Information Commissioner's Office

Audits of data protection compliance by UK political parties

Summary report
November 2020

ico.
Information Commissioner's Office

Contents

Foreword

In a world where digital innovation has changed so much of how we all live our lives, it is no surprise that our relationship with how we engage with the democratic process has also changed.

Whether we are sharing our views with others or registering to vote, the starting point for our political engagement is so often digital. This will also involve the use of personal information.

Data from the Electoral Commission shows 42.8% of advertising spending by campaigners was on digital advertising in 2017, compared to just 1.7% in 2014[1]. In their report into campaigning at the 2019 UK Parliamentary general election[2], the Commission's research found that transparency about who is behind political campaigns online at elections is important for people in the UK; with three quarters of people stating that they felt it was important for them to know who produced the political information they saw online, but less than a third knew how to find out who produced it. Nearly half (46%) agreed that they were concerned about why and how political advertising was targeted at them. The tools and techniques previously seen in commercial marketing are now increasingly explored by political parties.

Society benefits from political parties that want to keep in touch with people, through more informed voting decisions, better engagement with hard to reach groups and the potential for increased engagement in democratic processes. The use of new technologies that utilise personal information for political campaign purposes is only going to grow, and particularly so as society adapts to the challenges brought by COVID-19, and our increasing reliance on digital contact.

Trust is crucial in this process, not only in informing our confidence in political parties, but also in democracy more broadly. The transparency and accountability required by data protection is a key aspect in developing trust, and so there is an important role for the ICO in scrutinising this area.

In our Democracy Disrupted report, published in July 2018, we highlighted significant concerns about transparency around how people's data was being used in campaigning. Our report drew back the curtain on a complex ecosystem of digital campaigning, with many actors. Political parties have a central role in this ecosystem, both in how they collect and use data themselves, and through responsible use of data driven services.

---

[1] https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/changing-electoral-law/transparent-digital-campaigning/report-digital-campaigning-increasing-transparency-voters

[2] http://www.electoralcommission.org.uk/who-we-are-and-what-we-do/elections-and-referendums/past-elections-and-referendums/uk-general-elections/report-2019-uk-parliamentary-general-election-was-well-run/depth-campaigning-2019-uk-parliamentary-general-election

All political parties must use personal information in ways that are transparent, understood by people and lawful, if they are to retain the trust and confidence of electorates.

Among the key policy recommendations within that report was a commitment from my office to undertake data protection audits to assess compliance with data protection law. This work began in early 2019, when we issued assessment notices to seven political parties[3]. The parties engaged positively with the audit process, and there was a genuine desire from the parties to respect people's data protection rights.

This report details those positives, as well as setting out the changes we found they needed to make. We have taken the decision to publish these findings cumulatively, rather than each individual audit report, as we feel this overarching view provides a clearer picture of compliance, given the common themes we found.

These were the first comprehensive audits of political parties we have undertaken, and they took place in the context of a new data protection law coming in to force within a year of the start of the audits. Overall, the audits found only a limited level of assurance that processes and procedures were in place and delivering the necessary data protection compliance. We therefore identified considerable scope for improvement, and, whilst recognising there were some positive elements of compliance, our audits showed that the parties needed to take further steps. The positive manner in which the parties received our recommendations, and their commitments to make the changes we advised, led us to adopt a voluntary compliance approach when considering whether enforcement action was necessary.

All political parties must be clear and transparent with people about how their personal data is used and there should be improved governance and accountability. Political parties have always wanted to use data to understand voters' interests and priorities, and respond by explaining the right policies to the right people. Technology now makes that possible on a much more granular level.

This can be positive: engaging people on topics that interest them contributes to greater turnout at elections.

But engagement must be lawful, especially where there are risks of significant privacy intrusion – for instance around invisible profiling activities, use of sensitive categories of data and unwanted and intrusive marketing. The risk to democracy if elections are driven by unfair or opaque digital targeting is too great for us to shift our focus from this area.

