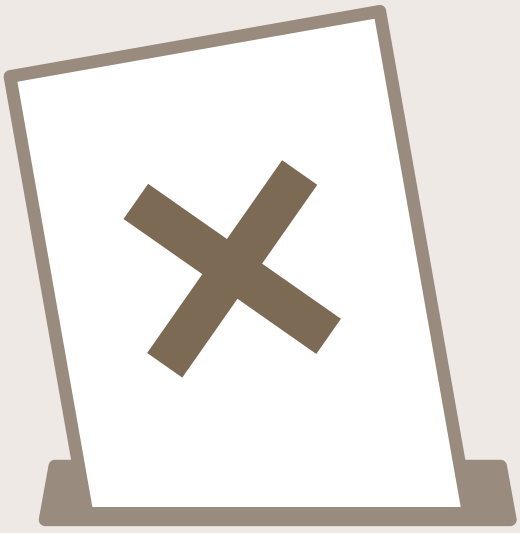
Guidance on political campaigning

Draft framework code for consultation



ico.
Information Commissioner's Office

Framework code of practice for the use of personal data in political campaigning

Contents

Commissioner's foreword

A foreword by Information Commissioner Elizabeth Denham will be included in the final version of the framework code.

About this framework code of practice

At a glance

- Being able to communicate with and engage voters, including using digital services, is an essential part of democratic life. It is equally important to retain the trust and confidence of voters in using their data and the integrity of elections.
- This framework code of practice (framework code) highlights the importance of processing personal data in compliance with data protection law during political campaigning.
- This framework code provides clarity and practical advice to help those processing personal data in political campaigning to comply with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulations 2003 (PECR).
- Those processing personal data for the purposes of political campaigning who don't comply with this framework code, are likely to find it difficult to demonstrate that their processing is fair and complies with the GDPR and PECR. Those not complying with the GDPR and PECR could face enforcement by the ICO including fines of up to £17m or 4% of global turnover.

In more detail

Introduction

It is vital in any democratic society that political parties and campaigners are able to communicate effectively with voters. But it is equally vital for the integrity of elections and democracy that all organisations involved in

political campaigning handle and process personal data in a way that is compliant with data protection law.

In recent years political campaigning has become increasingly sophisticated as new digital technologies and communication tools developed rapidly. Campaigners now use ever more innovative techniques to attempt to understand their potential voters and target them with political messaging.

Trust and confidence in the integrity of our democratic processes risks being disrupted because recent evidence[1] suggests that voters don't understand the invisible nature of these uses of personal data. However unintended, this poses a risk of hidden manipulation which undermines the democratic process. This must change. People can only make truly informed choices about who to vote for if they are sure their decisions have not been unfairly influenced.

The messaging and technologies used by political parties and campaigners may vary and change over time. But they all need to be working to the same rules when it comes to data protection and direct marketing laws, regardless of the method or future technological developments.

What is the purpose of this framework code?

This framework code provides clarity and practical advice to help those processing personal data in political campaigning to comply with the General Data Protection Regulation (EU) 2016/679 [2] (GDPR), the Data Protection Act 2018[3] (DPA) and the Privacy and Electronic Communications (EC Directive) Regulations[4] (PECR).

The ICO recommended the need for further guidance in its 2018 policy report, 'Democracy Disrupted'. This report was issued following our comprehensive investigation into the use of personal data for political purposes. We also recommended that this guidance should be supported as a statutory code of practice:

[1] ICO report: Democracy disrupted? Personal information and political influence
[2] Regulation (EU) 2016/679 of the European Parliament and of the Council
[3] Data Protection Act 2018
[4] Privacy and Electronic Communications (EC Directive) Regulations and subsequent amendments

"The Government should legislate at the earliest opportunity to introduce a statutory code of practice under the DPA2018 for the use of personal information in political campaigns. The ICO will work closely with Government to determine the scope of the code."

We decided to issue this framework code to provide clarity and support compliance with the law, whilst we continue to pursue this objective with Government.

Who is this framework code for?

This framework code is aimed at controllers (see section on controllership for further information) processing personal data for political campaigning purposes.

By political campaigning purposes we mean:

"activity in support of, or against, a political party, a referendum campaign or a candidate standing for election."

This includes, but is not limited to, processing by registered political parties, candidates, referendum campaigners, non-party campaigners and recall petition campaigners[5].

This framework code applies to you if you process personal data for political campaigning purposes, regardless of your status under electoral law.

It applies to you if you have a branch, office or other 'establishment' in the UK, and process personal data in the context of the activities of that establishment, whether or not you are based in the UK.

It may also apply to you even if you don't have an establishment in the UK and you are based outside the UK. The GDPR and the DPA still applies if you offer services to users in the UK, or monitor the behaviour of users in the UK, if your establishment is outside the European Economic Area (EEA).

Under the GDPR one-stop-shop arrangements, if you have a lead supervisory authority other than the ICO and you do not have a UK establishment, this framework code does not apply.

[5] as defined in Political Parties and Referendums Act 2000 sections 23, 88, 105

This framework code applies to processing for political campaigning in elections and referenda or potential elections and referenda in the UK. However, if you are processing for campaigning in non-UK elections and referenda and you are based in the UK, then the GDPR and DPA still applies and you may find this framework code helpful.

When does this framework code apply?

This framework code is not restricted to any 'regulated periods'. You can collect, process and handle personal data for political campaigning purposes before, during, after and between particular campaigns. This framework code applies for as long as you are processing personal data for political campaigning purposes.

What happens if we don't comply with this framework code?

Whilst this framework code is issued under the Commissioner's general powers, it does not have any special legal status beyond that. However, if you are processing personal data for the purposes of political campaigning and you don't comply with this framework code, you are likely to find it difficult to demonstrate that your processing is fair and complies with the GDPR and PECR. If you process personal data in breach of the GDPR or PECR, we can take action against you.

Tools at our disposal include assessment notices, warnings, reprimands, enforcement notices and penalty notices (administrative fines). For serious breaches of the data protection principles, we have the power to issue fines of up to £17 million or 4% of your annual worldwide turnover, whichever is higher.

How should we use this framework code?

This framework code assumes you are familiar with key terms and concepts in the GDPR, DPA and PECR. If you need an introduction to data protection – or more context and guidance on key concepts – you should refer to our separate Guide to Data Protection and Guide to the Privacy and Electronic Communications Regulations.

It focuses on specific compliance and good practice points for using personal data in political campaigning. It is divided into several sections, designed loosely to follow the lifecycle of a political campaign.

This framework code is not intended as an exhaustive guide to compliance. It only covers processing for political campaigning purposes; it does not cover your wider obligations such as processing employment

data or carrying out wider administrative tasks. Similarly, it does not elaborate on all your data protection obligations for political campaigning. For example, it does not cover accuracy, security, breach reporting or the right of access. Such obligations are equally as important as those explained in this framework code. However, the ways in which they apply are broadly the same whether you are processing for political campaigning purposes or any other purpose so we have not included them.

You need to ensure you are aware of all of your obligations, and you should read this framework code alongside our other guidance.

Further reading

For an introduction to data protection law and guidance on key concepts see our Guide to Data Protection.

For an introduction to electronic marketing laws see our Guide to Privacy and Electronic Communications Regulations.

What are our obligations?

At a glance

As well as electoral law, if you are involved in processing personal data for political campaigning you have to comply with the GDPR, DPA and PECR.

In more detail

Introduction

Organisations and candidates campaign using a variety of methods to engage with voters. Where this campaigning involves processing of personal data you must carry it out in compliance with the data protection law.

PECR complements the GDPR and DPA and provides additional rules for direct marketing by electronic means, such as phone, text message, and electronic mail. Direct marketing is defined in the DPA, section 122, Paragraph 5 as 'the communication (by whatever means) of advertising or marketing material which is directed to particular individuals'. This includes contacting an individual to promote a political view or otherwise influence an individual.

This framework code provides practical advice and good practice recommendations to aid compliance with the GDPR, DPA and PECR. In order to do this, the framework code refers to other legislation including electoral law. However, you should direct requests for guidance and questions on compliance with electoral law to the Electoral Commission.

What are the data protection principles and rights?

The GDPR sets out the key principles, rights and obligations for most processing of personal data.

The DPA supplements and tailors the GDPR, for example in specifying how lawful bases may apply or in providing further conditions for processing certain types of sensitive information.

The key principles set out by the GDPR are:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

The GDPR also provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

This framework code does not discuss each of these principles and rights in detail but highlights the most relevant considerations for processing for political campaigning purposes.

Further reading

For general guidance on key data protection concepts see our Guide to Data Protection.

For general guidance on electronic marketing laws see our Guide to Privacy and Electronic Communications Regulations.

Who is the controller?

At a glance

- Understanding whether you are a controller, joint controller or processor for the personal data you are processing is key to ensuring you are complying with data protection law.
- Controllers determine the purposes and means by which personal data is processed. Processors handle personal data on behalf of controllers. Whilst controllers have most responsibility for compliance with data protection law, processors have their own obligations as well. The ICO has the power to take action against both.
- Political parties and campaign groups are structured in different ways and may have complex set ups and constitutional and contractual arrangements. This may include national and local organisations. Also, elected representatives are often controllers in their own right.
- You should take the time to assess and document what personal data you hold; the processing activities you carry out with each organisation you work with; and what responsibilities you each have.

In more detail

Introduction

Understanding your responsibilities for the personal data you are processing is essential in ensuring compliance with data protection law.

Your obligations under the GDPR will vary depending on whether you are a controller, joint controller or processor.

What is the difference between a controller, joint controller or processor?

Controllers are the main decision-makers – they exercise overall control over the purposes and means of the processing of personal data.

If two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are **joint controllers**. However, they are not joint controllers if they are processing the same data for different purposes.

Controllers shoulder the highest level of compliance responsibility – they must comply with, and demonstrate compliance with, all the data protection principles as well as the other GDPR requirements. They are also responsible for the compliance of their processor(s). This framework code is primarily for controllers.

Processors act on behalf of, and only on the instructions of, the relevant controller.

Processors do not have the same level of compliance responsibility as controllers. But they do carry responsibility for some compliance such as security, data breach notification and accountability in their own right. See our guidance on controllers and processors and contracts and liabilities for further information[6].

The ICO has the power to take action against both controllers and processors, and individuals can bring claims against both.

How does controllership apply in political campaigning?

In political campaigning there can be many different controllership arrangements depending on the situation.

Political parties are set up in different ways with different legal entities. The controller might be central office, a local association, a candidate or a campaigner, or any combination of these acting as joint controllers. Therefore, the data held at any one time by a political party might be under the responsibility of different controllers.

[6] ICO guidance on Controllers and Processors.

Similarly, campaign groups may also have complex setups and contractual arrangements.

Under electoral law, registered political parties and other registered campaigners (see section on use of the electoral register) are permitted access to personal data held on the full electoral register for campaigning purposes. Regardless of any other setup arrangements, for data obtained from the electoral register, candidates and political parties are considered separate controllers. This does not mean you are unable to work as joint controllers if appropriate, but it is important to be clear that they are treated as distinct from each other under data protection law.

In addition, elected representatives are also separate controllers for work they carry out for the purpose of being an elected representative such as constituency case work. This means that you should not share data between elected representatives' offices and your local or national parties unless there is a clear lawful basis for doing so and the sharing is in compliance with the data protection principles.

Most political parties, campaign groups and candidates are controllers. But many also contract processors to process personal data on their behalf. Examples of controller - processor and joint controllers – processor relationships are below.

Example
An independent candidate in a local election holds a list of potential supporters' names and addresses. She decides to write to these supporters to encourage them to turnout to vote on polling day. She contracts a company to write, add the names and addresses and distribute the letters. Therefore, the candidate is the controller as she decides the purpose and means of processing the personal data. The company she contracts is the processor as it is acting on the instructions of the controller.

How do we determine whether an organisation is a controller or processor?

The examples above are fairly straightforward but often establishing whether you are acting as a processor or a controller in your own right can be more complicated. Examples include working with third party data

analytics, modelling, market research and marketing companies as well as online platforms.

The key is to determine your degree of independence in determining how and in what manner the data is processed as well as the degree of control you have over it. You may sometimes want to seek specific legal advice about this aspect of compliance.

In certain circumstances, and where included in the contract, a processor may have the freedom to use its technical knowledge to decide how to carry out certain activities on the controller's behalf. However, it cannot take any of the overarching decisions, such as what types of personal data to collect or what the personal data will be used for. These decisions must only be taken by the controller. As such many relationships where a controller has contracted out a service to a third party organisation will actually be joint controller relationships.

Example
A candidate representing a political party in a local election jointly holds a list of potential supporters' names and addresses with the local party association. The particular setup of the party means that the local party association is a separate legal entity to the party's central office. The candidate and the local party decide together to write to these potential supporters to encourage them to turnout to vote on polling day. They contract a company to write, add names and addresses and distribute the letters. Therefore, the candidate and the local party association are joint controllers as they jointly decide the purpose and means of processing the personal data. The company they contract is the processor as it is acting on the instructions of the joint controllers.

Example

A political party contracts a research company to carry out research for voter modelling purposes. The political party specifies its budget and that it wants to understand the characteristics of voters in particular geographical areas that are likely to vote for them. The party leaves it to the research company to determine sample sizes, survey methods and presentation of results.

