~~PRIVACY~~
~~INTERNATIONAL~~

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

October 2019

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.

On the whole, Privacy International welcomes the ICO's draft Code of Practice as a first step in seeking to ensure that the use of data in political campaigning complies with the law (the Data Protection Act 2018 ("DPA 2018"), the General Data Protection Regulation ("GDPR") and the Privacy and Electronic Communications Regulations). We also welcome the inclusion within the draft Code of a number of issues Privacy International raised in our response to the ICO's call for views in 2018.

However, the Code, even once in place, must only be seen as one step in the many that must be taken to ensure open and transparent political campaigning, that fosters rather than undermines trust and integrity in the democratic process. Much remains to be done to close the implementation and enforcement gap (in data protection and electronic marketing law) and strengthen existing regulatory frameworks (data protection, as noted elsewhere in this consultation; the pending ePrivacy Regulation; and electoral law). This is all essential to the protection of people's rights, including the right to privacy and data protection, the right to freedom of expression, the right to freedom of thought and the right to political participation.

That said, whilst the draft Code covers many of the requirements of data protection and electronic marketing laws, there is a lack of detail in some parts (explained further down) and there are some aspects of the law which are not included or elaborated upon at all with in the draft.

The following are particularly absent, despite being highlighted in Privacy International's response to the ICO's call for views, and should be included:

- **Rights of data subjects**

The rights of data subjects enshrined in Chapter III of the GDPR are a core pillar of data protection, which as noted above is a fundamental human right. These rights are essential for empowering individuals and are tools for enabling individuals to exercise some control over their data. We note that the Code is not an exhaustive guide to data protection, and that references to a number of rights are made within the draft, in particular the right to object – which is welcome. However, given the importance of these rights and the difficulties too often faced when individuals seek to exercise them, we consider that inclusion of further detail throughout/ a specific section on rights within the Code is merited. Examples, of how difficult it can be to exercise data subject rights in relation to political parties and data brokers (many of whom supply data to political parties) can be found here https://news.sky.com/story/labour-failing-on-digital-rights-say-campaigners-11795068 and here https://privacyinternational.org/blog/2549/have-companies-deleted-your-data .

- **Sanctions/ Remedies**

Sanctions and remedies are core to accountability in data protection and electronic marketing law, and are imperative in the political campaigning context. We strongly recommend including within the Code how these apply, including prior to and after elections and referenda given the often unique and far reaching consequences in the electoral context.

Whilst there is a note on page 6 of the draft Code listing some of the tools at the ICO's disposal and the power to issue fines, we recommend that the ICO's other powers be highlighted, including the ICO's investigative powers and, for example, the power to halt a particular processing operation. In many cases these will be more powerful than a monetary penalty. The Code is also an opportunity to set out how the ICO might use its audit/ assessment notice powers in this context. We note that in July 2018, the ICO wrote formally to 11 political parties in the UK, served assessment notices and as part of this audited their practices. However, as far as we are aware, no further information about the results of these steps has been made public. The Code should require regular audits of political parties and public reporting of the results. Scrutiny and resulting accountability are essential in order to improve practices.

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 2020 under section 189 of the Data Protection Act 2018. As it currently stands, it is not possible to bring systemic challenges to failures to comply with the law, including in the political campaigning arena. The failure of the UK to implement Article 80(2) of GDPR strips a core accountability mechanism from GDPR and puts the emphasis on complaints by individuals. This is often extremely challenging given the hidden nature of processing in political campaigns and those they work with, such as data brokers or ad tech companies, and the power imbalance that exists, for example with social media companies. Recent Privacy International research demonstrates the need to take action on systemic violations of data protection and electronic privacy law, which are often hidden or industry practice, including by data broker and ad tech companies (https://privacyinternational.org/campaigns/tell-companies-stop-exploiting-your-data) (many of which are used in political campaigns), mobile phone apps (https://privacyinternational.org/campaigns/investigating-apps-interactions-facebook-android and https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruation-apps-are-sharing-your-data) (this data sharing is likely prevalent in many political apps) and websites (https://privacyinternational.org/campaigns/your-mental-health-sale) (again, many political campaign websites are full of trackers). Privacy International complained to the ICO about data broker and ad tech companies in November 2018 (https://privacyinternational.org/legal-action/challenge-hidden-data-ecosystem). Despite the passing of almost a year since we complained and over a year since the ICO announced assessment notices of Experian, Equifax, Acxiom and a number of other data brokers and credit reference agencies, the ICO is yet to report publicly/ take any enforcement action. This serves to illustrate the need to set out what remedies are available and the need to implement Article 80(2).