These areas will be therefore among those the ICO reviews later this year, when we follow up our audits and ask the parties to show the changes they have made in response to our audit findings and recommendations. We reserve the right to take formal regulatory action should those reviews indicate parties have failed to take

[3] The Conservative Party, The Labour Party, The Liberal Democrats, The Scottish National Party (SNP), The Democratic Unionist Party (DUP), Plaid Cymru and The United Kingdom Independence Party (UKIP)

appropriate steps. This is both a proportionate and effective requirement given the level of engagement we have received so far, and in line with the ICO's Regulatory Action Policy.

Our learning from conducting these audits will also inform the update to our existing guidance on political campaigning, due later this year. The guidance will be relevant not only to political parties, but also to other campaigners, pressure groups, data brokers and data analytic companies.

Together, this body of work forms an important area of focus for the ICO, reflecting our stated commitment to improve standards of information rights practice through clear and targeted engagement.

Elizabeth Denham, CBE
Information Commissioner

Introduction

The ICO undertook this work as part of our investigation of the wider ecosystem of large, well-established trading and profiling of personal data. The scale and the scope of the processing is significant, involving the personal data of millions of individuals. However this ecosystem, and an individual's place in it, is unknown to the public. We have already made recommendations to the entire credit reference industry and undertaken audits of the main credit reference agencies and three data broker organisations. We have taken formal regulatory action where appropriate.

All the parties engaged positively with the audit process and seemed to welcome the opportunity to discuss and exchange their data protection issues and examples of good practice with the ICO's audit team. We recognise the unique role political parties play in a democratic society.

However, political parties are not exempt from data protection law; they have responsibilities as data controllers to follow all the requirements of the law, including the data protection principles. Developments in the use of data analytics and social media by political parties have been so rapid that they have left many voters on the back foot. If voters are unaware of how their data is being used to target them with political messages, then they may have limited awareness of how to exercise their rights about the use of that data and the techniques being deployed.

Our initial findings published in our Democracy Disrupted Report in July 2018, where we observed with concern the application of commercial behavioural advertising techniques and the lack of transparency of profiling in political campaigning, demanded that improvements were made to data protection frameworks to further safeguard individuals' privacy.

Key findings

The audits found some considerable areas for improvement in both transparency and lawfulness and we recommended several specific actions to bring the parties' processing in compliance with data protection laws. In addition, we recommended that the parties implemented several appropriate technical and organisational measures to meet the requirements of accountability. Overall there was a limited level of assurance that processes and procedures were in place and were delivering data protection compliance.

Key finding 1: Privacy information

Parties should review their privacy information and notices. They should ensure that the information is comprehensive yet brief, and use clear and plain language, so that individuals will understand from the outset how the parties are using their data.

Key finding 2: Lawful basis

Parties should review the lawful bases for their processing of personal data and special category data to ensure they have identified the most appropriate basis. Where the lawful basis is consent, they should update consent statements to ensure they are specific, granular, clear, opt-in and prominent.

Key finding 3: Profiling

Parties must be very clear with individuals about any unexpected or intrusive uses of personal data, such as combining information about them from several different sources for the purposes of profiling. They should carry out and record appropriate checks on suppliers, to ensure personal data is processed and supplied lawfully and in a manner which is compatible with what they originally obtained it for and their intended new processing.

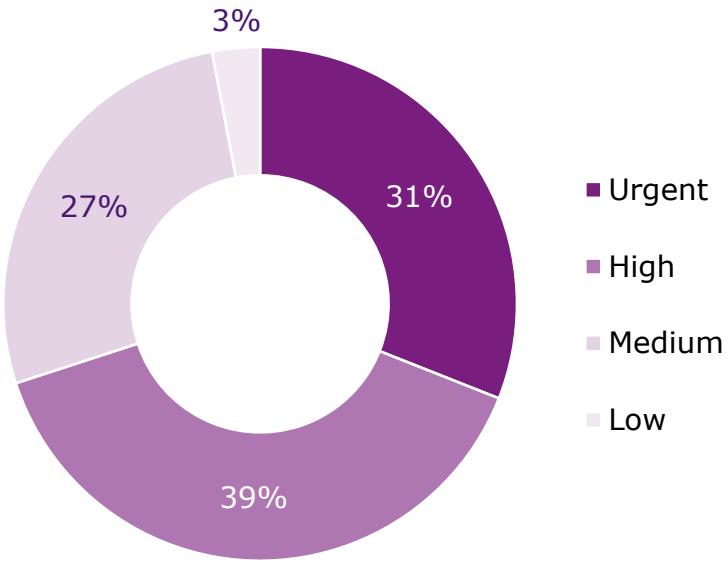
Key finding 4: Use of social media for marketing and campaigning