The research company is processing personal data on the party's behalf, but it is also determining what information they are collecting and how they are carrying out the processing (the survey). It has the freedom to decide such matters as which people to select for the survey, what form the survey should take, what information to collect and how to present the results. This means the research company is a joint controller with the party regarding the processing of personal data to carry out the survey, even though the party retains overall control of the data because it commissions the research and determines the purpose the data will be used for.

How do we identify controllership relationships in practice?

It is essential for compliance with the GDPR that you are clear who the controller is for what data and in what circumstances. There are many ways you can identify this but it is often helpful to map the flow of personal data – labelling which organisations are responsible.

It is then important to establish the types of controller relationship by fully considering how far each of you is determining how and in what manner you are processing the personal data. If you establish that there is more than one controller then you should further establish whether you are both processing personal data for the same purpose. You can consider these points as either a standalone exercise or as part of a data protection impact assessment (DPIA). See our section on DPIAs for more information.

What is required in each relationship?

Once you have established controller and/or processor relationships, both of you must ensure you fully understand your respective responsibilities under data protection law. You must also take into account the particular

circumstances and requirements that each type of relationship requires. See our guidance on controllers and processors and contracts and liabilities for further information on these requirements[7].

Regardless of where legal responsibility lies, with political campaigning in particular, you should also bear in mind that the media and general public are likely to be unaware of the complexities of controller relationships. You should consider how individuals are likely to contact you in order to exercise their GDPR rights. You should ensure you have effective processes in place for dealing with these.

Are we required to pay the data protection fee?

The Data Protection (Charges and Information) Regulations 2018 requires every controller who processes personal data to pay a data protection fee to the ICO, unless they are exempt.

Members of the House of Lords, elected representatives and prospective representatives are exempt from this requirement. However, in most circumstances political parties, campaign groups and other controllers need to pay the fee. See the ICO website for further information on this.

Further reading

For guidance on Data Protection Impact Assessments see our guidance section DPIAs.

For general guidance on key data protection concepts see our Guide to Data Protection.

[7] ICO guidance on Controllers and Processors.

Personal data

At a glance

- The GDPR only applies to 'personal data' so it is important to know what information you hold and whether it can be classed as personal data.
- Article 4(1) defines personal data as information that relates to an identified or identifiable individual. This is more than identifying individuals. It must concern them in some way.
- It is important to note that opinions and inferences will also be personal data, maybe special category data, if they directly or indirectly relate to that individual.

In more detail

Introduction

It is important to be clear what personal data you hold and whether the GDPR applies to this data.

The GDPR applies to the processing of personal data that is:

- wholly or partly by **automated means**; or
- the processing, other than by automated means, of personal data which forms part of, or is intended to form part of, a **filing system**.

In other words, it applies to personal data processed, or partly processed, by computer as well as any personal data that is placed, or you intend to place, in a manual filing system. In practice, most personal data that you process will be caught by this definition.

What is personal data?

The GDPR Article 4(1) defines personal data as:

> "any information **relating to** an **identified or identifiable natural person** ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"

In other words, if you can identify a particular individual from the information, or when put together with other information you hold, then this is personal data.

In most cases it is straightforward to establish whether you can identify an individual. The GDPR provides a non-exhaustive list of identifiers, including:

- name;
- identification number;
- location data; and
- online identifier (including IP addresses and cookie identifiers).

However, there are many other possible identifiers. In the context of political campaigning, examples include but are not limited to:

- names, addresses and electoral registration numbers on both the electoral register and the marked electoral register;
- membership names, numbers, subscription and financial details;
- dates of birth and ages (both inferred or known);
- attributes, opinions and characteristics (both inferred or known);
- propensity to vote scores; and
- communication preferences, eg by email, text, post or phone.

What is the meaning of 'relates to'?

Information must **'relate to'** the identifiable individual to be personal data.

This means that it does more than simply identifying them – it must concern the individual in some way.

To decide whether or not data relates to an individual, you may need to consider the:

- content of the data – is it directly about the individual or their activities?;
- purpose you are processing the data for; and
- results of, or effects on, the individual from processing the data.

There will be circumstances where it may be difficult to determine whether data relates to an individual. If this is the case, you should treat the information with care, ensure that you have a clear reason for processing the data and, in particular, ensure you hold and dispose of it securely.

Can opinions or inferences about people be personal data?

The definition of personal data is not restricted to factual information about an individual. Opinions and inferences are also personal data if the individual can be identified from that data, either directly or indirectly, and the information relates to that individual.

For example, if you are attaching inferences or opinions to individuals' names or addresses then this information is very likely to be considered personal data, regardless of how certain you are that these inferences or opinions are correct.

Example

A political party makes inferences about the likely characteristics of people living in a particular polling district. The party combines this information with the names and addresses of individuals on the electoral register. They categorise individuals and give them a percentage score indicating likeliness to support the party.

This information relates to identifiable individuals as the inferred characteristics, categories and scores are appended to individuals' names and addresses, so it is personal data.

Example

A political party makes inferences about the likely characteristics of people living in particular polling districts. The party is given the information for districts as a whole. It makes no attempt to attach this information to individual names or addresses. It categorises the districts and gives percentage scores indicating the likely support in each area for the party.

This information does not relate to identifiable individuals as the inferred characteristics, categories and scores are appended to broad areas, so it is not personal data.

As the above examples demonstrate, to establish whether opinions or inferences are personal data, it is not about whether the inferences or opinions are correct. The key question is whether they are processed with the intention to identify and relate to, or in a manner that identifies and relates to, individuals; whether by name, address or any other identifying factor.

Recommendations

1. If you make inferences about people living in a particular area, you should do this in a way that avoids processing personal data where possible. For example, using as large as possible a mapping area to cover more properties or households; and using formats, such as heat maps. These ways provide an overview without processing personal data that allows the inference of detailed information about a particular place or person. However, even if you are not processing personal data, you should assess the risks of processing such information, especially if it could be particularly sensitive, such as inferred ethnicity or religious beliefs.

2. You should be very careful when developing or purchasing software that makes inferences about people in an aggregated form. You should assess carefully whether this software processes personal data or adds special category data. If it does, you need to assess the necessity of processing this personal data and fully comply with data protection law.

Further reading
The General Data Protection Regulation is published here.

For general guidance on key data protection concepts see our Guide to Data Protection.

Accountability

At a glance

- Accountability is one of the most important data protection principles. It is not a one-off exercise. It means taking responsibility for complying and demonstrating compliance with the GDPR.
- Being accountable can help you to build and retain trust with voters and may help you mitigate enforcement action from the ICO.
- There are a number of ways to demonstrate accountability including embedding 'data protection by design principles' from the outset of a product or service and implementing Data Protection Impact Assessments (DPIA).

In more detail

Introduction

One of the most significant principles of the GDPR is accountability.

There are two key elements to this. First, the accountability principle makes it clear that you are responsible for complying with the GDPR. Second, you must be able to demonstrate your compliance.

Taking responsibility for what you do with personal data, and demonstrating the steps you have taken to protect people's rights, not only results in better legal compliance but is a real opportunity for you to show, and prove, how you respect people's privacy. This can help you to develop and sustain people's trust and confidence, in turn helping to underline the legitimacy of your political messages.

Furthermore, if something does go wrong, then being able to show that you actively considered the risks and put in place measures and safeguards can help you provide mitigation against any potential

enforcement action. On the other hand, if you can't show good data protection practices, it may leave you open to fines and reputational damage.

What does accountability mean in practice?

Accountability is not a box-ticking or one off exercise. Being responsible for compliance with the GDPR means that you need to be proactive and organised about your approach to data protection, while demonstrating your compliance means that you must be able to evidence the steps you take to comply. To be effective you must sustain this over time and embed and maintain a data protection management programme. It also requires leadership from the top of your organisation.

You need to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individuals' rights. This means you must consider data protection and privacy issues upfront in everything that you do. You should also report regularly at Board level and assess the effectiveness of your accountability programme.

There are a number of measures that you can, and in some cases must, take to comply with the accountability principle, including:

- adopt and implement data protection policies;
- put written contracts in place with contractors and data processors;
- maintain documentation of your processing activities;
- employ a data protection officer;
- train your staff and volunteers; and
- implement appropriate security measures.

See our Guide to GDPR for further information on these.

Some measures of particular importance to processing for political campaigning purposes are discussed in more detail below.

What is data protection by design and default?

Data protection by design and default is an integral element of being accountable. It is about embedding data protection into everything you do, throughout all your processing operations.

You must put in place appropriate technical and organisational measures designed to implement the data protection principles and safeguard individual rights.

There is no 'one size fits all' method to do this, and no one set of measures that you should put in place. However, there are some key times when it is particularly important to consider this obligation, including when you are:

- implementing a new campaigning contact or membership database;
- starting a new significant campaign;
- changing methods - for example changing from canvassing by paper to mobile applications;
- considering collecting or procuring new data sources and types of data; or
- considering the use of new advertising platforms.

The key is that you consider data protection issues from the start of any processing activity, and adopt appropriate policies and measures that meet the requirements of data protection by design and by default.

Example

Consider the differing approaches below.

Mr Matthews and Ms Ali both decide to campaign in their local town. Ms Ali is concerned that there aren't enough car parking spaces in the town centre whereas Mr Matthews wants to see the number of car parking spaces reduced to encourage workers in the area to use public transport.

Both decide to send petitions to their local council. They collect names and addresses of individuals for this purpose. They both know they need to comply with the GDPR.

Mr Matthews decides to focus on the effectiveness of his campaign messages first and consider how he complies with GDPR as he goes along.

Ms Ali decides to take a 'data protection by design and by default' approach and fully considers the data protection principles, thinking

carefully about her purposes and what individuals would reasonably expect.

A few months later, boosted by the popularity of their respective campaigns both Ms Ali and Mr Matthews decide to stand as independent candidates in their local election. They both want to send letters to the individuals who signed their petitions to encourage them to turn out and vote for them.

Mr Matthews finds that doing this would likely breach data protection law. The privacy information he provided on collection was inappropriate and his specified retention period has expired. He does not send the letters.

Ms Ali's privacy by design and default approach means that she had considered the principles and data protection risks from the outset. She provided appropriate privacy information, specified her purposes included direct marketing and communicated an appropriate retention period based on what was necessary for her purposes. She decides to send the letters.

What are data protection impact assessments?

Carrying out Data Protection Impact Assessments (DPIAs) is another important way to comply with the accountability principle.

A DPIA helps you to systematically and comprehensively analyse your processing and identify and minimise data protection risks.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – to individuals or to society at large, whether it is physical, material or non-material. This is an important factor to consider in political campaigning.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals.

When must we carry out DPIAs?

DPIAs are a legal requirement for processing that is likely to be high risk. This means you need to assess your risk to some extent prior to carrying out a full DPIA.

There are various circumstances where you must carry out a DPIA. Those of most relevance to processing for political campaigning purposes include:

- using systematic and extensive profiling with significant effects (see section on restricted profiling);
- processing special category data on a large scale (see special category data section);
- using innovative technology (in combination with any of the criteria from the European guidelines - see further reading section below);
- using profiling or special category data to decide on access to services;
- profiling individuals on a large scale;
- matching data or combine datasets from different sources;
- collecting personal data from a source other than the individual without providing them with a privacy notice ('invisible processing'); or
- tracking individuals' location or behaviour.

Many political parties and campaign groups are required to carry out DPIAs for various aspects of their campaigning.

Recommendation

You should consider carrying out a DPIA even when you are not required by law. An effective DPIA can bring broader compliance, financial and reputational benefits, helping you demonstrate accountability and building trust and engagement with individuals.

Further reading

The European Commission Guidelines on Data Protection Impact Assessment (DPIA) are available here.

For advice and guidance on carrying out DPIAs see our guidance.

For general guidance on key data protection concepts see our Guide to Data Protection.

Purpose limitation, data minimisation and storage limitation

At a glance

- You may want to use personal data obtained for one purpose in a political campaign, for a different purpose. You must be clear about why you're processing the data from the start, be able to evidence it and specify it in your privacy information to individuals.
- You must ensure the personal data is adequate, relevant and limited to what is necessary for the purposes for which you are processing it.
- You must not keep personal data for longer than you need it. You need to justify why and how long you are holding personal data - and that is linked to the purposes.

In more detail

Can we use personal data collected for another purpose for political campaigning purposes?

Often political campaigners seek to use personal data obtained through petitions, surveys, casework, enquiries and other sources, for more general political campaigning purposes.

If you are using this data, it is first important to ensure that you have provided individuals with appropriate privacy information on collection (see section on collecting personal information).

It is equally important to comply with the 'purpose limitation' principle – GDPR Article 5(1)(b).

Article 5(1)(b) states:

> "1. Personal data shall be:
>
> …(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes…"

In practice this means you must:

- be clear from the outset why you are collecting personal data and what you intend to do with it;
- specify and document your purposes;
- comply with your transparency obligations to inform individuals about your purposes; and
- only use this information for political campaigning purposes in two circumstances: where the purpose of political campaigning is compatible with the original purpose; or where you have obtained the individual's specific consent for processing data.