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

☐ Yes
☒ No

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

The draft Code clearly makes some effort to go into detail, as demonstrated by its length. However, in our view much of the draft Code re-explains data protection law as opposed to setting out what this means in practice for political campaigning.

A Code should by nature go into detail on the practical application of the law, including in relation to specific contexts and technologies. This Code is, therefore, the opportunity to 'put the meat on the bones' and state clearly what the principles and other parts of data protection and ePrivacy law mean in the context of political campaigning, by way of practical guidelines and useful examples. The Code will be a yardstick by which campaigns develop and measure their practices, thus it must include more detail, be more clear and, in some cases, prescriptive.

Some key areas where we consider that more detail needs to be provided are:

- **Transparency**

  Transparency is a core principle under GDPR, and a new principle, given that it was not explicit under the Data Protection Act 1998. This principle ties in with many other aspects of GDPR and the DPA 2018, in particular the right to information in Articles 13 and 14 of GDPR. Transparency is a theme throughout the draft Code and is addressed specifically in the section of the draft Code on the principle of lawful, fair and transparent processing. The provision of 'privacy information' is raised multiple times. However, we consider that in its current form, the draft Code does not provide sufficient detail as to what this principle means in the political context and what should be done in practice. More detail must be added. This is particularly important, given the reference at a number of points in the code to 'invisible processing' in this context. The current lack of pro-active transparency by political campaigns and those companies they work with is a huge obstacle to scrutinising their practices, further eroding trust.

  We therefore suggest adding a more detailed section on Transparency with the following prescriptive but non-exhaustive suggestions. There may be value in addressing these at specific types of controllers covered by the Code, such as political parties and social media platforms as well as other actors like data brokers and data analytics companies. Adding checklists to this effect would also be helpful.

We also note that page 50 of the draft Code mentions centralised transparency initiatives organised by the ICO or the Electoral Commission. We would welcome more detail on what these are and what they entail.

The below suggestions are not intended as new obligations, which we understand the Code is not intended for, but rather ideas which if elaborated on by the ICO would provide practical guidance on the Transparency principle and the provision of information under Article 13 and 14 of GDPR. A cursory review of privacy policies of political parties in the UK, the social media platforms, data brokers, and campaign tool companies, highlighted by the ICO in previous reports, demonstrates that all have a long way to go in terms of providing the bare minimum prescribed by Articles 13 and 14, let alone meaningful transparency in terms of the Transparency principle and the EDPB Guidelines on Transparency and Automated decision-making and profiling.

Political Parties/ Campaign groups:

Should as a minimum:

1. Be transparent about their data processing activities, including any practices of their processors or joint controllers, including, identifying the mechanisms they use to reach/ engage with voters (e.g. social media, websites, direct messaging and campaign and targeting methods) and what personal data they process.
2. Be transparent about how they collect people's data and the sources of this;
3. Be transparent as to their profiling practices, including any practices of their processors or joint controllers, including making inferences, as well as explaining any automated decision making.
4. Be transparent on their political ads and messaging. They should ensure that the public can easily recognise political messages and communications and the organisation behind them. They should make available information on any targeting criteria used in the dissemination of such political messages;
5. Publish a complete, easily accessible and easily understandable list of any campaign groups they have financial or informal collaborative campaigning relationships with, including all third parties and joint campaigners.
6. Publish data protection policies and data protection audits and impact assessments;
7. Be transparent as to the companies they contract with as part of their campaigns both to obtain data and to further process data, including profiling and targeting, such as data brokers and political

advertising companies, as well as which companies are providing campaign tools/ software and the products they are using;

8. Make publicly available timely information on their expenditure for online activities, including paid online political advertisements and communications. This should include information regarding companies assisting them in their online activities, including the amount spent on each companies' services and which services;
9. Provide detailed information about how people's data is processed, including purposes, the data they process, the recipients, retention periods, the legal basis, the source, profiling and any targeting techniques used.
10. Publish mechanisms and procedures for reporting and responding to concerns.