Parties must inform individuals and be transparent when using their personal data to profile and then target them with marketing via social media platforms. When parties look to use a platform's targeting tools, both the party and the platform itself should clearly set up the circumstances where joint controllership exists and have appropriate contracts in place.

Key finding 5: Accountability

Parties must be able to demonstrate their compliance and be proactive about data protection, evidencing the steps they have taken to meet their obligations and protect people's rights. They must also carry out thorough checks on all contracted and potential processors and third-party suppliers throughout the supply chain to gain assurances that they comply with the key transparency, security and accountability requirements of data protection law.

Summary of the recommendation priorities assigned across all audits



The chart shows the percentage of urgent and high priority recommendations we made across all audits. We made these recommendations to assist the parties to address compliance issues which represented clear and immediate risks to their ability to comply with the requirements of data protection legislation.

Methodology

From June 2019 to September 2019, the ICO conducted audits of seven political parties in the UK. The scope of the audits covered certain key areas:

- **Management structures** – a review of the management framework, to ensure there was a delegated process of accountability and responsibility and effective oversight of data protection compliance.
- **Policies and procedures** – to ensure that management support and direction for data protection compliance was set out in a framework of policies and procedures, which were approved by senior management and subject to routine review so they remained fit-for-purpose.
- **Data Protection Impact Assessment (DPIA) governance and processes** – to ensure that robust technical or organisational measures were in place so that a DPIA was initiated for all appropriate projects in a timely fashion.
- **DPIA consultation and outcomes** – to review the process of internal and external consultation on the completion of a DPIA and ensure that the results of the DPIA were documented in a formal report.
- **Accuracy and integrity of records** – to audit the procedures in place to ensure the adequacy and accuracy of information, confirming that it was not

excessive for the purposes. This included the technical and operational measures to ensure the integrity and security of information.

- **Fairness and transparency** – to ensure that individuals were informed about the use of their personal data. This included a review of the various types of processing the parties carried out and the lawful basis for processing activities. Where consent was used as the lawful basis (or condition) for processing, consent mechanisms should comply with the GDPR.
- **Management of data broker arrangements** – to ensure that personal data (such as lifestyle information or marketing data) was only obtained from reliable sources. Also, that personal data was only obtained for specified purposes, and was reliant on pre-identified legal bases. Finally, to ensure that data was obtained through secure mechanisms and reviewed on receipt to ensure it was relevant, adequate, accurate and not excessive and that parties undertook regular reviews of data brokering to ensure systems were effective.
- **Data analytics and profiling** – to ensure that appropriate checks and safeguards were in place prior to the use of data analytics companies and that profiling or data modelling of data subjects complied with the GDPR.
- **The use of social media for marketing and campaigning purposes** – to audit the sharing of personal data to confirm that personal data was only shared with appropriate partners, was only shared for specified purposes and was reliant on pre-identified legal bases. Where data was shared, this was done through secure mechanisms and reviewed to ensure it was relevant, adequate, accurate and not excessive.
- **The use of online campaign platforms** – to ensure the collection and use of public domain information for political campaigning was managed in a lawful and secure way.
- **Individual rights** – to ensure there were procedures in place to allow individuals to exercise their rights of erasure, restriction and objection under data protection law and for recognising and responding to individuals' requests for access to their personal data.

The audits were conducted following the ICO's data protection audit methodology. The key elements of this were a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff and an inspection of selected records.

The findings from our work are taken as a 'snapshot in time'. It is therefore important to view the findings as being solely based on what we found at the time of each audit, and consider that the parties may have undertaken work since to change the nature of their processing and campaigning activities, improve compliance and mitigate risks.