The GDPR says that to decide whether a new purpose is compatible (or as the GDPR says, "not incompatible") with your original purpose you should take into account:

- any link between your original purpose and the new purpose;
- the context in which you originally collected the personal data – in particular, your relationship with the individual and what they would reasonably expect;
- the nature of the personal data – eg is it particularly sensitive;
- the possible consequences for individuals of the new processing; and
- whether there are appropriate safeguards - eg encryption or pseudonymisation. See our Guide to GDPR for further information on these safeguards.

Example

A local political party association conducts a survey of residents in a nearby village to understand more about their views on public transport availability in their local area. They collect names, addresses, and individuals' concerns about public transport to contact them to update them on the party's campaign to improve it.

At the next general election, the local political party association supports the national campaign and the campaign to elect their party's candidate for MP. Following data analytics on modelled data, the party's national headquarters tells the local association that it has found that people who care about public transport are more likely to support the party's national leader. The political party uses the data it obtained from the survey to find those who believe there needs to be better public transport provision and targets them with campaigning leaflets.

This is unlikely to be a compatible purpose. The link between the original and new purpose for the processing is tenuous and is unlikely to be within individuals' reasonable expectations that their data is processed for this new purpose. The party is therefore unable to use this data unless they take further steps to comply, as required by GDPR.

Can we use personal data obtained from constituency casework in political campaigns?

In general, you should not use personal data you obtained when carrying out constituency or similar casework for political campaigning purposes. The exception is if you are sure that those constituents would expect you to contact them for political campaigning purposes and would not object. If you believe this is the case, you should document your reasoning and any evidence. If in any doubt, however, you should be cautious and not use the information.

Example

An MP receives a number of letters from constituents raising concerns about their rights as leaseholders. The MP has corresponded with his constituents about the issue so he can raise their concerns with the Minister responsible and in Parliamentary debate. A general election takes place a couple of months later. The MP decides to use the constituents' contact details to send campaigning leaflets tailored to these constituents. The leaflet outlines his commitment to leasehold reform and encourages the constituents to vote for him at the upcoming election.

In this example, although the issue being discussed is broadly the same, the purpose for processing the personal information has changed from representing constituents to political campaigning. It is unlikely that the constituents will expect their MP to use their personal data for this new purpose.

It is worth highlighting that the rules around making automated calls, some live calls and sending electronic communications for political campaigning purposes are different. See the section on PECR. In addition to ensuring that constituents expect this contact, you also need their specific consent before using these communication methods to send them marketing material including campaigning messages. See direct marketing methods section for more information.

How much personal data can we process for political campaigning purposes?

Article 5(1)(c) says:

"1. Personal data shall be:

…(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)"

This means you should identify the minimum amount of personal data you need to fulfil your purpose. You should process that information, but no more.

The GDPR does not define what 'adequate', 'relevant' and 'limited to what is necessary' mean. Instead it depends on your purpose and may differ from one individual to another.

To assess whether you are holding the right amount of personal data, you must first be clear about why you need it. You must not collect or retain personal data on the off-chance that it might be useful in the future. You must be able to justify the necessity of processing the data for your purpose(s). This is particularly important for special category data (see the section on special category data for more information) where there is a greater risk of harm in processing this data, particularly in the event of a personal data breach.

The amount of data you hold may also differ from one individual or one group of individuals to another. For example, you are very likely to need to process more personal data for members of a party or campaign group than for members of the public.

In addition you should consider any specific factors that an individual brings to your attention. For example, as part of an objection, request for rectification of incomplete data, or request for erasure of unnecessary data.

You should periodically review your processing to check that the personal data you hold is still relevant and adequate for your purposes, and delete anything you no longer need. This is closely linked with the storage limitation principle.

How long should we keep personal data for political campaigning purposes?

Article 5(1)(e) says:

> "1. Personal data shall be:
>
> …(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed…"

This is known as the storage limitation principle. It does not specify how long you should keep personal data for political campaigning purposes – this is for you to determine as the controller. However it does say that you must not keep personal data for longer than you need it.

Therefore how long you keep personal data for political campaigning purposes depends on how long you need the data for this purpose. The onus is on you to properly consider why you need to retain personal data and be able to justify why it is necessary for your purpose to keep it.

In order to comply with the accountability principle you need a policy that sets your retention periods. Likewise one of the requirements of the right to be informed is that you state the period you store the personal data for or the criteria you use to determine the period.

If you no longer need the personal data for your purposes, you should erase (delete) it or anonymise it (ie so it is no longer in a form that allows the individual to be identified). You should also keep a log of what you have deleted and when for good records management.

It is important to regularly review the personal data that you hold for political campaigning purposes in order to reduce the risk that it has become irrelevant, excessive or inaccurate.

Example

A political party has stood candidates for MP in a London constituency for decades. The party appoints a new data protection officer - she decides to review the personal data held on a local party office system. As part of her search she sees a spreadsheet called '1998 Greater London Authority referendum'. The spreadsheet contains the names of local residents and their likely voting intentions in the referendum.

The data protection officer is very surprised. She asks a local party representative the reasons for keeping this spreadsheet for so long. He explains that he is keeping it just in case there is ever another referendum on the issue. The data protection officer deletes the spreadsheet.

The data protection officer is right to delete the spreadsheet. Although there may be another referendum in the future, this is not appropriate justification for keeping the data. There are also likely to be data minimisation, purpose limitation, accuracy, fairness and transparency issues with continuing to hold it.

Further reading

For general guidance on PECR see our Guide to Privacy and Electronic Communications Regulations.

For general guidance on key data protection concepts see our Guide to Data Protection.

The General Data Protection Regulation is published here.

Lawful, fair and transparent processing

At a glance

- GDPR Article 5(1)(a) is concerned with lawfulness, fairness and transparency.
- Lawful processing means you must have an appropriate lawful basis (or bases if more than one purpose) for processing personal data and you must also process it lawfully in a more general sense.
- Fairness means handling personal data in a way individuals expect and not using it in ways that lead to unjustified adverse effects. You must consider the fairness of your processing.
- In order to process personal data in a transparent manner you must be clear, open and honest to individuals and comply with the transparency obligation of the right to be informed.

In more detail

Introduction

The first data protection principle, listed in Article 5(1)(a) of the GDPR says:

> "1. Personal data shall be:
>
> (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness, transparency')"

This is the cornerstone of data protection law. The three elements of lawfulness, fairness and transparency overlap, but you must make sure you satisfy all three. For example, it's not enough to show your processing is lawful, if it is fundamentally unfair to or hidden from the individuals concerned.

What does lawfulness mean?

There are two key aspects to lawful processing.

Firstly, you must have an appropriate lawful basis for processing personal data for your particular purpose(s). The lawful bases of most relevance for processing in political campaigning are covered in detail in the section on lawful bases.

Secondly, lawfulness means that you don't do anything with the personal data which is unlawful in a more general sense. This includes statute and common law obligations, whether criminal or civil. If processing involves committing a criminal offence, it is obviously unlawful. However, processing may also be unlawful if it results in other breaches such as duty of confidence, contractual agreements or the Human Rights Act 1998.

As well as the Privacy and Electronic Communications Regulations, electoral law is of great relevance to political campaigning. This interacts with data protection law in many areas, particularly around the use of electoral register data.

You must ensure you fully comply with other laws. If you don't, then you could risk breaching GDPR as well as committing an offence or civil breach in another area.

What does fairness mean?

In general, fairness means that you should only handle personal data in ways that people reasonably expect and not use it in ways that have unjustified adverse effects on them.

Assessing whether you are processing data fairly depends partly on how you obtain it. In particular, if anyone is deceived or misled when you obtained the personal data, then this is unlikely to be fair.

Similarly, the way in which you use personal data is also important. The purpose of political campaigning is by nature to influence individuals' opinions and persuade them to vote in particular ways. Processing personal data for this purpose and in particular using it to profile and micro target individuals with political messaging, can raise ethical questions both for individuals and for society at large. You should feed these ethical questions about personal data use into any assessment you make of fairness.

Because of the competitive nature of political campaigning sometimes campaigners are quick to utilise innovative methods to engage with voters, without necessarily thinking of the underlying fairness of doing so. Examples include new data analytics and micro-targeting methods, as well as innovative automated calling systems. You must carefully consider how fair it is to use the methods you are using. In other words, in order to process personal data fairly, you need to stop and think not just about how you **can** use personal data, but also about whether you **should**. This should link to your data protection impact assessment.

What does transparency mean?

Linked to fairness is transparency. Transparent processing is about being clear, open and honest with people from the start about who you are and how and why you use their personal data.

This is of fundamental importance when using personal data in political campaigning. Often you have no direct relationship with individuals. You collect your data from the electoral register and other sources. In many cases, individuals may have no idea that you are collecting and using their personal data and this affects their ability to assert their rights over it. This is sometimes known as 'invisible processing'.

People need to have confidence in the democratic process and a part of that is trusting that you are not using their personal data to influence their voting behaviour in ways they don't expect.

You must ensure you are transparent throughout your processing, such as when responding to right of access requests or in carrying out DPIAs. The most significant aspect to this is the right to be informed. This is discussed in more detail in the section on collecting personal data.

Further reading

For general guidance on key data protection concepts see our Guide to Data Protection.

The General Data Protection Regulation is published here.

Lawful bases

At a glance

- You must have a lawful basis for processing personal data. The applicable lawful basis depends on your specific purposes, your powers and the context of the processing.
- The vast majority of processing for political campaigning purposes falls under three lawful bases: public task (democratic engagement); consent; and legitimate interests. You must evidence your reasoning for choosing a lawful basis.

In more detail

Introduction

In order to process any personal data for any purpose, you must have a lawful basis. GDPR Article 6 outlines six lawful bases with further expansion of what these include in DPA Section 8. Which lawful basis applies depends on your specific purposes, your powers and the context of the processing. You should think about why you want to process the data, and consider which lawful basis best fits the circumstances.

Once you have decided which lawful basis applies to each of your purposes, you need to keep a record of which basis you are relying on for each processing purpose, and a justification for why you believe it applies. There is no standard form for this, as long as you ensure that what you record is sufficient to demonstrate that a lawful basis applies. This helps you comply with accountability obligations, and also when writing your privacy notices.

The vast majority of processing for political campaigning purposes will fall under one of the following three lawful bases:

- Public task – democratic engagement
- Consent
- Legitimate interests

Can we use 'public task – democratic engagement' as our lawful basis?

This lawful basis is often misunderstood as an overarching exemption, so it is important that you understand the purpose of the provision.

GDPR Article 6(1)(e) gives a lawful basis for processing personal data (only and to the extent that it is) necessary for the performance of a task carried out in the public interest.

DPA Section 8 further specifies that this includes processing of personal data that is:

> "**necessary** for … (e) an activity that supports or promotes **democratic engagement**."

In addition, GDPR Article 6(3) requires that this task must be laid down by domestic or EU law (in addition to the DPA).

What additional law could satisfy Article 6(3)?

For the processing of personal data sourced from the electoral register, most campaigners will be able to rely upon electoral law[8].

Some campaigners, such as MPs or other elected officials, may also be able to rely on other laws to process additional 'non electoral register' data. Such laws do not have to be explicit statutory provisions, as long as the application of the law is clear and foreseeable. This means that it includes clear common law tasks, functions or powers as well as those set out in statute or statutory guidance. You should obtain specific legal

[8] Representation of the People (England and Wales) Regulations 2001 (SI 2001/341) regulations 103-106 and Schedule 3 of the Representation of the People (England and Wales) (Description of Electoral Registers and Amendment) Regulations 2013 (2013/3198) and equivalent devolved legislation.

advice if you are unsure what particular laws may apply to your role/organisation to satisfy Article 6(3).

Other campaigners may not have an additional law available to them to allow them to process 'non- electoral register' data. In this situation, if the processing is necessary for an activity that supports or promotes democratic engagement you will most likely be able to rely on 'legitimate interests' (see below section).

What does 'necessary' mean?

In order to rely on this lawful basis, processing personal data must be **necessary** for an activity that supports or promotes democratic engagement. This does not mean that processing has to be absolutely essential. However, it must be more than just useful or standard practice. It must be a targeted and proportionate way of achieving your specific purpose. This basis does not apply if you can reasonably achieve your purpose by some other less privacy intrusive means, or by processing less personal data.

Example

A candidate in an upcoming local election would like to contact people who live on a particular housing development to promote their campaign commitment to build a new playground. Rather than canvassing door-to-door in person, or posting leaflets, he decides to use electoral register data to inform which residents he ought to speak to.

Processing personal data in this way is unlikely to be necessary for this purpose, as the candidate could have feasibly achieved this by not processing any personal data in the first place, ie by leafleting door-to-door. If there wasn't a reasonable alternative mechanism available then the processing could be considered necessary for the purpose.

What activities support or promote 'democratic engagement'?

The Explanatory Notes accompanying the Data Protection Act 2018 explain:

"The term "democratic engagement" is intended to cover a wide range of political activities inside and outside election periods, including but not limited to:

- democratic representation;
- communicating with electors and interested parties;
- surveying and opinion gathering;
- campaigning activities;
- activities to increase voter turnout;
- supporting the work of elected representatives, prospective candidates and official candidates; and
- fundraising to support any of these activities."