Social Media or other platforms where political adverts are displayed:

Should as a minimum:

1. Be transparent about how political campaigns can use their platform and whether there are any restrictions in place.
2. Be transparent about any political campaigns they are working with, including directly, such as embedding staff into a campaign.
3. Be transparent about any policies in relation to political or issue ads and communications.
4. Be transparent as to how they define political or issue ads and the basis for this definition.
5. Be transparent in relation to any specific measures or steps being taken in specific contexts, such as an upcoming election or referendum.
6. Be transparent to users about how they are targeted with ads, this includes insight into what data was used to target the ad, including the source of that data; the target and audience of the advertiser; who uploaded the ad; who sponsored the ad/ paid for it; if profiling was used; and whether the data was used to create a 'lookalike' audience and/ or whether they are being shown an add as part of a 'lookalike' audience.
7. Ensure that advertising, including political and issue ads, are publicly accessible, with information about data sources, who has paid for the ad and the targeting criteria for the ad.
8. Be transparent about steps being taken to ensure sponsored content or other forms of alternative advertising occurring on their platform are included within any transparency efforts.
9. Be transparent as to reporting mechanisms and national contact points.

Companies that provide services to Political Campaigns – including as a data source (i.e. data broker or ad tech company) or a provider of software/campaign tools:

Should as a minimum:

1. Publish the names of any clients involved in political campaigning and what services they provide to them, including any data provided or data processing activity (such as, for example, a 'Match' type service).
2. Publish data protection impact assessments in relation to any work related to political campaigning.
3. Be transparent about how they have implemented data protection by design and by default.
4. Be transparent about how they ensure individuals whose data is processed by them or their clients are provided with the information they are entitled to under Articles 13 and 14 of GDPR and what that information is.

- **Profiling**

We welcome this section and many aspects of it. However, we consider further detail is required. This includes in terms of transparency, whereby what is required should be more explicit. The EDPB guidelines on Transparency and Automated Decision-making and Profiling elaborate on transparency and profiling, including specifically in relation to data sources/ input data. Similarly, in relation to profiling, it is essential to be clear regarding the legal basis and further elaboration is needed on the principle of purpose limitation. We also consider that the Code should spell out the need to do and publish a Data Protection Impact Assessment in relation to any profiling undertaken in political campaigning.

- **DPIAs and other assessments re lawful basis**

Data Protection Impact Assessments ("DPIAs") are referenced and encouraged throughout the draft Code. This is welcome. In particular, we note that in case of reliance on the disproportionate effort provision, the draft Code indicates that the DPIA should be made public. We consider that the Code should go even further and indicate that the default position be that the 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.

Furthermore, publication of a justification for reliance on other lawful bases should be encouraged, including section 8 of the DPA 2018 together with Article 6(1)(e) of GDPR.

We have concerns about the condition in paragraph 22 of Schedule 1 to the DPA 2018 (expressed elsewhere in this submission). However, as a minimum, if a party is to rely on this condition, the appropriate policy document should be published.

- **Purpose limitation**

This principle is addressed in the section in the draft Code on 'Purpose limitation, data minimisation and storage limitation'. However, it should be referenced much more throughout, in particular in the final sections of the draft Code, from 'Profiling' onwards, including as noted above in relation to profiling but also for example in relation to list based/ audience targeting on social media.

- **Fairness**

As acknowledged throughout the code, fairness is an important core principle of data protection law and links to the reasonable expectations of individuals and the potential consequences of particular processing operations. However, it is so vital in the political context, that is merits

further elaboration throughout, especially when it comes to the section on political campaigning in the online world. The ICO's own research in relation to AdTech ((https://ico.org.uk/media/about-the-ico/documents/2614568/ico-ofcom-adtech-research-20190320.pdf)as well as many other studies (for example, by DotEveryone (https://doteveryone.org.uk/report/digital-understanding) or the Eurobarometer 2019 (see para 5 http://europa.eu/rapid/press-release_IP-19-2956_en.htm
)) demonstrate that most people do not have a clear understanding of how their data is collected, observed and inferred, used for profiling and then targeting them – whether that be with advertising, search results, a recommendation or curation of a feed. However, as soon as they do become aware they become increasingly uncomfortable and the processing does indeed not fall within their reasonable expect**ations.**

Therefore, it is important to emphasise in terms of fairness that the apparent normalisation of the use of many campaigning methods in the online world coupled with lack of enforcement action against the majority of actors does not mean that the processing is fair.