Findings in relation to political processing activities

Data collected, processed and retained

There are over 45 million people across the UK who are at voting age or will reach this age in the coming year. All political parties in the UK collect, process and retain data for use in political campaigning and associated activities[4]. The volume of data collected, processed and retained for use in political campaigning and associated activities varied across the parties depending on the size of the electorate they were targeting. For example, the Scottish National Party (SNP), the Democratic Unionist Party (DUP), Plaid Cymru and the United Kingdom Independence Party (UKIP) collected, processed and retained less voter data than Labour, the Conservatives and the Liberal Democrats.

Parties also retained and processed data that was necessary for administering their own internal governance and membership systems.

All parties typically obtained data from the following sources:

- The full electoral register, which political parties have a statutory right to access under the Representation of the People (England and Wales) Regulations 2001 and the Political Parties, Elections and Referendums Act. It contains details about every registered individual who is of an eligible age to vote, or will reach that age in the next year, and equates to over 45 million voter records. This will then act as the 'spine' to which other data can be appended.
- The marked register (which is a copy of the electoral register that has a mark by the name of each elector who has voted).
- Directly from individuals, usually by asking them in person on their doorstep or over the telephone. The information collected usually included their voting intention but could include answers to a variety of other questions. Parties also collected information electors had themselves placed in the public domain about their political views.
- Publicly available data and other data sets such as census data, election result data, Land Registry data, polling data, social housing data and data sets compiled by government or independent government agencies.

Lifestyle information obtained from third-party organisations ('data brokers')

Some political parties obtained lifestyle-type information on individuals from data broking organisations under commercial agreements. The information was used to

[4] Parties are processing two types of data: personal data (eg name, address, age); and data relating to political opinions (termed special category data). The law provides special protections to special category data, which parties process under Article 9(2)(g) and Recital 56 of the General Data Protection Regulation (GDPR), and the Data Protection Act 2018 (DPA 2018) Schedule 1 section 22; this is because its use could create significant risks to the individual's fundamental rights and freedoms or open someone up to discrimination.

categorise individuals in several areas according to various social and lifestyle factors. This information was then directly linked to individuals forming an attribute on which processing decisions were made.

The Labour Party, the Conservative Party and the Liberal Democrats obtained commercially available data about individuals, either factual, estimated, or a combination of both, from suppliers under commercial terms, in addition to the standard data sets used by most parties (as mentioned above). These three parties also had access to other UK-wide databases through commercial agreements.

Commercially available estimated data that Labour and the Conservatives bought, which was typically available at both household and individual level, included estimates of:

- employment status;
- income;
- presence or absence of children in the household age;
- family structure;
- level of educational achievement; and
- onomastic data, which identified a person's gender based on their first name.

Another set of commercially available estimated data bought by Labour and the Conservatives was a geodemographic segmentation, widely used in commercial direct marketing, available at three levels of spatial granularity (postcode, household and person). They did not use this specifically for direct marketing but to formulate a better understanding of voter patterns and issues through segmented groups.

The Conservatives purchased estimated onomastic data, ie information derived from the study of people's names which identified a person's county of origin, ethnic origin and religion based on their first and last name. This was appended to the records of 10 million voters. They also had access to the National Deceased Register under commercial agreement, purchased telephone numbers from suppliers and instructed anonymised market research.

Labour only sourced data from one supplier; who used information about individuals aggregated from multiple sources, or otherwise enhanced, to build individual profiles. The party had previously sourced other onomastic data, however they ceased buying this type of data as they could not justify its lawful use following the GDPR and the DPA 2018 coming into force.

The Liberal Democrats sourced commercial data which included a selection of 25 voter 'attributes'. The supplier estimated the attributes they obtained, including data implying an individual's age or the likelihood of them reading a newspaper. They used this data to better target the Liberal Democrat's advertising to individuals who may support the party.

At the time of the audits, the SNP, DUP, Plaid Cymru and UKIP did not source any commercially available data.

Use of data analytics and modelling

Most parties maintained their own databases of UK voters which stored all the data collected about an individual from that party's campaigning activities. Parties then analysed and profiled this data to derive further data.