Therefore, this lawful basis is designed to apply in the context of many political activities where the processing is supported by additional law (such as electoral law).

When can we use legitimate interests as our lawful basis?

If the public task - democratic engagement lawful basis is not appropriate for your purposes (ie if there is no appropriate law you can rely upon to satisfy Article 6(3)), then you will most likely be able to rely on 'legitimate interests' for the processing of personal data that supports or promotes democratic engagement.

You may also be able to rely on 'legitimate interests' where you are processing personal data for activities which do not support or promote democratic engagement but where you have another compelling justification for the processing.

Whether processing in support of democratic engagement or not, in order to rely on the 'legitimate interests' lawful basis, you will need to carry out and document the results of a three-part assessment. You need to:

- identify a legitimate interest (either your own or a third party's - eg democratic engagement);
- show that the processing is necessary to achieve it (as with public task- democratic engagement); and
- balance it against the individual's interests, rights and freedoms. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests.

Example

A charity providing general advice and support to older people, having made clear they would do this in their privacy notice, decides to write to their customers encouraging them to vote in an upcoming election. They provide information about how to obtain a postal vote. In this example, the charity is likely to be able to rely on the 'legitimate interests' lawful basis for the processing. They carry out a 'legitimate interests test'. They identify their 'legitimate interest' as 'democratic engagement', they provide justification to show that the processing is necessary and they balance their 'democratic engagement' interest against the individual's interests, rights and freedoms - finding that the processing is within their customers' reasonable expectations and unlikely to cause unjustified harm.

When can we use consent as our lawful basis?

The lawful basis of consent is in Article 6(1)(a).

Consent is an appropriate basis if you can offer people real choice and control over how you use their data, and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you still process the personal data without consent, asking for consent is misleading and inherently unfair.

It is important to note that consent:

- should be obvious and require a positive action to opt in;
- must be obtained through prominent requests, unbundled from other terms and conditions, concise and easy to understand, and user-friendly;
- must specifically cover the controller's name, the purposes of the processing and the types of processing activity;
- must be recorded. You must keep records to evidence consent – who consented, when, how, and what they were told;
- can be withdrawn. People have a specific right to withdraw consent. You need to tell people about their right to withdraw, and offer

them easy ways to withdraw consent at any time; and

- has no set time limit. How long it lasts will depend on the context. You should review and refresh consent as appropriate.

If you are processing personal data in order to send individuals direct marketing by electronic means (ie emails, texts, direct messages, automated calls and live calls) then PECR may require you to have consent. PECR takes its definition of consent from the GDPR. If PECR requires consent then processing personal data for electronic direct marketing purposes is unlawful under the GDPR without consent. If you have obtained consent in compliance with PECR, then in practice consent is also the appropriate lawful basis under the GDPR.

Further reading

For further information see our Guide to GDPR, our interactive lawful basis guidance tool and detailed guidance on consent and legitimate interests.

Special category data

At a glance

- There are various types of particularly sensitive personal data known as special category data. This includes political opinions.
- In order to process special category data, you need to identify a lawful basis under Article 6 and a separate condition under Article 9 of the GDPR. The DPA introduces additional conditions and safeguards.
- **In most circumstances, you should not use special category data, inferred or otherwise, to target individuals with political messaging without the explicit consent of the individual.**
- There is a qualified condition in the DPA for registered political parties to process political opinion data. You must have an 'appropriate policy document' in place to rely on this condition.
- There is another condition for processing special category data belonging to members of not-for-profit bodies with a political, philosophical, religious or trade union aim and those who the bodies regularly contact.
- There is a further condition of explicit consent that you can also rely upon.

In more detail

What is special category data?

Article 9 of the GDPR gives special protection for certain types of personal data which are considered to be particularly sensitive. These are known as 'special category data'.

Political opinions are classed as special category data.

Other special category data includes information about an individual's:

- race;
- ethnic origin;
- religious or philosophical beliefs;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

In order to lawfully process special category data, in addition to identifying a lawful basis under Article 6 you also need a separate condition for processing special category data under Article 9. The DPA Schedule 1 provides further clarification on the application of some of these conditions.

You must determine your condition for processing special category data before you begin this processing, and you should ensure you document this.

As well as factual information, if you are able to infer or guess details about people that fall within the special categories of data then whether or not this counts as special category data and triggers Article 9 will depend on whether you are intentionally processing the data in order to infer those details.

You need to comply with Article 9 if you intend to create such inferences. This is because you are processing special category data, regardless of how confident you are as to the accuracy. You also need to be careful that these assumptions about people do not lead to you processing inaccurate, inadequate or irrelevant personal data.

Can special category data be used to target individuals with political messaging?

You should not use special category data, inferred or otherwise, to target individuals with political messaging without the explicit consent of the individual.

Except in very specific circumstances where other conditions may apply (see sections below), there is unlikely to be another condition under Article 9 of GDPR that applies to such processing.

Targeting individuals using special category data raises significant questions around fairness. Under Article 5(1)(a) of GDPR, personal data must be processed fairly. Using special category data to target individuals is intrusive and could be discriminatory.

In addition, Article 5(1)(c) of GDPR is clear that the processing of personal information should be "limited to what is necessary in relation to the purposes for which they are processed". With the exception of political opinions, it is difficult to see in what circumstances it would be necessary to process special category data for the purposes of targeting political messaging.

Example

A political party wants to send cards to people in a marginal constituency to celebrate a particular religious festival and encourage them to support the party. The party is aware that many people in the constituency do not celebrate the festival. The party does not wish to offend these individuals by sending them a card for a festival that they do not celebrate. They decide to use software to screen the names of constituents and infer a likely ethnic origin and religious belief. They then send cards to those they have identified as likely to celebrate the festival.

In this example, the party is intentionally processing personal data in order to infer the religious beliefs or ethnic origin of constituents. Regardless of how confident the party is about this inference they are still processing special category data. They should therefore not carry out this processing without the explicit consent of the individuals.

Can political parties process political opinions?

There is a relevant condition under GDPR Article 9(2)(g) further clarified by the DPA Schedule 1, Paragraph 22. This condition is narrowly defined and can only be relied upon by registered political parties.[9]

This condition only applies where:

- the processing is of personal data revealing political opinions;
- the processing is necessary for the purposes of the party's political activities;
- the processing is not likely to cause substantial damage or substantial distress to a person; and
- the individual subject to the processing has not given written notice to the party requiring them not to process their personal data.

Parties can only rely on this condition if they can demonstrate that it is necessary for the purposes of their political activities. Political activities in this context include campaigning, fund-raising, political surveys and case-work.

If relying on this condition, you must be able to demonstrate the necessity to process political opinion data specifically. In other words, if you can achieve the same political campaigning purpose without processing data relating people's political opinion data, then you cannot rely on this condition.

You should also ensure that you appropriately assess the likeliness of the processing causing an individual substantial damage or substantial distress. You should include this in your DPIAs.

You must also ensure you have an effective process for recognising and dealing with written notices from individuals to the party requiring them not to process their personal information. The notice must give the party a reasonable time period to stop the processing. After this time, the party must stop processing the data.

In addition, DPA Schedule 1, Part 4, Paragraph 39 requires you to have an 'appropriate policy document' in place if you are relying on this condition. See our guidance on special category data for further information.

[9] Under section 23 of the Political Parties, Elections and Referendums Act 2000

You cannot rely on this condition for processing any other special category data aside from political opinions.

Only registered political parties can rely on this condition. If you are not, then you need to rely on the explicit consent of the individual to process political opinions.

Can membership and regular supporter data be processed for political campaigning purposes?

It is worth highlighting Article 9(2)(d), which is another relevant condition for the processing of special category data. You can only rely on this for processing special category data belonging to members or those with whom you have regular contact with.

Article 9(2)(d) permits you to process special category data if:

> "processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects".

You can only rely on this condition if you:

- are a not-for-profit body. Not-for-profit bodies may include charities, clubs, political parties, churches, trade unions and other associations which have a political, philosophical, or religious aim;

- are processing special category data as part of your legitimate activities. This is fairly broad, and will cover most of what you do, as long as it does not stray outside your established purposes or powers, and is not unlawful or unethical in any way;

- are only processing the data of members, former members, or other individuals in regular contact with you 'in connection with your purposes' – eg partners, supporters or beneficiaries. This condition will not therefore apply to processing the data of prospective members or other individuals who have not had any prior contact with your organisation;

- have appropriate safeguards in place. This might for example include restricting access to the data, applying shorter retention periods, or providing individuals with an opt-out; and

- do not disclose this data to a third party without the individual's consent. You must get explicit consent for any disclosures. If you need to disclose the data to a third party without consent, you will need to rely on a different condition for the disclosure.

You do not need to demonstrate that it is necessary to process special category data to rely on this condition. However, this does not mean it is a blanket condition for all processing by not-for-profit bodies. You must still demonstrate how you meet the specific requirements of the condition, and consider your data minimisation obligations.

What is explicit consent?

Article 9(2)(a) provides a condition for processing special category data of all types if the individual subject of the data has provided their explicit consent for the processing.

Explicit consent is not defined in the GDPR, but it is not likely to be very different from the usual high standard of consent (see consent lawful basis above). All consent must involve a specific, informed and unambiguous indication of the individual's wishes. The key difference is likely to be that explicit consent must be expressly confirmed in words which refer to the type of special category data involved, rather than by any other positive action.

If you need to rely on this condition, you should take extra care over the wording. Even in a written context, not all consent will be explicit. You should always use an express statement of consent. You must keep records of these expressions. For further information see our guidance on consent.

Further reading

For further information see our Guide to GDPR, our interactive lawful basis guidance tool and details guidance on consent and legitimate interests.

For general guidance on key data protection concepts see our Guide to Data Protection.

The General Data Protection Regulation is published here.

Use of the electoral register

At a glance

- Registered political parties, candidates and campaigners are entitled to receive copies of the full electoral register which includes eligible voters' names and addresses.
- They are also entitled to access the 'marked register', which enables identification of individuals who have voted in previous elections and referendums, but not how they have voted.
- Access to this information is important for promoting political participation. But it does not come at the expense of complying with data protection law.

In more detail

What is the electoral register?

People eligible to vote in UK elections and referenda are required to register to vote. Their names and addresses are held on the electoral register. There are two versions of this register - the full register and the open register[10].

The open register is available for anybody to purchase. Individuals have the right to opt out of appearing on the open register. The full version has restricted access and there is no right to opt out.

Can we use personal data from the electoral register for political campaigning purposes?

Registered political parties, candidates, registered referendum campaigners, registered non-party campaigners (who campaign at elections) and registered recall petition campaigners are entitled to

[10] Called the 'edited register' in Northern Ireland.

receive copies of the full electoral register[11]. They are also entitled to access the 'marked register' (where they reach certain criteria), which enables identification of individuals who have voted in previous elections and referendums, but not how they have voted.

Much political campaigning makes use of the names and addresses held on the electoral register. Access to this information is important. It helps you to convey your messages to voters - furthering political debate and promoting democratic participation. However, even if you have the legal right to process the information contained within the full electoral register, it is important to understand that this does not exempt you from complying with data protection law.

In particular, you must:

- only obtain and use the register in ways compatible with electoral law;
- take steps to ensure the accuracy of the data. You should request updated versions of the register on a regular basis. Using older versions risks writing to people who are no longer living in certain addresses or not taking account of other factors such as changes of name or individual wishes not to be on the register;
- not share electoral register data with any other controllers; and
- only share data with processors where allowed under electoral law.

In addition, even though there is a legal entitlement to obtain and process electoral register data, you must still meet the requirement in GDPR to provide privacy information to those individuals. As a controller you must take all reasonable steps to do this, which could include signposting to other sources of information about how the register is used.

The ICO does not expect this to extend to campaigners contacting all voters directly with this information, but you must take regular and active steps to communicate alongside other privacy information. We would also expect relevant controllers to take part in centralised transparency initiatives organised by the ICO or the Electoral Commission.

Further reading

For more information on your obligations under electoral law visit the Electoral Commission's website.

For general guidance on key data protection concepts see our Guide to Data Protection.

How should we collect personal data?

At a glance

- Campaigners collect data on individuals beyond the electoral register for various reasons. Demonstrating compliance with the principles, rights and obligations of GDPR is essential.
- You need to give individuals clear, accessible and intelligible privacy information regardless of whether the information is derived directly or from a third party such as a data broker. The best way to do this depends on the method of collection.
- Individuals should not be surprised to learn that you are using their personal data for particular campaigning purposes.

In more detail

Introduction

There are many reasons why you may wish to collect personal data in addition to the data contained in the electoral register. Campaigners often seek to use the register as a 'spine' on which to add more granular and detailed information, including:

- market research to inform wider campaigns;
- to understand more about individual voters to enable better targeting of political messages;
- to identify individuals to persuade to turnout to vote;
- to contact individuals; and

- to sign up potential members, supporters, donors or volunteers.

Whatever the reason, whenever you process personal data (including when you collect it) you must do so in accordance with all the data protection principles and individuals' rights.

What is the right to be informed?

When collecting personal data, the right to be informed is of particular importance. This right covers some of the key transparency requirements of the GDPR.

