Information Commissioner's Office

Direct marketing code of practice

Draft code for consultation

ico.
Information Commissioner's Office

Contents

Foreword

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

Summary

About this code

- This is a statutory code of practice prepared under section 122 of the Data Protection Act 2018. It provides practical guidance for those conducting direct marketing or operating within the broader direct marketing ecosystem. It explains the law and provides good practice recommendations. Following the code along with other ICO guidance will help you to comply with the GDPR and PECR.

Does this code apply to us?

- This code applies if you process personal data for direct marketing purposes.

- Direct marketing includes the promotion of aims and ideals as well as advertising goods or services. Any method of communication which is directed to particular individuals could constitute direct marketing. Direct marketing purposes include all processing activities that lead up to, enable or support the sending of direct marketing.

Planning your marketing: DP by design

- A key part of the GDPR is accountability and you must be able to demonstrate your compliance. You must consider data protection and privacy issues upfront when you are planning your direct marketing activities. Depending on your direct marketing activity you may be required to conduct a DPIA.

- Generally speaking the two lawful bases most likely to be applicable to your direct marketing purposes are consent and legitimate interests. However if PECR requires consent then in practice consent will be your lawful basis under the GDPR. If you intend to process special category data for direct marketing purposes it is likely that the only Article 9 condition available to you will be 'explicit consent'.

- In most cases it is unlikely that you will be able to make using an individual's data for direct marketing purposes a condition of your service or buying your product.

- It is important to keep personal data accurate and up to date. It should not be kept for longer than is necessary. Children's personal data requires specific protection in regard to direct marketing.

Generating leads and collecting contact details

- Transparency is a key part of the GDPR and as part of this individuals have the right to be informed about your collection and use of their personal data for direct marketing purposes.

- If you collect data directly from individuals you must provide privacy information at the time you collect their details. If you collect personal data from sources other than the individual (eg public sources or from third parties) you must provide privacy information within a reasonable period of obtaining the data and no later than one month from the date of collection. Your privacy information must be in clear and plain language and easily accessible.

- If you are considering buying or renting direct marketing lists you must ensure you have completed appropriate due diligence.

Profiling and data enrichment

- Profiling and enrichment activities must be done in a way that is fair, lawful and transparent. If you are considering using profiling or enrichment services you must ensure you have completed appropriate due diligence.

- If you are carrying out solely automated decision making, including profiling, that has legal or similarly significant effects on individuals then there are addition rules in the GDPR that you must comply with. If you want to profile people on the using their special categories of data you must have their explicit consent to do this.

- If you use non-personal data such as assumptions about the type of people who live in a particular postcode to enrich the details you hold about an individual it will become personal data.

- In most instances, buying additional contact details for your existing customers or supporters is likely to be unfair unless the individual has previously agreed to you having these extra contact details.

- You are unlikely to be able to justify tracing an individual in order to send direct marketing to their new address – such tracing takes away control from the individual to be able to choose not to tell you their new details.

Sending direct marketing messages

- No matter which method you use for sending direct marketing messages the GDPR will apply when you are processing personal data.

- The direct marketing provisions in PECR only apply to live and automated calls, electronic mail (eg text and emails) and faxes. The electronic mail 'soft opt-in' only applies to the commercial marketing of products and services, it does not apply to the promotion of aims and ideals.

- PECR may apply differently to business to business marketing depending on the type of subscriber you want to contact.

- PECR may still apply even if you ask someone else to send your electronic direct marketing messages.

Online advertising and new technologies

- Individuals may not understand how non-traditional direct marketing technologies work. Therefore it is particularly important that you are clear and transparent about what you intend to do with their personal data.

- Individuals are unlikely to understand how you target them with marketing on social media so you must be upfront about targeting individuals in this way.

- If you are planning to use cookies or similar technologies for direct marketing purposes you must provide clear and comprehensive information to the user about these and gain their consent (which must be to the GDPR standard).

- Regardless of what technology or contact method you consider, you still need to comply with the GDPR and PECR. If you are using new technologies for marketing and online advertising, it is highly likely that you require a DPIA.

Selling or sharing data

- If you are planning on selling or sharing personal data for direct marketing purposes you must ensure that it is fair and lawful to do so. You must also be transparent and tell people about the selling or sharing.