Some political parties were using third-party organisations to carry out data analytics modelling, to create predictive scores on the party's behalf. For example, the likelihood of individuals voting in a certain way, their likelihood of turning out to vote at all, or both.

Parties then used their datasets and analysis in a number of ways, which included, for example:

- informing the purchase of advertising on social media to target individual social media users;
- sending out targeted emails or telephone canvassing voters to encourage individuals to vote or change their voting behaviour; and
- deciding who to canvass on the doorstep during a campaign or on the day of voting itself.

The Conservatives carried out data analytics and profiling internally; however, external consultants were contracted to assist with data analytics. The party had their own analytics and profiling platform which they used to build propensity and turn-out models and target voters in the ways set out above.

Labour conducted this activity in-house by party staff in their head office. They then used these results for analysis and targeting, as detailed above.

The Liberal Democrats carried out modelling and analytics using a third-party analytics company to produce voter scores which predicted the likelihood of an individual supporting a particular political party, as well as the likelihood of individuals switching votes between parties.

Plaid Cymru used publicly available census data to identify Welsh speakers so that they could target their campaigning activities at those individuals or demographic areas.

Social media used for marketing purposes

Labour, the Conservatives and the Liberal Democrats used social media platforms, such as Facebook, organically as well as for paid marketing campaigns. Audience selection tools on social media platforms were used to create target 'custom' audiences to which political messages could be delivered. These parties manually selected a target audience for a particular advert or advertising campaign based on various characteristics, including age or gender, location, interests and behaviours. These characteristics were used to build profiles to target social media platform users with advertising. Telephone numbers and email addresses of individuals on the parties databases were provided to Facebook in 'hashed' data files to protect the security of the content in transmission. The hashed contact details of individuals were then

matched against the platform's existing list of hashed data, and a 'custom audience' created.

These parties also used Facebook's 'lookalike audience' tool, whereby the characteristics of the custom audience (eg location, age, gender, interests etc) created a larger group of other individuals who shared the same characteristics but who were not yet engaged with the parties through Facebook. They were then targeted with adverts that appeared on their Facebook pages in the same way as the custom audience.

Following the campaigns, the parties received data on the number of individuals who had received the adverts, but not information to identify who those individuals were.

Plaid Cymru, the SNP, DUP and UKIP also used some social media platforms to engage with voters; however, they did not load any personal data to social media campaign platforms. Instead they relied on an organic spread of content through their supporter base. Content posted to their own Facebook page by the parties was delivered to followers of that page and those individuals could choose to share it on to their own contacts.

Good practice

There are some individual areas where we noted that individual political parties had put measures in place to help them to follow the legislation. These included:

- **consent** – deleting all contact information where it was not possible to demonstrate when and how consent was collected, after the implementation of the GDPR. This helped to ensure that consent records were compliant with the clear requirements outlined within the law. This is an important recognition that genuine consent should put individuals in control and build trust and engagement;
- **awareness** – designing guides, booklets and posters to provide guidance and advice to staff in data protection matters. This helped to raise data protection awareness across the party and provide some assurances that staff understood their responsibilities to maintaining the privacy of the personal data of voters;
- **rights** – putting in place procedures to deal with individuals' rights to erasure and to object to processing. Under Article 17 of the GDPR, individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. Article 21 of the GDPR gives individuals the right to object to the processing of their personal data at any time. This effectively allows individuals to stop or prevent organisations from processing their personal data. Having appropriate procedures in place to deal with these requests helps an organisation to ensure they do this in compliance with the GDPR; and

accountability – having Data Protection Officers (DPOs) in post to:

- monitor internal compliance;
- inform and advise on data protection obligations;
- provide advice about DPIAs; and
- act as a contact point for data subjects and the supervisory authority.

Headline areas of concern

Engaging voters is important in a healthy democracy, and to do that political parties, their campaigners and their candidates campaign using a variety of communication methods. However, they must follow the law when doing so; this includes how they handle the personal data they collect and hold.

We identified some common themes within our audits, where parties needed to implement further measures to comply with data protection legislation. Common areas for improvement and action are outlined below. We also recognise that the measures taken by the parties must be feasible, practical and proportionate whilst still achieving legal compliance.