The GDPR contains specific provisions about the information that you must give to individuals when you process their personal data. These are set out at Article 13 and Article 14. This information includes[12] the:

- controller's details;
- purpose(s) of the processing;
- lawful basis being relied upon;
- retention periods of the data;
- rights available to the individuals; and
- details of the existence of automated decision-making, including profiling.

We call this 'privacy information'.

You must ensure individuals are provided with privacy information regardless of whether you collect the personal data directly from individuals or from a third party. Privacy information must always be:

- concise;
- transparent;
- intelligible;
- easily accessible; and
- use clear and plain language.

However there are different considerations depending on how you obtain it.

[12] See our guidance on the right to be informed for a comprehensive list.

What are the requirements when we collect personal data directly from individuals?

Article 13 of GDPR lays out the 'right to be informed' requirements when you collect personal data directly from the individual it relates to. In these circumstances you must provide them with privacy information at the time you obtain their data. There are some exemptions to this, but in the majority of cases these don't apply to processing for the purposes of political campaigning.

You can meet this requirement by putting the information in a prominent position on your website or other digital services such as apps, but you must make individuals aware of it and give them an easy way to access it. You should also provide an alternative method, where appropriate, in case individuals do not have access to the internet.

For political campaigning purposes the best way to do this will depend on the method of collection. Some collection methods and suggested ways to provide privacy information are below.

Method of Collection	**Suggested ways to provide privacy information**
Face to face canvassing	Provide individuals with a leaflet containing the privacy information or a more basic privacy statement with a link to a website with an alternative contact address where people can write to obtain the privacy information.
Paper petitions and surveys	Prominently display privacy information or a more basic privacy statement with a link to a website with an alternative contact address where people can write to obtain the privacy information.
Online petitions, surveys and quizzes	Prominently display a link to the privacy information on the

	petition/ survey/ quiz document itself Or Prominently display a link to the privacy information on the landing page for the petition/ survey/ quiz. Carry out user testing to ensure individuals can access this information easily and are fully aware of who is behind the survey and for what purpose their data will be used.
Mobile applications	Prominently display privacy information before the individual downloads the app. This could be done via an app store or via a link to privacy information on your website. If you provide privacy information after an app is downloaded and installed, make sure that this is done before the app processes the relevant personal data.
Telephone canvassing, petitions and surveys (where lawful under PECR – see direct marketing methods section)	Include privacy information in scripts for those making the phone calls. Ensure individuals have heard the information and have an opportunity to hear it again if necessary. Provide a website address or alternative contact address for individuals to access again in the future if they wish.

In addition, you should ensure that you consider language alternatives and accessibility options in providing privacy information. You should make alternatives available on request.

You should carefully consider the necessity for collecting any personal data for individuals under the age of 18. If you do decide it is necessary (eg for membership purposes or where under 18 year olds are eligible to

vote in an election or referendum) you must provide age appropriate privacy information. See our Age Appropriate Design Code for further information (currently in draft).

You do not need to put all your privacy information in a single block of text. In fact, displaying privacy information in this way may be disadvantageous in many cases, such as collecting data through applications. You should consider the easiest way for individuals to read and understand this information depending on your method of collection. Other ways to display privacy information include:

- **A layered approach** – short notices containing key privacy information that have additional layers of more detailed information.
- **Dashboards** – preference management tools that inform people how you use their data and allow them to manage what happens with it.
- **Just-in-time notices** – relevant and focused privacy information delivered at the time you collect individual pieces of information about people.
- **Icons** – small, meaningful, symbols that indicate the existence of a particular type of data processing.
- **Mobile and smart device functionalities** – including pop-ups, voice alerts and mobile device gestures.

You need to provide appropriate training and guidance for staff and volunteers to ensure they include appropriate privacy information on relevant documents or when collecting data on the doorstep or by phone.

Can we collect Voter Registration Applications?

Political parties, candidates and others play an important role in promoting democratic engagement by encouraging individuals to register to vote. This means that you may handle registration and absent voting applications.

If you do handle these applications, then you should do so with great care and forward them to the appropriate Electoral Registration Officer at the earliest opportunity.

You must also be clear in your privacy information about the purposes for which you are collecting these forms and the lawful bases you are relying upon. In particular, you must be clear about what personal data you are collecting for your own political campaigning purposes and what personal data you are collecting for the purposes of voter registration. In other words, there should be no deception - individuals should not be surprised to learn that you have used their data for campaigning purposes.

What are the requirements when we collect personal data not directly from the individual?

Article 14 of GDPR lays out the 'right to be informed' requirements when you obtain personal data from a source other than the individual it relates to, such as a data broker. In these circumstances you need to provide the individual with privacy information, including:

- the source of the data and details of the categories of the data; and
- within a reasonable period of obtaining the personal data and no later than one month.

Also:

- if you use the data to communicate with the individual, at the latest, when the first communication takes place; or
- if you envisage disclosure to someone else, at the latest, when you disclose the data.

Article 14(5) of GDPR provides a number of exceptions to providing privacy information to individuals where you have collected personal data from a third party.The majority of these are unlikely to be relevant in the political campaigning context. However two of these may be relevant depending on the particular circumstances:

- the individual already has the information; or
- providing the information to the individual would involve a disproportionate effort.

If you are considering relying on the individual already having the information, you must be able to demonstrate and verify what information the individual has already been provided with. It is not sufficient to simply rely on assurances from the third party. You should do your own due diligence and request evidence, if appropriate. You must ensure that they have been provided with all of the information that is listed in Article 14 –

if you are unsure what they have been given or if anything is missing you must provide this to individuals.

If you want to rely on the disproportionate effort exception not to tell people about your processing, you must assess this fully on a case by case basis. The ICO recognises that the unique circumstances of political campaigning may sometimes present situations where disproportionate effort may apply, particularly with regards to electoral register data. However, you must fully assess and document whether there's a proportionate balance between the effort involved for you to give privacy information and the effect of the processing on the individual. If the processing has a minor effect on the individual then your assessment might find that it is not proportionate to put large resources into informing individuals. However, the more significant the effect on the individual, the less likely it is that you can rely on this exception.

It is difficult to argue disproportionate effort if you are contacting the individual as part of your processing. This includes all direct marketing by any means including the freepost electoral address. Unless you are certain the individual has already been provided with privacy information, you should provide it as part of your communication.

If you determine that providing privacy information to individuals does involve a disproportionate effort, you must still publish the privacy information, for example on your website. You must also carry out a DPIA as the processing is considered to be 'invisible processing'. See the section on DPIAs for further information.

Can we use data collected from third parties such as data brokers or other companies providing marketing data services?

Many organisations including political parties buy or rent data from data brokers or other companies to use for direct marketing purposes. In political campaigning these can be split into three broad categories:

- buying or renting a list of contact details;
- buying additional factual personal data to undertake analysis in house and draw out inferences, such as dates of birth, number of children or car ownership; or
- buying inferred data directly from the individual or from other sources, to append to names and addresses obtained from the electoral register, such as likely interests and characteristics.

Contact details

Buying or renting additional contact details in most instances is likely to be unfair without the consent of the individual. For example, buying phone numbers or email addresses to add to the address details that you already hold. This is likely be true no matter how clearly you explain in your privacy information that you might seek out further contact details from third parties. This is because individuals don't reasonably expect you to contact them using details they never gave you or they were never required to give in their electoral registrations. In many cases, if you contact them, this is also likely to be a breach of PECR.

If an individual has consented via a third party for you to have their contact details to use for political campaigning or direct marketing then you can match this to what you already hold about them. However, it is important to be clear that the consent must have named you specifically. It is not sufficient if it referred to you in a general sense, eg 'selected third parties', 'trusted partners' or 'for political campaigning purposes'.

Factual personal data

If you buy or rent factual personal data from a data broker or other third party, then you must ensure that the individual has been provided with appropriate privacy information and the type of information is in their reasonable expectations for you to process.

You must comply with the right to be informed and provide people with your own privacy information, detailing anything that they have not already been told. This includes informing them of any change of lawful basis (ie if processing under public task - democratic engagement or otherwise, if different from the lawful basis under which the data was originally obtained).

Inferred data

Whether inferred data is personal data or not depends on whether the individual is identified or identifiable, directly or indirectly, from that data or any other information you hold or are likely to hold. If a data broker or other third party provides you with purely anonymous data, and you don't process this further in any way that could identify individuals, then this is not personal data. For example, you receive anonymous data that people living in Wilmslow are more likely to read a particular newspaper and you don't append it to names and addresses.

However, if you receive inferred data against names or addresses or you append it to names and addresses or other identifiable information then this is personal data. You should treat this data in the same way as you would treat factual personal data.

Due diligence

It is important to remember that you are responsible for ensuring compliance with the GDPR and PECR. Simply accepting a data broker or other third party's assurances is not enough. You must be able to demonstrate your compliance and be accountable.

You must make rigorous checks to satisfy yourself that:

- the third party obtained the personal data fairly and lawfully;
- the individuals understood their details would be passed on for political campaigning purposes; and
- you have the necessary consent (where this is required) which specifically names you and covers the method of communication that you want to use.

As part of your due diligence you could ask the third party to give you:

- details of who compiled the data or direct marketing list – ie was it the third party or someone else;
- a copy of the privacy information that was used when the details were collected;
- details of how they collected the personal data;
- the dates the list was compiled – ie how old is the data;
- details of how the nature of the third parties who were to receive the data were explained – if they were told 'third parties' in general terms this is not enough for the consent to be informed;
- records of the consent (if it is a 'consented' list) – ie what the individual consented to, what they were told, when and how they consented;
- if it is claimed that the list has already been checked against the Telephone Preference Service - evidence that this has happened and how recently.

A reputable third party should be able to demonstrate to you that they obtained and processed the data for sale or rent in compliance with data protection law. If they cannot do this, or if you are not satisfied with their explanations, you should not use the data.

As well as relevant data sharing agreements, you may wish to have a written contract confirming the reliability of the data, as well as making your own checks. The contract should give you reasonable control and audit powers. However it is important to remember that you are still responsible for compliance and such a contract does not remove this responsibility from you.

Example

A campaign group wants to purchase email addresses from a data broker so it can email people it believes will be supportive of their campaign. The data broker assures the campaign group that the email addresses have all been obtained and can be shared in compliance with data protection law. The campaign group is unsure about this so asks the broker to put these assurances in their contract. The broker agrees and the campaign group uses the email addresses to send out political campaigning messages.

A few weeks later the campaign group receives a letter from the ICO. They have received a number of complaints about the emails and targeted messages. The campaign group tells the ICO that they have been assured that the data has been collected and shared in accordance with data protection law. The ICO ask the campaign group to provide the evidence and explain the due diligence the campaign group took. The data broker is not able to provide any evidence and the campaign group admits that the only due diligence they did was to have it written into the contract.

The ICO may fine the campaign group and the data broker for breach of the GDPR and the campaign group for breach of PECR. The campaign group's reputation is significantly damaged.

Once you have obtained the list, you must be prepared to deal with any inaccuracies or complaints arising from its use. If you receive complaints from individuals whose details came from a particular source, this suggests that the source is unreliable and you should not use it.

Can we collect personal data from publicly available sources including social media?

The GDPR does not stop you from obtaining and using personal data from publicly available sources for political campaigning. However, you should not assume that because the data is publicly available that data protection law doesn't apply. If you process this data, you become the

controller for it, and you must ensure that you comply with the GDPR and PECR.

For example, the transparency requirements of the GDPR will apply. This means you must comply with the right to be informed and ensure that you provide people with privacy information (unless you are relying on an exception).

You also cannot assume that simply because an individual has put their personal data into the public domain, they are agreeing to it being used for political campaigning purposes.

For example, individuals may want as many people as possible to read their social media post, but that does not mean they are agreeing to have that data collected and analysed to profile them to target with your campaigns. Likewise just because an individual's social media page has not been made private does not mean that you are free to use their data for political campaigning purposes.

You should carefully consider the use of online campaigning platforms that contain a match function capable of matching data from your databases with social media data from public profiles or other publically available online sources. These platforms usually act as a processor and could prove a significant risk if you contract them. Of particular concern is if there is no option within the platform to turn off the matching functionality or if it matches individuals on an automatic or blanket basis.

As well as lacking transparency, collecting personal data from online sources including social media platforms on a blanket basis is likely to be unfair as well as in breach of the data minimisation principle. If you decide to use these platforms, you must carry out a DPIA to help identify and mitigate against the risks.

Can we collect personal data from our own social media pages?

Many political parties, campaigners and candidates have dedicated pages on social media which individuals can 'like' or 'follow'. These are considered a useful way to engage with members, supporters or potential supporters. Depending on the platform and terms of service, you may have the ability to collect personal data from the individuals' personal social media profiles. In addition, the social media company is likely to place cookies or similar technologies on the individuals' devices. If you have a dedicated page on social media, it is important to be aware that you are likely to be a joint controller with the social media company. This

is because you both have a role in deciding the manner and the purpose for processing the data.

You both have joint responsibility for complying with data protection laws. In particular, this means that you need to ensure you provide appropriate privacy information for individuals on your page that clearly explains how, by whom and for what purpose their data is being processed. You must also ensure that you and the social media company are both aware of your obligations.