Individual rights

- As well as the right to be informed, the rights to objection, rectification, erasure and access are the most likely to be relevant in the direct marketing context.

- The right to object to direct marketing is absolute. This means if someone objects you must stop processing for direct marketing purposes (which is not limited to sending direct marketing). You should add their details to your suppression list so that you can screen any new marketing lists against it.

Exemptions

- The DPA 2018 contains a number of exemptions from particular GDPR provisions and these add to the exceptions that are already built into certain GDPR provisions. There are no exemptions that specifically apply to processing for direct marketing purposes.

- PECR contains very few exemptions. The two exemptions in Regulation 6 from the requirement to provide clear and comprehensive information and gain consent for cookies and similar technologies do not apply to online advertising, tracking technologies or social media plugins.

Enforcement of this code

- The ICO upholds information rights in the public interest. We will monitor compliance with this code through proactive audits, will consider complaints and enforce the direct marketing rules in line with our Regulatory Action Policy. Adherence to this code will be a key measure of your compliance with data protection laws. If you do not follow this code, you will find it difficult to demonstrate that your processing complies with the GDPR or PECR.

About this code

At a glance

This is a statutory code of practice prepared under section 122 of the Data Protection Act 2018. It provides practical guidance for those conducting direct marketing or operating within the broader direct marketing ecosystem. It explains the law and provides good practice recommendations. Following the code along with other ICO guidance will help you to comply with the GDPR and PECR.

In more detail

Who is this code for?

This code is for anyone who intends to conduct marketing that is directed to particular individuals or anyone that operates within the broader direct marketing ecosystem. For example, if you are processing for direct marketing purposes and use or offer profiling, data enrichment, or list brokering services.

You will be caught by the direct marketing rules if you are using data with the intention to market, advertise, or promote products, services, aims or ideals. For example:

- commercial businesses marketing their products and services;
- charities and third sector organisations fundraising or promoting their aims and ideals;
- political parties fundraising or canvassing for votes;
- public authorities promoting their services or objectives; or
- organisations involved in buying, selling, profiling or enriching personal data for direct marketing purposes.

This code assumes familiarity with key data protection and PECR terms and concepts. If you need an introduction to either, including key concepts – you should refer to our Guides to Data Protection and PECR.

What is the purpose of this code?

The code helps you to comply and demonstrate that you comply with data protection and e-privacy rules when you are processing data for direct marketing purposes or conducting direct marketing campaigns.

How does this code support data protection and e-privacy compliance?

The UK data protection regime is set out in the Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulation (GDPR). This regime requires you to take a risk-based approach when you use people's data, based on certain key principles.

The e-privacy rules in the UK are set out in the Privacy and Electronic Communications Regulation 2003 (PECR). This regime sets out more detailed privacy rules in the area of electronic marketing communications and cookies and similar technologies. It is broader than the GDPR in the sense that it applies even if you are not processing any personal data.

There is some overlap between the data protection and e-privacy regimes, and they use some of the same concepts and definitions – including the definition of consent. In some circumstances you will find your direct marketing is covered by both GDPR and PECR but on other occasions you may find that only one of these applies.

This code looks at both regimes and takes you through the steps to comply with the rules.

The regulatory framework

The Commissioner regulates data protection and e-privacy laws. However there are other rules and industry standards affecting direct marketing which are regulated by other bodies.

Compliance with other regulation and industry standards can assist in you demonstrating that your processing of personal data for direct marketing purposes is lawful and fair.

Other resources outside this code

Ofcom regulates the Communications Act 2003, which covers the improper use of a public electronic communications network, including making silent or abandoned calls. Ofcom has powers to issue fines up to £2 million for persistent misuse.

The Competition and Markets Authority (CMA) and local trading standards offices enforce The Consumer Protection from Unfair Trading Regulations 2008 which prohibit a number of unfair, misleading or aggressive marketing practices, including 'making persistent and unwanted solicitations by telephone, fax, email or other remote media'.

The Advertising Standards Authority (ASA) enforces the UK Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing (the CAP code). The CAP code contains rules which all advertisers, agencies and media must follow. It covers the content of advertising material, and specific rules on certain types of advertising (eg advertising to children, advertising certain types of products, or distance selling).