- **Processors**

Whilst processors, including the difference between processors and controllers, are mentioned in the draft Code, we would suggest having a specific section making clear processor responsibilities and providing practical guidelines and good practice. This is important given the introduction of specific obligations on processors under Article 28 of GDPR.

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.

The response to this question should be read in conjunction with the above answer. In a number of places where we have suggested that more detail be added, it is because we consider that the Code needs to go into detail both to provide more clarity on the law and on good practice.

In addition, we would highlight the following:

- **Special category data**

Special category personal data, including political opinions, should not be interpreted narrowly. The prohibition in Article 9(1) of GDPR clearly covers "Processing of personal data revealing racial or ethnic origin, political opinions etc…" This must be made even more clear in the Code i.e. data that is not explicitly political opinion or another category, may still be special category personal data.

Privacy International has expressed concerns on numerous occasions, including during the passage of the DPA 2018 and in response to the ICO's call for views, on the condition in paragraph 22 of Schedule 1 to the DPA 2018 relating to political parties. A similar provision in the Spanish data protection law has been declared unconstitutional (https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2019_076/Press%20Release%20No.%2076.2019.pdf) and another in Romania is the subject of a complaint to the European Commission (https://privacyinternational.org/news/2735/romanian-ngo-files-complaint-european-commission-national-implementation-gdpr). We are concerned that political parties are using this loophole to avoid the need to get explicit consent. As a minimum, the Code should (i) indicate that the 'appropriate policy document' be published; and (ii) provide an example in relation to this provision. However, in tandem the ICO should investigate how and for what purposes political parties in the UK are relying on this provision.

- **Data from Third Party Sources**

We welcome the inclusion of a section in the draft Code covering the use of data from third party sources - 'Can we use data collected from third parties such as data brokers or other companies providing marketing services' - as Privacy International has a number of concerns about this practice. However, we consider that further clarity and guidance on the law and good practice is needed. In relation to 'factual data' for example, the draft Code notes that this data can be used where an individual has been provided with appropriate privacy information and its use is within their reasonable expectations. Again, as highlighted elsewhere, we do not consider current practices are within people’s reasonable expectations. There continues to be a dearth of transparency in terms of these data sources (both by the sources themselves and those using them).

As our submissions to the ICO regarding data brokers (whom, as the ICO itself has reported, have worked with political parties) make clear, these companies are systematically failing to be transparent and fair, lack a legal basis for the majority of their processing and present numerous challenges for the exercise of data subject’s rights (https://privacyinternational.org/legal-action/challenge-hidden-data-ecosystem). Therefore, it is imperative that more detail is added to the due diligence section. Ultimately, given the problematic nature of these practices, we question how the use of this data can comply with the requirements of data protection and electronic privacy law, in particular the principles of transparency, fairness, lawfulness, purpose limitation and minimisation. Noting the ICO’s previous calls for an ‘ethical pause’ in July 2018, and due to the highly problematic nature of these practices, it is hard to see how the law (including people’s rights) can be complied with without some pause of the procurement by political campaigns and those they work with of data from these companies. In almost every case, this involves the hidden collection or generation (i.e. observed and inferred data) of data about someone, being used in a way they would not expect for a purpose other than that which it was originally intended.

In this section we are also concerned that it be made explicitly clear, that even where data provided might not be ‘personal’, where this is related back to individuals, including at household level, then this is personal data and all the provisions of the GDPR and DPA 2018 must be complied with. As the ICO is well aware, and as is made clear elsewhere in the Code, the definition of personal data, includes indirectly identifiable data, and names and addresses are not the only identifiers.

As noted above, the due diligence section requires further elaboration given the existing problems in this industry, as set out in our submissions to the ICO. This due diligence may require numerous ‘layers’. For example, as noted in our submissions to the ICO concerning Acxiom (see page 14 https://privacyinternational.org/sites/default/files/2019-08/08.11.18%20Final%20Complaint%20Acxiom%20%26%20Oracle.pdf), when a member of Privacy International’s staff obtained a copy of their data from Acxiom, the source was listed as another data broker, ‘Read Group’, which disclosed, upon a further subject access request that the source was ‘Omnis Data Ltd’. This demonstrates that it is excruciatingly difficult to untangle the web of data, finding the original source of the data is like finding a needle in the haystack.