Example

A political party sets up a page on a social media platform. The purpose of the page is to encourage followers to support the party's aims and understand more about the types of people who follow the page so they can better target campaigns. The party subscribes to the social media platform's conditions of use of the page, including their cookie policy, and acts as an administrator.

The social media platform places a cookie on the computer of those who visit the page (both users and non-users of the social media platform). This cookie feeds back personal data to the social media platform that helps the platform tailor its advertising services across its platform. The platform also feeds back anonymised analytics information to the party on those who have visited their page.

In this example, the party and social media platform are joint controllers. They both have a role in deciding the purpose and manner of processing the personal data. The campaign group decides on the overall purpose of processing the data and ultimately chooses to setup a page on the platform which encourages processing of personal data. The social media platform decides on the purpose to help tailor its advertising services and provide analytics to the campaign group. It also decides what personal data it processes from the cookie and the manner in which the processing takes place.

Both the political party and social media platform must ensure they process personal data in accordance with the GDPR, in particular providing appropriate privacy information.

Further reading

For advice and guidance on carrying out DPIAs see our guidance.

For general guidance on key data protection concepts see our Guide to Data Protection.

Profiling in political campaigning

At a glance

- Profiling is analysing information in a way that classifies individuals into different groups or sectors, using algorithms or machine-learning.
- When carrying out profiling you must consider the fairness of the processing. This includes the potential effects on individuals and wider society.
- Individuals have the right to object to profiling. If you are profiling for direct marketing purposes there are no grounds to refuse this objection.
- Article 22 of the GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them. If carrying out profiling or micro-targeting you should fully consider whether Article 22 could apply.
- Where Article 22 does apply to your processing you must take additional steps including carrying out a DPIA and obtaining the explicit consent of the individuals subject to the decisions.

In more detail

Introduction

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, including the ever increasing scale of data collection and sophistication of analytics techniques, means there is greater scope for significant privacy intrusion or wider societal risks. This is because:

- profiling is often invisible to individuals;
- people might not expect their personal data to be used for political campaigning purposes in this way;
- people might not understand how the process works or how it can affect them;
- people's trust in the democratic system can be undermined if there is a lack of transparency and understanding of techniques being used; and
- campaigns involving sophisticated profiling techniques have the potential to influence the voting behaviour of a large number of individuals.

If you are carrying out or intend to carry out profiling then there are particular considerations that you need to take into account into order to comply with data protection law.

What is profiling?

> "Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

Article 4(4) of GDPR says that profiling is:

In other words, profiling is analysing information in a way that classifies individuals into different groups or sectors, using algorithms or machine-learning. This analysis identifies links between different behaviours and characteristics to create profiles for individuals. For example, a list of people who read a particular newspaper or who you think are likely to vote a certain way.

There is more information about algorithms and machine-learning in our paper on big data, artificial intelligence, machine learning and data protection[13].

How does the concept of fairness apply to profiling?

Of utmost importance when profiling or using data analytics techniques is fairness. Fairness is used in its general sense and is about processing personal data in ways that are in the reasonable expectations of individuals. It is very closely linked to data ethics.

You must consider the potential effects of your processing on individuals, whether these are direct or indirect. You should also consider the general effects on wider society in using certain techniques in political campaigning. As techniques become less expensive and perhaps more effective you need to ask yourself not just whether you **can** use these techniques but also whether you **should**.

You need to pay particular attention if you use psychographic analytics and psychometric profiling with regards to fairness obligations in the law. These techniques involve attempting to deduce certain personality attributes from both factual and inferred personal data about individuals. Campaigns have used these attributes to target particular political messages designed to influence voting behaviour, which could be considered unfair and thus in breach of GDPR.

Example

A campaign group uses psychometric profiling and scores certain individuals highly on a scale of neuroticism about crime. It then targets these individuals with political messaging about knife crime in a way that is designed to invoke a fear response. Processing personal data in this way is likely to be unfair.

What are the other key considerations when carrying out profiling for political campaigning purposes?

If carrying out profiling for political campaigning purposes, you should also do the following:

[13] https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

- revise your privacy policy and inform individuals about the profiling that you carry out. This is particularly important if you are profiling individuals who have had no contact with you, such as members of the public who you are trying to understand. Profiling is often not well understood and when being carried out in a political context can be disconcerting if people do not fully understand what it entails and how it is used;

- remember that if the data you're using isn't correct then any profile or decision based on the data will also be flawed. Where possible you should try to ensure the accuracy of the personal data you use; and

- don't collect too much information or keep it for too long. Just because your systems allow you to retain vast quantities of data doesn't mean you should. It also makes it more difficult to keep the data up to date, accurate and relevant for the profiling you're carrying out.

Can individuals object to profiling?

Article 21 of the GDPR gives individuals the right to object to profiling.

Most profiling in political campaigning will be for direct marketing purposes (see the section on direct marketing for more information). If this is the case, you must stop the profiling as soon as you receive an objection. There are no exemptions or grounds to refuse this objection.

If you are profiling for purposes other than direct marketing, such as creating models with no intention to send political campaigning messages to those individuals, then the right to object applies slightly differently. In these cases an individual can object on any grounds relating to the individual's interests. You have to stop the processing unless you can show that you have a compelling reason to continue the profiling that overrides the individual's interests.

You must bring this right to object to the attention of individuals and present it separately from other information.

If you receive an objection under Article 21, you need to respond within one month and confirm the action you've taken.

Can we use third parties to carry out profiling or analytics on our behalf?

You may wish to use third parties to carry out profiling on your behalf. What considerations you need to take into account will partly depend on whether the third party is acting as your processor, a joint controller or a separate controller (see our guidance on controllers and processors for more information). However, you should also consider the following:

- where is the third party going to be processing the data? If this is outside the EEA then this will be an international transfer and you will need to take other considerations into account. (See our guidance for further information on this[14].);
- you must carry out due diligence to ensure they are carrying out profiling in compliance with data protection law;
- you must ensure there is an appropriate mechanism for complying with individuals rights; and
- you should ensure that any personal data shared with the third party is not being amalgamated into a shared pool of data used across multiple campaigns or organisations.

What profiling is restricted?

Article 22(1) of the GDPR limits the circumstances in which you can make **solely automated decisions**, including those based on profiling, that have a **legal or similarly significant effect on individuals.**

If you carry out automated decisions that are subject to Article 22(1) then you must not do this without the explicit consent of the individuals subject to the decisions.

It is important that political parties and campaign groups are able to engage with voters. It is equally important for campaigners to communicate information and promote their opinions effectively. Where it is carried out fairly, transparently and in compliance with the law, the use of profiling and micro-targeting is an acceptable communication method. As a general approach, Article 22(1) will not restrict this.

Much of the profiling and micro-targeting carried out by political parties and campaign groups is likely to be considered **solely automated decision making**. In most cases, this is unlikely to produce a legal or 'similarly significant effect' on an individual. However, there are likely to be exceptions to this.

[14] ICO guidance on international transfers.

In this context a decision producing a **legal effect** is something that affects a person's legal status or their legal rights. For example, affecting somebody's legal right to vote.

A decision that has a **similarly significant effect** is something that has an equivalent impact on an individual's circumstances, behaviour or choices. This effect must be on the individual specifically subject to the profiling. Although political campaigning can have significant effects for society in general, this does not mean that a decision to target an individual with a campaign message will have a significant effect on that particular individual. It may indeed have an effect on the way in which they choose to vote, but it is very difficult to establish cause and effect – there could be many reasons that influenced his/her choice. Simply changing an opinion, even on something as important as voting choices, is unlikely to be similarly significant to a legal effect.

What could be considered a legal or similarly significant effect?

Particularly intrusive methods or outcomes of a decision about whether to micro-target an individual with a political campaigning message could have a legal or 'similarly significant effect'. For example, there are international examples of messages having been targeted that contain an element of threat, are discriminatory in nature, or seek to manipulate or disenfranchise an individual:

Example

A political campaigner decides it would be beneficial for their preferred candidate if a particular minority group was to be underrepresented on polling day in an upcoming election. The campaigner makes a solely automated decision to micro-target those individuals who he has identified as being members of a particular minority group. The message encourages these individuals not to vote in the election. This kind of processing is very likely to be restricted by Article 22.

It is also possible that a similarly significant or even legal effect on the individual could come from the compound effect of the underlying profiling, the methods and techniques used to target an individual and the individual's expectations and lack of knowledge about how their data is being used, combined with the nature of the message.

Example

A political party, through a combination of the data they hold and the data held by a social media company, is able to identify and target messages about NHS waiting times to individuals who are recently bereaved or have a certain medical condition. The intention is to invoke an emotional reaction from the individual to encourage them to support the party, who is advocating for an increase in NHS funding. This kind of processing is very likely to be restricted by Article 22.

If carrying out profiling or micro-targeting you should fully consider whether the decision could have a legal or 'similarly significant effect' on the individuals you profile. You should consider the following questions:

1. **Is the profiling process particularly intrusive?**

    - Would individuals likely be surprised to discover you were profiling them in this way? Is there a lack of transparency?
    - Is the personal data you are using to profile individuals particularly sensitive or special category data?

2. **Is the way the advert is delivered particularly intrusive?**

    - Is the frequency of messages beyond an individual's reasonable expectations?
    - Are you delivering the messages in a way that is designed to have a strong effect on an individual, such as at a particular time of day?
    - Do the techniques you are using exploit the possibility of conveying a message, or of otherwise influencing their minds without their being aware, or fully aware, of what has occurred?

3. **Is the combination of the profiling of personal data alongside the nature of the message of a particular type that is highly emotive and affects the individual?**

    - Could this combination amount to seeking to influence the autonomy of an individual, rather than simply seeking to influence views or change opinions?

4. **Are there any particular vulnerabilities of the individuals targeted that could be significantly affected by the message?**

    - Are you using psychometrics to target people with particular characteristics in order to invoke a particularly strong reaction?

5. **Is the profiling and targeting likely to cause detriment to an individual?**

    - Does the decision produce a discriminatory effect?
    - Could the message be considered threatening in nature?
    - Could the individual in effect be disenfranchised as a result of profiling and micro-targeting?

If your answer is 'yes' to any of the questions above or you have reason to believe your decision about whether to micro-target could legally or similarly significantly affect the individuals concerned, you need to give serious consideration about whether you continue with the processing. As a minimum, you should carry out a DPIA to identify and help mitigate any risks.

If you find that your processing is likely to have a legal or similarly significant effect on an individual and you are unable to mitigate this risk sufficiently, then Article 22 is likely to apply.

If Article 22 applies, what do we need to do?

If your processing is restricted by Article 22 then, in addition to complying with GDPR requirements as normal, you must:

- have the explicit consent of the individual subject to the decision;
- carry out a data protection impact assessment;
- inform individuals that you are using their data for solely automated decision-making processes with legal or similarly significant effects; and
- provide meaningful information about the logic involved and what the likely consequences are for individuals.

You will also need to ensure that individuals are able to:

- obtain a human intervention;
- express their point of view; and
- obtain an explanation of the decision and challenge it.

Further reading

For further information about automated decision making and the application of Article 22, please see our Guidance on Automated Decision Making and Profiling.

For general guidance on key data protection concepts see our Guide to Data Protection.

Political campaigning - direct marketing

At a glance

- The vast majority of political messaging directed to particular individuals is considered to be 'direct marketing'.
- If you engage in direct marketing, you have additional responsibilities under the GDPR and PECR.
- Genuine service communications and market research do not fall under direct marketing rules. However, the rules apply if you use these to send political campaigning messages.
- Individuals have an absolute right to object to direct marketing at any time. This includes profiling of data linked to the marketing.

In more detail

Introduction

The GDPR and PECR place additional responsibilities on data controllers for processing for the purposes of direct marketing. It is important to comply with these.

What is direct marketing?

Section 122 of the DPA defines 'direct marketing' as:

"the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals".

This definition extends to any means of communication including:

- in person;
- post;
- telephone;
- email;
- online;
- through social media; or
- other emerging channels of communication.

It also covers any messages which include some marketing elements, even if this is not their main purpose.

Direct marketing is not limited to the offer for sale of goods or services only, but also includes the promotion of the aims and ideals of any organisation including political campaigns. This includes appeals for funds or support for a campaign, encouraging individuals to take some form of direct action or vote for a particular political party or candidate.

The vast majority of political messaging directed to particular individuals is considered to be 'direct marketing'.

However, not all the messages you send are direct marketing. For example, messages you send for administrative purposes about an individual's account – such as simply reminding a party or campaign group member how to contact you in case of a problem, or to check that your member's details are correct. If a message is truly a service message and you are not attempting to market, promote or advertise anything then it does not constitute direct marketing. See our direct marketing code for further information (currently being drafted).

In political campaigning, generally service messages are only sent to party or campaign group members or supporters. It is difficult to see in what circumstances contacting a member of the public for political campaigning purposes would not constitute direct marketing.

When does market research become direct marketing?

A political campaign can conduct genuine research to help inform their views and formulate policies, in the same way that professional market

research companies do. The direct marketing rules do not apply to genuine market research as this does not involve the communication of advertising or marketing material.