Privacy information

Data protection law requires clear and accessible information to be provided to individuals. Our 2018 report also highlighted the importance of effective transparency across the whole digital campaigning system. All actors in this ecosystem must comply with their transparency obligations.

Article 13 of the GDPR lays out the 'right to be informed' requirements when personal data is collected directly from the individual it relates to. In these circumstances, organisations must provide privacy information at the time they obtain the data. There are some exemptions to this, but in most cases these do not apply to processing for the purposes of political campaigning.

Our audits identified that all parties should review their privacy information and notices. They should ensure that the information is comprehensive yet brief, and use clear and plain language, so that individuals will understand how the parties are using their data.

For example, parties must:

- be more transparent about the processing that is taking place to profile or target individual voters with advertising as part of political campaigning activities;
- inform voters who their data is being shared with, what is being shared and why, eg the data that is shared with social media companies;
- clearly set out within privacy notices the data that they sourced directly, commercially and through open sources. Include in each section the types of data collected, the source of each data set and the purposes for collecting it, so

that an individual can easily locate the information relevant to them from within the notice;

- provide appropriate privacy information at the door or over the telephone, when collecting personal data;
- be more explicit about the processing that takes place under the public task lawful basis and ensure that, where relevant, they include separate information about the use of public interest for processing special category personal data;
- provide privacy information to all individuals that they process personal data about, for example employees or young party members; and
- provide sufficient details about the retention of personal data.

ICO guidance[5] on the 'right to be informed' explains how organisations can use techniques such as layered notices to convey detailed information.

Article 14 of GDPR lays out the 'right to be informed' requirements when organisations obtain personal data from a source other than the individual it relates to, such as a data broker. In these circumstances parties should provide the individual with privacy information, including the source of the data and details of the categories of the data, within a reasonable period of obtaining the personal data and no later than one month.

Example

Individuals will find it harder to exercise their rights, when a party does not provide privacy information to individuals whose data is obtained from third parties and these third parties are not named directly on supplier privacy notices. The burden of obtaining this information is not on the individual; it ought to be provided upfront by the party.

Where a party had been or was obtaining data from third parties, they were relying on proper privacy information being provided to individuals directly by the third party suppliers throughout the supply chain and by those who initially collected the data. Where this was the case, we recommended parties should undertake due diligence to make sure that proper privacy information had been provided to individuals on the party's behalf. If it had not, then this should be provided, unless it is determined that this would involve a disproportionate effort in line with Article 14(5).

To rely on the exemption set out in Article 14(5) parties must undertake a DPIA and then formally document the outcome of their assessment of the effort required to provide privacy information against the impact on the individuals. The parties must fully consider the impact of the processing, and whether it would be within the reasonable expectations of the individual when considering this assessment. If the assessment determines this not to be the case, then they should explore all means of

[5] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/

providing such information as effectively and efficiently as possible, within a reasonable period of obtaining the data.

We recognise that achieving effective transparency to the UK adult population is challenging. In our 2018 report we recommended that wider, joined-up approaches should be also taken to raising awareness of how data is used in campaigning. The ICO will continue to work with the Electoral Commission on this recommendation.

Lawful basis

Most of the processing for political campaigning purposes falls under three lawful bases: public task (democratic engagement); consent; and legitimate interests. Data protection law should not be a barrier to the use of personal data for political campaigning and there are a range of lawful bases available. However, it is important that they are appropriately applied to the context. Our audits included a review of the lawful bases the parties were applying; we identified the following issues and recommended the following actions must be taken:

- The lawful bases that parties were processing personal data under were not always appropriate. We recommended that a complete review of the currently identified Article 6 lawful bases should be undertaken to make sure they are the most appropriate basis for the processing activity they relate to.
- The use of the 'public task' lawful basis that had been applied for some types of data processing undertaken using non-electoral roll data was not appropriate; as to process this data lawfully using this basis, Article 6(3) requires that the relevant task or authority must be laid down by domestic or EU law.
- If there is no separate domestic or EU law to support the use of the public task basis, then an alternative lawful basis must be applied or processing should cease.
- Where there had been a change to the purposes of processing personal data since that data had been collected, and therefore a change to the lawful basis under which this processing was now taking place, parties should implement processes and a review to ensure this processing could still take place lawfully.
- The Article 9 condition for the processing of special category data had not been assessed in all instances and so we recommended that this was actioned and documented. Where no Article 9 condition can be identified for the processing of special category data such as estimated onomastic data, the processing of this data must cease.
- Consent statements did not all meet the GDPR requirements; they should be updated to ensure they are specific, granular, clear, opt-in and prominent.