- **Electoral register – opt out**

We note the explanations regarding access to the two versions of the electoral register data. However, the draft Code does not provide an explanation of the law in terms of why inclusion in the open register, operates on an opt-out basis, including in terms of the principles of transparency, fairness, lawfulness and purpose limitation. Furthermore, we do not know whether the Code is the correct place, but we consider that there must be a publicly accessible database of all parties that have bought access to the register and for what purpose.

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?

As highlighted in Privacy International's response to the ICO's call for views, there are numerous actors involved in political campaigning and therefore it is important that the Code applies beyond, for example, registered political parties. We, therefore, welcome that the scope of the draft Code covers "controllers processing personal data for political purposes". However, as noted above we consider guidance for processors should also be provided. We also consider that more detail is required in relation to the following activities:

- **Campaigning outside of an election**

In terms of the political campaigning activities covered by the draft Code, we are concerned that the draft Code may be unduly narrow, as even though it is not limited to a restricted time period, it seems to generally relate to campaigning during elections. This does not reflect the reality of political campaigning which takes place outside of an election. This is re-enforced by the chosen examples, (as highlighted further below), which do not cover party leadership campaigns or issue advocacy, and tend to focus on political parties and candidates without sufficient reference to other actors involved (such as platforms) and digital campaigning methods.

- **Digital and experimental campaign techniques**

The ICO acknowledges in the draft Code and in previous reports, including Democracy Disrupted, that the nature of political campaigning has fundamentally changed and a primary driver of the Code is to cover digital campaigning. Various digital political campaigning methods are highlighted in Privacy International's response to the ICO's call for views, and in case studies we have gathered (for example, re France https://privacyinternational.org/examples/data-exploitation-french-elections , Italy https://privacyinternational.org/examples/data-exploitation-italian-elections Germany https://privacyinternational.org/examples/data-exploitation-german-elections and Ukraine https://privacyinternational.org/examples/data-exploitation-ukrainian-elections.) The report by Demos for the ICO illustrates examples, as does the report by Tactical Tech 'Personal Data: Political Persuasion. Inside the Influence Industry. How it works.' (https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/Personal-Data-Political-Persuasion-How-it-works_print-friendly.pdf)

Therefore, whilst we welcome specific sections on profiling, direct marketing and campaigning in the online world, in our view the draft Code still does not go into sufficient detail (campaigning in the online world begins at page 82) nor does it provide enough examples to reflect use of new and emerging technologies in political campaigning (more below).

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?

As noted above, whilst the draft Code covers a number of important points about political campaigning in the online world, more detail and examples are required, in particular in relation to the following:

- **More detail and examples on digital/ online campaigning techniques and tools**

Examples, which it would be helpful to include within the Code and that are not currently covered, include the use of:

- ○ **Apps** (various types, including canvassing) – apart from reference to privacy information and that they might be used for canvassing, no further detail or examples are provided within the draft Code. Political campaigns are increasingly using apps, as illustrated in the reports etc mentioned above, and the failures in terms of data protection and ePrivacy in many apps are numerous (as demonstrated by Privacy International's research (https://privacyinternational.org/campaigns/investigating-apps-interactions-facebook-android and https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruation-apps-are-sharing-your-data)

- **Targeted digital advertising on TV** – despite mention of this in, for example, the Tactical Tech and Demos reports cited above and recent academic papers (see a summary here https://twitter.com/random_walker/status/1177570679232876544) , targeted TV advertising/ addressable TV, is not mentioned in the draft Code and much more attention needs to be paid to the implications of this for the political context.

Despite examples being provided in the reports referenced above, noted in Privacy International's response to the call for views, and meida reporting that these techniques are being used or available for use, the following are not addressed in the draft Code, but should be:

- Geo-targeting and Geo-fencing
- A/B Testing
- Cross device targeting
- Sentiment analysis and emotion recognition

- **More detail/ examples regarding actors other than political parties/ candidates**

More examples should be provided as to how the Code applies to actors other than political parties and candidates. These include the social media platforms, data brokers, data analytics companies and companies providing tools such as data matching and web-scraping. Examples should also be provided of those processing personal data for political purposes that are not in a registered party or part of an official campaign.

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.

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint
Instagram @privacyinternational

UK Registered Charity No. 1147471