either not understanding the basics of statistical data science or selling snake oil.¹¹ It is therefore correct that data protection law, rather than the marketing claims of data science companies, is centred in this conversation.

If fairness is so crucial to lawful political profiling, however, its requirements should be more clearly defined within the guidance. Recital 39 of the GDPR does address Article 5 (1) a., which defines lawfulness, fairness and transparency as the first principle of data protection in processing personal data.¹² It focuses primarily on transparency, however, and fairness is left reasonably undefined. Nevertheless, ORG considers this guidance the appropriate place to flesh out what fairness in processing *requires* in the context of political profiling.

Additionally, ORG suggests that any further clarification of the requirements for 'fairness' in processing in this context ought to be narrower, and to a higher standard, than the requirements of 'fairness' in processing in a commercial context. The stakes are higher in an election and engage with a greater number of individual rights. Furthermore, whilst you can return a product that is unlawfully sold to you, you cannot return an election result. The Information

¹⁰ Tactical Tech, *Psychometric Profiling: Persuasion by Personality in Elections*, 2018.
< <https://ourdataourselves.tacticaltech.org/posts/psychometric-profiling/> >

¹¹ BBC Radio 4, *SLICE: Politics and Personality; L is for Likes*, 2018.
< <https://www.bbc.co.uk/sounds/play/b0b5t81m> >

¹² REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 5 (1) a., 2016.
< <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e2884-1-1> >

Commissioner has herself alluded to this distinction in her testimony to the Department of Digital, Culture, Media and Sport's Select Committee, stating that:

"I don't think we want to use the same model that sells us shoes and cars to engage with people and voters. I think that people expect more than that."¹³

A closely defined, high standard interpretation of the requirements of the fairness principle in the context of political campaigning would bring the ICO a step closer to realising this statement.

Q7 Does the draft framework code cover the right political campaigning activities?

- ☐ Yes
☒ No

Q8 If no, what other activities would you like to be covered in it?

Undue focus on electoral campaigning amongst political parties

The guidance feels like it has been written in response to the political upheaval of recent years; at least one of its examples clearly paraphrases activity widely alleged to have been carried out by Vote Leave campaign in the 2016 EU membership referendum.¹⁴ In that sense it is appropriate to focus on election campaigning. ORG is concerned, however, that this focus risks myopia. For example, the guidance does not give examples of party leadership campaigns or issue

¹³ The Telegraph, *Facebook should disclose how political parties target people online, ICO says*, 2018. <<https://www.telegraph.co.uk/technology/2018/11/06/facebook-should-disclose-political-parties-target-people-online/>>

¹⁴ ICO, *Framework code of practice for the use of personal data in political campaigning*, 2019, page 66. <<https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf>>

advocacy campaigns. In particular it does not offer any examples of relationships with third party campaign groups (although it does acknowledge that the guidance applies to political campaigners outside of political parties).

These groups (such Mainstream Network, an 'astroturf' organisation) and their activities go to the heart of contemporary anxieties about political campaigning. They are particularly pertinent in the context of the guidance, as they may transfer data between themselves, or between themselves and political parties. This sort of activity was suggested in the coordination between Vote Leave and other campaign groups in the 2016 EU membership referendum. Similarly, this can happen when political parties split, or when a member of a campaign group decides to campaign for a political party.¹⁵

Additionally, smaller grassroots campaigning organisations may not have the resources to seek the "specific legal advice" that is repeatedly alluded to in the document.¹⁶ The next iteration of the guidance should include specific legal clarifications for, and examples of, third party campaigning activity. The requirements of smaller campaigns both within and external to political parties should be centred.

Q9 Does the draft framework code appropriately recognise and understand the ways in which political campaigning takes place in practice in the online world?

- ☐ Yes
☒ No

Q10 If no, in what way does the draft framework code fail to recognise and understand this?

¹⁵ The Evening Standard, *Momentum turns on its own chief*, 2019.

<<https://www.standard.co.uk/news/londoners-diary/the-londoner-momentum-turns-on-its-own-chief-a4235886.html>>

¹⁶ ICO, *Framework code of practice for the use of personal data in political campaigning*, 2019, pages 13 and 27.

< <https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf>>

The relationship between the ICO and Electoral Commission

It is clear that it is in online political campaigning that data protection law and campaign finance law meet. The guidance alludes to this, stating that they would expect controllers for electoral register data “to take part in centralised transparency initiatives organised by the ICO or the Electoral Commission”.¹⁷

ORG considers it unclear why this sentence should not read “the ICO *and* the Electoral Commission”. Better interfacing between the two regulators could help both of them more fully carry out their statutory duties. For example, the ICO could draw upon the Electoral Commission’s expertise in campaign finance regulation, whilst offering technical capacity, in order to get a better picture of the lawfulness and financial value of data sets and other data assets. ORG considers enhancing transparency and accountability around the financial value of data assets key to ensuring that the regulation of data driven campaigning is fit for purpose in the 21st Century.

When an organisation registers with the Electoral Commission, the regulator has no idea of its assets or their value, including data sets. The reporting of both spending and donations during elections happen after the fact. Whilst both the Electoral Commission and the ICO can do proactive audits of political campaigners, within the remit of their respective powers, historically this has not often been used. In light of recent political events however, both regulators, but particularly the ICO have stepped up their auditing of political parties. ORG welcomes this and encourages the ICO to make the results public.

There are a number of improvements that could allow the Electoral Commission and the ICO to interact more effectively. For example, the power of regulators to share information in the public interest could be strengthened under law, although this would likely require primary legislation. There are also structural organisational issues that can create friction. Addressing these issues would encourage a regulatory ecosystem that more fully reflects the reality of political campaigning online.

¹⁷ Ibid, page 50.

A comparative document for platforms

ORG considers that it would be useful for the ICO to issue a sister document to the guidance that outlines the data protection requirements for political campaigning as they relate to online platforms and businesses. This is particularly in light of the joint controllership role outlined in the guidance.¹⁸

Q11 Does the draft framework code provide examples relevant to your organisation?

☐ Yes

☐ No

Q12 Please provide any further comments or suggestions you may have about examples in the draft framework code.

Usability for non-campaigners and individual citizens

The guidance reads like a document that is intended for the compliance departments of political parties, and in many ways it is. It would be difficult, however, for an ordinary citizen to understand. ORG feels that this speaks to the guidance's narrow focus.

This guidance is an opportunity not just to make data driven campaigning easier for political parties, but also to empower citizens to exercise their rights, under data protection law, in the context of political campaigning. Further consideration should be given to its usability.

For instance, it would be useful to have examples that are centred in the lived experience of individual citizens rather than political campaigners. Additionally, the guidance could include a summary checklist or list of questions for individuals to assess against their situation.

¹⁸ Ibid, pp 10-15.

Q13 To what extent do you agree that the draft framework code is clear and easy to understand?

- ☐ Strongly agree
- ☐ Agree
- ☒ Neither agree nor disagree
- ☐ Disagree
- ☐ Strongly disagree

Q14 Are you answering as:

- ☐ An individual acting in a private capacity (e.g. someone providing their views as a member of the public or the public)
- ☐ An individual acting in a professional capacity
- ☒ On behalf of an organisation
- ☐ Other

Please specify the name of your organisation:

Open Rights Group

Thank you for taking the time to share your views.