Profiling

Political parties and campaigners have been employing techniques to understand more about potential voters' interests and characteristics for decades, even centuries. This is an important part of democratic engagement. However, in recent years rapid

technological advancements mean there is greater scope for significant privacy intrusion or wider societal risks such as:

- invisible profiling activities;
- statistically inaccurate automated decision making; or
- unwanted direct marketing.

Where parties do not collect data directly from individuals, they are reliant on data suppliers to collect and share data in a compliant manner. The audits identified that due diligence was not being completed to provide assurances of compliance in this respect and so there is a risk that data used for political profiling is being processed unlawfully.

During our audits we identified the following improvements that must be implemented by parties to improve current practices. Parties should:

- be very clear with individuals about any unexpected or intrusive uses of personal data, such as combining information about them from several different sources for the purposes of profiling;
- carry out and record appropriate checks on suppliers to ensure personal data is processed and supplied lawfully, and in a manner which is compatible with what they originally obtained it for and their intended new processing;
- ensure that, where the data was collected using consent by a supplier, this was done using compliant mechanisms and the consent remains valid under the GDPR. Parties should check supplier consent methods to ensure that individuals were informed of what it is exactly that they have consented to, ie that consent statements were sufficiently transparent to include the type of further processing carried out on behalf of a political party;
- document and implement proper due diligence checks of processors conducting data analytics and profiling on their behalf to provide assurances on the data security arrangements and retention of data;
- carry out due diligence where processors are based outside the EU, to scrutinise their understanding of legislation through the policies, procedures and training they have in place;
- present clear privacy information to voters in the first party communication sent out, relating to the Article 21(4) right to object to profiling for marketing purposes, and ensure this information is separate from any other information; and
- conduct a DPIA to decide if the outcome of automated profiling they do will have a legal or similarly significant effect on voters, as outlined in Article 22.

Relationships with social media companies when it involves targeting activities

Social media platforms process substantial amounts of personal data about their users' behaviour and interactions. Where a party has decided to use social media platforms to

target political messaging at individuals, it is important they understand that many different data sources are likely to be used for this purpose. The parties need to be very clear about what data they are using and why, both internally and with voters.

When parties look to use a platform's targeting tools, both the party and the platform itself should clearly identify the circumstances where joint controllership exists and put measures in place to fulfil those obligations. They must assess this on a case-by-case basis, irrespective of the content of any controller or processor arrangement. Joint controllership may exist in practice, if the platform exercises a significant degree of control over the tools and techniques they use to target individual users of their service with political messages on behalf of the party.

Article 26 of the GDPR specifies the requirements for joint controller situations. Parties should agree and fully understand who is responsible for what. This means they must work with any social media platform they use to make sure there are no gaps in compliance, and ensure they have appropriate contracts or agreements in place. They should also undertake in-life contract monitoring to ensure that the platforms are adhering to these contracts.

The data protection implications of this activity are complex and we recognise that the solutions to the issues below may take more time to resolve and will require more guidance for all the actors involved. Since our audits, we understand that some steps have been taken by social media companies within their revised terms and conditions of service for digital advertising.

The transparent use of social media for marketing and campaigning purposes

Social media was used by all parties to promote their work to people who may be interested in their values. The majority was delivered via Facebook – including their Instagram platform - and Twitter.

Where political parties were using audience choice tools, we had concerns with the lack of transparency of this practice. Privacy information did not make it clear that personal data of voters collected or processed by the party would then be profiled and used to target marketing to them via social media platforms. A key recommendation made following our audits was that parties must inform individuals and be transparent about this processing, so that voters fully understand their personal data will be used in this way to comply with Article 13(1)(e) of the GDPR. For example, parties should tell voters that their email addresses will be used to match them on social media for the purposes of showing them political messaging.