However, communications claiming to be for research that are in reality intended to gain support now or at some point in the future are covered by the direct marketing rules. For example the following are direct marketing:

- a telephone call which starts by seeking an individual's opinions and then urges support or invites contact with a political party, referendum campaigner or candidate or to provide promotional materials on request; and

- a telephone call which seeks an individual's opinions in order to use that data to identify those people likely to support the political party or referendum campaign at a future date, in order to target them with marketing.

It should be possible for you to carry out market research without recording the information in a way that identifies the individual respondent. If you record the responses in a way that it can be linked to the individual so you can then follow up their responses and target them in the future, this is direct marketing.

How does the GDPR's right to object apply?

Under the GDPR, if you are processing personal data for direct marketing purposes you need to be aware that individuals have the right to object at any time. This includes any profiling of data that is related to direct marketing.

This is an absolute right and there are no exemptions or grounds for you to refuse. Therefore, when you receive an objection to processing for direct marketing purposes, you must stop processing the individual's data for this purpose.

Objections to processing can be verbal or in writing, so it is important that you have an effective procedure for recognising, recording and dealing with these objections. This is likely to involve training your public facing staff and volunteers and having a mechanism to ensure individuals are not marketed to again.

You do not automatically need to erase the individual's personal data. In most cases it is preferable to suppress their details. Suppression involves

retaining just enough information about them to ensure that you respect their preference not to receive direct marketing in future. This is particularly important if you have obtained data from the electoral register. If you simply delete the data rather than add it to a suppression list, then when you obtain the register again you will have no record of those who have objected. In this situation there is a high risk that you could market to these individuals again in breach of their objection.

How does PECR apply?

If you are carrying out any direct marketing by electronic means then, alongside the GDPR right to object, you also need to comply with the PECR rules on direct marketing. The rules differ depending on the method of communication (see below for detail on each method) but in many cases, you can only carry out direct marketing by electronic means with the consent of the individual. See the consent section for further information on what is meant by consent.

How do we carry out political campaigning by post?

Marketing by post is not subject to PECR. PECR only applies to electronic communications.

Post directed to particular individuals

However, mailings addressed to individuals by name are caught by the definition of 'direct marketing' in nearly all circumstances – whether delivered by the Royal Mail, private delivery firms or by local volunteers. Data protection law, including the right to object, applies in these circumstances.

Post not directed to particular individuals

Leaflet-drops and mailings not directed to particular individuals are not subject to data protection law and not considered to be direct marketing. For example mail which is unaddressed, or addressed merely to 'the occupier'.

However, if you know the name of the person you are mailing, you cannot avoid your obligations by simply addressing the mail to 'the occupier', as you are still processing that individual's personal data behind the scenes.

Is the Freepost Election Address direct marketing?

Candidates, political parties and referendum campaigners have a right (depending on the type of election or referendum) to send an 'election address' by Freepost, either addressed to each individual elector or unaddressed to each postal address.[15] This applies to elections for the UK Parliament, Scottish Parliament, Northern Ireland Assembly, National Assembly for Wales, European Parliament, or at a particular referendum. Although you may direct this type of Freepost mailing to particular individuals and is subject to data protection law, it does not constitute direct marketing so the right to object does not apply.

Political campaigning – face to face

Face to face campaigning directed to particular individuals is covered by data protection law in much the same way as campaigning by post. PECR does not apply, but individuals have the right to object to the processing for direct marketing purposes.

The key difference is that in face to face campaigning, requests to object will usually be made verbally rather than in writing. You should fully consider how the right to object could apply in practice, such as through targeted door to door canvassing. You should ensure there is appropriate training for staff and volunteers as well as procedures for recognising, recording and managing objections.

Managing verbal requests can be complicated, even more so when dealing with door to door canvassing where there are often several individuals in the same house. If in doubt as to whether a request is valid, it is best to be cautious and treat it as if it is.

[15] Section 91, Representation of the People Act 1983 for UK Parliament elections; Regulation 63, European Parliamentary Election Regulations 2004; Regulation 58, European Parliamentary Elections (Northern Ireland) Regulations 2004; Article 61, Scottish Parliament (Elections etc) Order 2010; Article 65, Representation of the People (National Assembly of Wales) Order 2007 and Schedule 1, Northern Ireland Assembly (Elections) Order 2001 (applying section 91 of the RPA 1983). Further guidance is available from the Electoral Commission website: http://www.electoralcommission.org.uk/

Example

A campaigner working for a political party canvasses door to door to encourage support in an upcoming Scottish Parliament election. She uses a list of particular individuals who have been identified as likely swing voters who ought to be targeted. The next individual she chooses to target is Lee Smith. She knocks on the door of the house where Lee Smith lives with his brother Adam Smith. A man answers the door. She introduces herself stating the party she works for. The man tells the campaigner that he does not wish to speak to her and tells her that he does not wish to be contacted by the party again and promptly shuts the door.

The campaigner has been appropriately trained on the right to object but is not sure whether the man who answered the door is Lee Smith or not. She is therefore not sure whether it is a valid request.

In this example, although the right to object would legally only apply to Lee Smith as he was the one subject to the processing, the campaigner should be cautious and add both individuals to their suppression list.

How do we carry out political campaigning by electronic mail?

You need to comply with regulation 22 of PECR, if you are campaigning by electronic mail, in addition to complying with the GDPR.

The term 'electronic mail' has an intentionally broad meaning. It is defined as:

"any text, voice, sound or image message sent over a public electronic communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient and includes messages sent using a short message service".

This definition includes:

- emails;
- texts;
- picture messages;

- video messages;
- voicemails;
- direct messages via social media; or
- any similar message that is stored electronically.

When you are sending political campaigning messages by electronic mail, you must:

- not send electronic mail marketing to individuals, unless they have **specifically consented** to receiving electronic mail from you;
- not disguise or conceal your identity; and
- provide a valid contact address so they can opt out or unsubscribe. It must be as easy to withdraw consent (opt out or unsubscribe) as it is to give consent.

For the avoidance of doubt, the 'soft opt in' does not apply to political campaigning messages. See our direct marketing code for further information (currently being drafted).

Electronic mail does not include online advertising through social media and other online platforms, even where directed at particular individuals. See section online advertising and use of social media for more information on the use of these campaigning methods.

However, electronic mail does include direct messages sent through social media or other online platforms that are stored electronically. Examples include messaging applications and web based email platforms.

Can we carry out viral political campaigning by electronic mail?

The direct marketing by electronic mail rules also apply to asking individuals to send your political messages to their family and friends. This is often known as viral marketing or 'tell a friend' campaigns. You still need to comply even if you do not send the messages yourself, but instead **instigate** individuals to send or forward these.

This includes asking or suggesting that an individual forwards your messages to their friends without providing a reward or benefit. This still means that you are instigating the sending of the message and you therefore need to comply with PECR and obtain consent. You do not necessarily have to incentivise an individual to pass on the message.

As you have no direct contact with the individual who is receiving your direct marketing, it is impossible for you to collect valid consent.

It is likely therefore that viral marketing and 'tell a friend' campaigns breach PECR.

However you are not responsible if the individual chooses, with no encouragement from you, to send their family or friends a link to a product from your website or details of your promotion or campaign.

Can we carry out political campaigning by live call?

If you are campaigning by live telephone call, you need to comply with Regulation 21 of PECR, in addition to the GDPR.

You can call any individual who has specifically consented to receive marketing calls from you.

You can also make live calls without consent to a number if it is not listed on the Telephone Preference Service (TPS) – unless they have already told you that they do not want to be called.

In practice, this means you need to screen most call lists against the TPS register. You also need to keep your own 'do not call' list of people who object or opt out, and screen against that as well.

You must ensure that you screen against the TPS when undertaking telephone campaigns.

Where you are permitted to telephone an individual, you must:

- identify your organisation at the start of the call;
- allow your number (or an alternative contact number) to be displayed to the person receiving the call;
- if requested, provide an address or number where you can be reached free of charge to object to marketing; and
- record and respect any objection to marketing made by the individual at the time of the call.

Can we carry out political campaigning by automated call?

The rules on automated marketing calls are in Regulation 19 of PECR and are stricter than for live calls. This is when a recorded message is played to the person who answers the phone. It is worth noting that many

individuals have told the ICO that they consider automated calls to be extremely intrusive and even disturbing.

There are systems available that allow calls to be partly automated and partly live. For example, where there is an automated message which is then connected to a live call if the individual presses a particular key. The rules on automated calls still apply in these circumstances.

If you wish to use automated calling you need the specific consent of the individual. Obtaining consent to make live voice calls is not sufficient and the automated nature of the calls must be clear in the information you give to individuals to inform their decision.

All automated marketing calls must include the name of your organisation and a contact address or Freephone number, and must allow your number (or alternative contact details) to be displayed to the person receiving the call.

The ICO has issued a number of enforcement notices to political parties for the use of automated calls without appropriate consent. We view this with great concern. You must ensure you comply with the rules.

Further reading

For more information on electoral law see the Electoral Commission's website.

For general guidance on PECR see our Guide to Privacy and Electronic Communications Regulations.

For general guidance on key data protection concepts see our Guide to Data Protection.

Political campaigning in the online world

At a glance

- Any use of cookies or similar technologies for the purposes of online advertising requires prior consent under Regulation 6 of PECR – you cannot rely on any other lawful basis for the setting of cookies for this purpose.
- Similarly, any other third party plugin your online services use – such as pixel tags from a social media platform – also requires prior consent under PECR where it is used for the purpose of facilitating the targeting of political messaging.
- If you use social media and/or online advertising technologies to target political messaging, you must be very clear about what personal data is involved, the tools and techniques you are using, and how you provide privacy information to individuals.
- When using a social media platform to target political messaging, you are likely to be a joint controller with the platform, and therefore need to establish who is responsible for what aspects of the processing, and ensure you have an appropriate arrangement in place with the platform.
- If your campaign uses a third party platform, you need to take steps to ensure that any processing it undertakes is in line with data protection requirements.

In more detail

- Are we joint controllers with social media platforms?
- What should we consider when using campaigning platforms?

What's different in the online world?

In recent years there has been a sharp rise in the use of social media platforms, online advertising and third-party campaigning platforms in political campaigning.

In the online world, the tools and techniques and amount of personal data available differ substantially from traditional advertising methods, and have a greater potential impact on individual rights as a result.
One of the most obvious examples is the concept of 'micro-targeting'. This is where you select your messages and/or your intended audience according to the perceived characteristics, interests or preferences of the individuals concerned.

The type and volume of processing that you can undertake in the online world means that you are highly likely to have to undertake a DPIA prior to the processing – particularly if you are using the available tools and techniques for political campaigning. This is because the processing may involve:

- the use of new technologies;
- profiling of individuals on a large scale;
- combining, comparing or matching personal data obtained from multiple sources;
- personal data that has not been obtained directly from individuals, where you consider that compliance with Article 14's transparency obligations are impossible or involve disproportionate effort – known as 'invisible processing';
- tracking an individual's geolocation or behaviour; and
- the use of personal data of vulnerable individuals for marketing purposes, profiling or other automated decision making.

These are all examples of processing likely to result in a high risk to the rights and freedoms of individuals, for which DPIAs are required.

Further reading

See our guidance on DPIAs in the Guide to the GDPR for more information. You should also read the examples of high risk processing, where DPIAs are legally required.

Does online political messaging count as direct marketing?

In the vast majority of cases, delivering political messages online through social media platforms and online advertising technologies involves the processing of personal data and also constitutes direct marketing (in cases where it is directed to an individual). This means that you need to comply with data protection law.

If you use cookies and similar technologies – which most online advertising do – then PECR also applies, whether or not this use involves the processing of personal data or constitutes direct marketing.
If this is the case, you need to consider PECR first, because its rules particularise data protection law in certain areas, such as cookies.

Not all online advertising may be covered by data protection law and PECR. For example if:

- the method of delivery for the advertisement does not involve the storage of information, or access to information stored, on user devices, then Regulation 6 of PECR is not engaged; and

- the advertisements themselves do not involve the processing of personal data, ie they are not based on any interests or behaviours, or any other information about an individual – then they may not involve the GDPR.

Further reading

See the Guide to PECR and the Guide to the GDPR for more information.

How does PECR apply to political campaigning and online advertising?

PECR has specific rules about the use of cookies or similar technologies (including tracking pixels and device fingerprinting techniques). These cover any technology used to store information or access stored

information on a user's device, including:

- first-party and third-party advertising cookies;
- device fingerprinting techniques;
- tracking pixels and plugins from third parties, such as social media platforms; and
- other third party tracking technologies.

Your website may incorporate some or all of the above, depending on the decisions that you take when building and developing it. They facilitate the tracking and targeting of individuals in the online (and, increasingly, offline) environment.

If your online service uses cookies, you need to understand that you are not only using cookies to target individuals for your own purposes but also allowing third parties to do the same.

Example

A political party's website incorporates a number of third party advertising technologies, including cookies, tracking pixels and social media plugins. When an individual visits the website, these technologies process information about that individual's device, as well as their personal data. This means that both the website and a variety of third parties may process this information, and potentially the individual's personal data as well – so both PECR and the GDPR may apply.

In the case of a social media tracking pixel, the individual's visit to the website can lead to the social media platform adding that individual to an audience and targeting them with messaging when they visit the platform.