Due diligence should be undertaken before any campaign begins so that parties can assure themselves that the social media company has:

- appropriate privacy information and tools in place; and
- the data processing they will be doing on the party's behalf is lawful and transparent, and upholds the rights of individuals under data protection law.

Accountability

Accountability is one of the data protection requirements under the law. It makes organisations responsible for complying with data protection law and says that they must be able to demonstrate their compliance. Organisations must be proactive about data protection to evidence the steps they have taken to meet their obligations and protect people's rights.

There are several measures that political parties must improve on in this area, including:

- putting in place a framework of policies to document their approach to data protection compliance;
- implementing an effective training programme for all staff and volunteers across the party, which is supported by more specialised training for key roles;
- implementing detailed operational procedures which set out a clear process for conducting a DPIA, in line with Article 35 and 36 of the GDPR; and
- discussing data protection on a regular basis at appropriate meetings and sharing issues and risks with senior management to integrate data protection into business processes and promote a privacy by design culture.

Example

Many parties had only recently drafted data protection policies and procedures, which had not yet been fully communicated or embedded across the organisation. There was no formal requirement for staff, volunteers or members to sign to confirm that they had read and understood any key data protection policies.

Training needs analysis had not been undertaken for key roles to identify the requirement for specialised training for key information governance roles. Data protection responsibilities specific to the new role were sometimes covered in the informal role-based training delivered by the line manager in the first few weeks; however, there was a lack of formal data protection training delivered at induction which presents the risk that staff or volunteers may handle personal data without adequate training.

As part of demonstrating their accountability, it is important that the parties know and communicate what personal data they collect, store and process. This is important, not only because it is a legal requirement to document this, but also because it can support good data governance and help demonstrate compliance with other aspects of the GDPR.

Example

Some parties had completed data flows of how data travels between various databases and applications; however, they had not undertaken a comprehensive data mapping exercise nor recorded all their processing activities in line with the requirements of Article 30 of the GDPR. In some cases, they had done the data-mapping exercises prior to the advent of the GDPR and had not updated them since.

We recommended the following actions must be taken by the parties:

- undertake an information audit or data-mapping exercise to help find out what personal data they hold and where it is;
- conduct a review to find out why they are using personal data, who they share it with and how long it is kept, by distributing questionnaires to relevant areas, meeting directly with key business functions and reviewing policies, procedures, contracts and agreements; and
- document their findings in writing, in a detailed and meaningful way.

Next steps

Following the initial audit engagement, we asked all parties to provide a response to our recommendations. The responses showed that the parties were willing to take action to improve compliance on a voluntary basis. We needed to pause our work during the election in late 2019 and this, along with the impact of the COVID-19 pandemic, has delayed completion of this process and finalisation of this report.

It is our intention to follow up on these responses later this year to ensure progress has been made in key compliance risk areas. This work will consist of a review of updated action plans alongside supporting evidence and documentation to demonstrate the work each party has undertaken towards implementing each of the higher priority recommendations made. Should our follow-up reviews indicate parties have failed to take appropriate steps to comply, we reserve the right to take further regulatory action in line with our Regulatory Action Policy.

Through this work, the ICO has gained an improved understanding of:

- the political campaigning landscape;
- party structures and data protection governance arrangements; and
- the use of voter data to help inform our decision-making and approach to guidance.

The ICO expects to publish our guidance on political campaigning soon. The combination of all this work will assist us to evaluate data protection compliance of political parties in future elections.

In the wider ecosystem, the ICO also recognises that there are still other matters that need to be addressed about the use of personal data in the political context. These include some of the issues set out in the report it made to the Irish Data Protection Commission (IDPC), as the lead authority under GDPR, about targeted advertising on Facebook and other issuing including where the platform could be used in political contexts. The ICO will continue to liaise with the technology platforms to consider what, if any, further steps might be required to address the issues raised by our Democracy Disrupted report. This will be of relevance to the parties' use of social media platforms in future elections.