If you are planning to use cookies to show your users political messaging (whether or not they are targeted on the basis of those users' personal data), you need to ensure that you comply with Regulation 6 of PECR by:

- providing your users with clear and comprehensive information about the purposes of the cookies you intend to use; and

- getting their consent, which must be to a GDPR standard (see the section on consent).

Regulation 6 of PECR contains two exemptions from these requirements where:

- the use of the cookie or similar technology is necessary for the sole purpose of transmission of a communication; or

- the cookie or similar technology is 'strictly necessary' for the provision of the online service the user requests (ie your website, in this case).

However, in the context of online advertising, tracking technologies and social media plugins, neither of these exemptions apply. This means that you need to get consent from your users for any cookie or similar technology that you use for these purposes – whether the cookie is yours, or that of a third party.

You must also rely on the consent lawful basis. You cannot rely on the other lawful bases from the GDPR for your use of cookies. For example, 'public task – democratic engagement' or 'legitimate interests'.

Further reading

Read our guidance on the use of cookies in the Guide to PECR. We have also published more detailed guidance on how you can comply with PECR when using cookies and similar technologies.

What else should we consider when using online advertising?

In order to provide users with advertising more relevant to their interests and behaviours, online advertising can track them in a variety of ways – across the web, across devices, or both.

In addition to ensuring that you comply with PECR's requirements, there may be further implications if you decide to use online advertising. Whilst these apply generally, in political campaigning you also need to consider the extent to which online advertising involves the processing of special categories of data.

You should also remember that even if you do obtain valid consent for PECR, if you are also processing personal data, you must also comply with the applicable requirements of the GDPR.

The online advertising ecosystem is complex and brings a number of potential issues that you need to consider if you intend to use it for

political campaigning. You should ensure that you are aware of all of these, including how personal data is processed throughout the entire process of advertisement selection and delivery.

For example, there are a variety of methods through which you can advertise online, ranging from contextual advertising (where the content of the page that the user views determines the advert they see) up to complex ecosystems involving automated transactions to display adverts in the time it takes for a webpage to load.

Example

Real-time bidding (RTB) is a type of online advertising that involves open auctions, where advertisers bid for an ad slot that a user is viewing. As the webpage loads in the user's browser, information about the user's device, and the user themselves, is collected through the use of cookies and similar technologies, such as device fingerprinting.

The information is then sent into a complex ecosystem of hundreds of different organisations – from advertisers to ad exchanges and more – where a bidding process takes place. In order to take part in the auction, any one of these parties must process the data collected about the user. Only one will 'win' the auction, and the resulting advert is then displayed in the user's browser or mobile app.

This entire process takes place in milliseconds.

When considering the use of online advertising techniques in political campaigns, you need to statisfy yourself that:

- you have prior consent for the use of cookies, as required under PECR;
- any processing of special category data has the user's explicit consent;
- you comply with the requirements for your lawful basis for processing;
- you undertake a DPIA to appropriately assess and mitigate the risks;

- the privacy information you provide is clear so that individuals know what data you want to process, for what purposes, and with whom you intend to share it; and

- you have appropriate arrangements in place where processors act on your behalf, or where you are joint controllers with another party.

Further reading

Read our update report into adtech and real-time bidding (PDF) for more specific information about data protection considerations in respect of this type of online advertising.

What are the considerations if we use social media platforms to target messages?

Social media platforms process large amounts of personal data about their users' behaviour and interactions. Generally, this falls into three main types of personal data:

- Personal data the users provide, such as their account profile information. This may for example include their email address, certain demographic information etc.

- Personal data observed through use of the platform – social media platforms process personal data about how their users interact with the service, such as:

    - their activity on the platform (eg content they have generated);
    - the devices they use to access the platform;
    - personal data obtained by use of a third party application developer;
    - data collected by third-party websites that include the platform's plugins;
    - data collected through other third parties the user interacts with; and
    - data collected through other services the social media platform operates.

- Personal data inferred about the user – inferred data in this context is personal data created on the basis of data provided by individuals or observed by their use of the service. For example, social media platforms generate 'insights' based on provided and observed data which constitute inferences about the characteristics and interests of the user.

The platforms may enable the targeting of individuals based on all of the above types. When you decide to use social media platforms to target political messaging at individuals, it is therefore important to understand that many different data sources are likely to be used for this purpose. You need to be very clear about what data you are using and why.

What are the considerations if we target social media users based on data we already have?

Social media platforms offer 'list-based' targeting tools that allow you to send political messages to users of the platform. This list-based targeting is where you upload personal data you already have, such as a list of email addresses, to a platform. It then matches this data with its own userbase. Any user that matches the uploaded list is then added into a group that you then target your messaging to on the platform itself. These tools are generally known as 'audiences' although the precise term can differ, depending on the platform. Examples include Facebook Custom Audiences or Linkedin Contact Targeting.

Generally, the process of uploading the list to the platform involves a technique known as 'hashing'. The list is hashed when you upload it, and compared to a list of hash values in the platform's database. The audience is built on any matching hashes. Whilst this provides a level of assurance regarding the security of the processing, this does not take into account all data protection considerations and is not an anonymisation technique.

If you use list-based tools, you also need to:

- assess whether special category data such as political opinions can be inferred from the list you provide. Although your creation of a list for uploading to the platform may not by itself represent the processing of special category data, the further use of the list by you and the platform to target political messaging may be;

- inform individuals and be transparent about this processing so that they fully understand you will use their personal data in this way.

For example, that you will use their email addresses to match them on social media for the purposes of showing them political messaging; and

- take into account any objections. If an individual has objected to you using their personal data for direct marketing purposes you cannot use their data to target them on social media. You also cannot process their data to help you find similar people to target, because using their data in this way is still for direct marketing purposes.

What are the considerations if we target similar individuals on social media?

Social media platforms also offer you the ability to build other audiences, based on the characteristics of an original audience that you've created using a list-based tool. These are commonly known as 'lookalike' audiences, although again the terminology may change depending on the platform.

These groups generally comprise individuals that you have not previously engaged with, but who 'look like' your list-based audience, ie they are individuals with similar interests, behaviours or characteristics to the kinds of people you want to target.

When you create this sort of target group, the social media platform uses insights data it has on other users of its platform to find people who match the interests and behaviours of people you want to target. Additionally, the widespread use of social media plugins and tracking pixels on other websites can be used to add users into this sort of audience – so you need to be aware that this can take place and have considered the data protection implications.

The data protection implications of this activity are complex. Whilst the social media platform undertakes the majority of the processing activities, you are the organisation that instigated this processing and provided the platform with the initial dataset (ie your original list-based audience). Both you and the platform are joint controllers for this activity.

However, you do not have any direct relationship with the individuals that are being added to this type of audience. You therefore need to be satisfied that the social media platform has taken all necessary steps to provide the appropriate information to individuals. This is particularly the case because this type of audience can change according to people's

behaviour or interests.

You also need to ensure you appropriately inform individuals who have provided information to you that you will process their data to create these other audiences. As mentioned above, if individuals have objected to the use of their personal data for marketing purposes, you also need to ensure that you do not use their data for the creation of a 'lookalike' audience.

Are we joint controllers with social media platforms?

Yes. When using a third party to target political messaging at individuals, you act as a joint controller with that organisation. This is because you are jointly deciding the purposes and means of the processing. For example:

- you decide to have a presence on the social media platform;
- the platform in turn provides a number of tools and techniques that you can use to target messaging at its users, both on and off the platform; and
- you create 'audiences' on the basis of the tools and personal data available.

You are also a joint controller even if you are just using the platform's tools to generate aggregate data about how your users interact with your social media presence.

In joint controller relationships, both you and your fellow controller have responsibility for complying with the GDPR's requirements. However, this does not mean you have the same responsibility for all aspects of the processing – but you do need to agree and fully understand who is responsible for what. This means working with any third party you use to make sure there are no gaps in compliance.

Article 26 of the GDPR specifies the requirements for joint controller situations. These are no different when you decide to use a social media platform to target political messaging. See our guidance on controllers and processors for further information on these requirements.

In some cases, the social media platform may make available a 'standard' joint controller arrangement. These may be appropriate for the requirements of Article 26, but you need to ensure this is the case.

Further reading – ICO guidance

Read our guidance on controllers and processors and contracts and liabilities in the Guide to the GDPR.

What should we consider when using campaigning platforms or other third party tools?

You can also use a variety of third-party digital campaigning platforms to host data and enable political engagement. They can also provide tools for this engagement, such as emails, fundraising and links to social media.

Using these platforms can be a way of managing a political campaign, and the personal data involved, without needing to build your own infrastructure. However, you need to ensure that your arrangements with these platforms are clear and transparent. For example, if the campaigning platform acts as your processor, it must only act on your instructions.

This is crucial because in some cases the platform's service offerings may essentially determine what techniques are used for your particular campaign. For example:

- a 'basic' service level could include the creation of a database of individuals, a website for your campaign, electronic mail marketing, and payment services (eg if you accept donations); and

- a higher service level could include the above, plus additional marketing and engagement tools (eg SMS messaging along with email or other more advanced features), campaign dashboards, membership and ticketing functionalities, and data analytics services.

Many of these platforms also create customised service packages depending on the specifics of your campaign.

Your use of these platforms must comply with data protection law and PECR, so it is vital that you know and can evidence:

- what data you are going to use (and provide to the platform);

- how you are going to comply with legal requirements when using the platform's tools to target individuals with political messages;

- where the platform hosts the data, ie will data about your campaign or your supporters be stored outside the European Economic Area, and if so, what steps have you taken to ensure compliance.

Additionally, these platforms are used by any number of political campaigning organisations across many election periods – including in different countries. They can therefore process a large amount of personal data from multiple political campaigns, and you need to establish how the platform holds not just your data, but that from any other organisation.

Depending on the available services, campaigning platforms can also undertake certain types of processing on your behalf. For example, they:

- may match the data you provide with data available publicly (eg on social media profiles);

- could use other techniques such as 'web scraping'. This is an automated process whereby content – which can include personal data – is 'scraped' from a web page and stored for further processing; and

- are likely to offer a 'suite' of tools to enable online direct marketing.

In the case of data matching and web scraping, data protection law does not stop you processing publicly available personal data, but you must do it in compliance with the GDPR and PECR. For example, if you 'scrape' publicly-available personal data from social media profiles, you become the controller for that data. See the section on collecting data from social media platforms for more information.

If you intend to use campaigning platforms or other third party tools, then you need to incorporate this into your campaign's DPIA. If the platform is your processor, it can assist you in doing this.

Further reading

For general guidance on PECR see our Guide to Privacy and Electronic Communications Regulations.

For general guidance on key data protection concepts see our Guide to Data Protection.

After a campaign

At a glance

- You should carry out a review of the data you have gathered and processed during a campaign.
- You may be able to use personal data from one campaign to another, but you need to consider this carefully and in compliance with data protection law.
- If your organisation is disbanding after a campaign, you must destroy personal data securely and in certain circumstances should use a third party to conduct an audit of how you processed the data.

In more detail

Introduction

Whether a political party, campaign group or candidate, it is important you carry out a review of the data you have gathered and processed during a campaign. This is important to help you learn any compliance lessons for the future about what went well and what didn't. It is also important to assess what information you need to retain both for future campaigns and for audit purposes.

The answers to these will be different depending on your type of organisation and your circumstances. In particular they will differ depending on whether your organisation has disbanded or not following the campaign. This is the case with many campaign groups and others campaigning in particular referenda or elections.

Can we use personal data from one campaign to another?

In general, it can be acceptable to keep personal data to use from one campaign to another, but you must consider:

- whether the personal data is necessary for future campaigns;
- whether it would be in individuals' reasonable expectations that you keep the data;
- what you told individuals at the point of collection;
- whether the nature of future campaigns could amount to processing for a different purpose, eg a referendum campaign on EU membership to a local election (see section on purpose limitation);
- how long you have retained the data and whether it is still adequate, relevant or accurate; and
- whether you are able to keep the data securely and whether keeping the data creates any unjustifiable risk of it being subject to unauthorised disclosure.

You should consider carrying out a DPIA to help you identify and mitigate the risks of retaining the data as well as demonstrating your compliance.

What do we need to do if our organisation is to disband?

If your organisation is disbanding then you should ensure that you:

- securely destroy personal data that you no longer need for audit purposes;
- mitigate the risk as far as possible of employees, secondees or volunteers being able to take personal data for use in other campaigns or for other unauthorised purposes - for example, ensuring you have robust exit procedures;
- carry out due diligence to ensure that any processors have securely destroyed all personal data that they were processing on your behalf; and
- do not share any personal data with any other controller unless you are able to do so in accordance with data protection law (see our data sharing code of practice for further information – currently being drafted).

In addition, if your organisation is disbanding, it is advisable to use a third party to conduct an audit to create a clear record of how you processed data both during and after the campaign including what was deleted and when. This is particularly relevant to campaigners that have been operating at scale in a national referendum using comprehensive datasets. This helps to demonstrate that you have complied with the law and in turn encourages public trust in our democratic system.

Further reading

For general guidance on key data protection concepts see our Guide to Data Protection.

At a glance checklists

[It is anticipated 'at a glance' checklists will be included in the final version of this framework code.]