The Data & Marketing Association (DMA) (formally the Direct Marketing Association) publishes the DMA code, setting standards of ethical conduct and best practice in direct marketing. Compliance is mandatory for all DMA members and the code is enforced by the independent Direct Marketing Commission.

The Fundraising Regulator is the independent, non-statutory body that regulates fundraising across the charitable sector in England, Wales and Northern Ireland. It sets standards for fundraising including in its Code of fundraising practice.

You should always ensure that you are familiar with all laws and standards of conduct that apply to you.

What is the status of this code?

What is the legal status of the code?

This is a statutory code of practice prepared under section 122 of the DPA 2018:

"(1) The Commissioner must prepare a code of practice which contains—

> (a) practical guidance in relation to the carrying out of direct marketing in accordance with the requirements of the data protection legislation and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 2003/2426), and
>
> (b) such other guidance as the Commissioner considers appropriate to promote good practice in direct marketing."

Section 122(5) of DPA 2018 states that 'good practice in direct marketing' means:

> "such practice in direct marketing as appears to the Commissioner to be desirable having regard to the interests of data subjects and others, including compliance with the requirements mentioned in subsection (1)(a)"

This code was laid before parliament on **[DATE]** and issued on **[date 40 days after laid, ignoring parliamentary recess]** under section 125 of the DPA 2018. It comes into force on **[date 21 days after issue]**.

The code contains practical guidance on how to carry out direct marketing fairly and lawfully, and how to meet your accountability obligations. It does not impose any additional legal obligations that go beyond the requirements of the GDPR or PECR, but following the code will ensure you comply with those obligations. It also contains some optional good practice recommendations, which do not have the status of legal requirements but aim to help you adopt an effective approach to data protection compliance.

In accordance with section 127 of the DPA 2018, the Commissioner must take the code into account when considering whether those engaging in direct marketing purposes have complied with its obligations under the GDPR or PECR. In particular, the Commissioner will take the code into account when considering questions of fairness, lawfulness, transparency and accountability under the GDPR, and in the use of her enforcement powers.

The code can also be used in evidence in court proceedings, and the courts must take its provisions into account wherever relevant.

What happens if we do not comply with the code?

If you do not comply with the guidance in this code, you may find it more difficult to demonstrate that your processing for direct marketing purposes is fair, lawful and accountable and complies with the GDPR and PECR.

We can take action against you if you send direct marketing or process personal data for direct marketing purposes in breach of this code and this results in an infringement of the GDPR or PECR.

Tools at our disposal include assessment notices, warnings, reprimands, enforcement notices and penalty notices (administrative fines). For serious infringements of the data protection principles, we have the power to issue fines of up to €20 million or 4% of your annual worldwide turnover, whichever is higher.

There is no penalty if you fail to adopt good practice recommendations, as long as you find another way to comply with the law.

For more information see the Enforcement of this code section.

What is the status of 'further reading' or other linked resources?

Any further reading or other resources which are mentioned in or linked from this code do not form part of the code. We provide links to give you helpful context and further guidance on specific issues, but there is no statutory obligation under the DPA 2018 for the Commissioner or courts to take it into account (unless it is another of our statutory codes of practice).

However, where we link to other ICO guidance, that guidance inevitably reflects the Commissioner's views and informs our general approach to interpretation, compliance and enforcement.

We may also link to relevant guidance provided by the European Data Protection Board (EDPB), which is the independent body established to ensure consistency within the EU when interpreting the GDPR and taking regulatory action.

How do we use this code?

The code takes a life-cycle approach to direct marketing. It starts with a section that looks at the definition of direct marketing to help you decide if this code applies to you. It then contains separate sections on planning your marketing, collecting data, delivering your marketing messages, working with others, and individuals' rights.

As well as having examples throughout, the code has a glossary of terms in its annex. Outside of this code the ICO has produced practical tools and resources, including checklists, to help you work through your compliance with the direct marketing rules.

The code is designed to reflect all of the different stages that might be involved in end-to-end marketing activities. In practice, the sections that you need to read depend on the type of activities you engage in. You may not

need to read every section, but you should always start with the section on planning and DP by design.

The key recommendations of this code are highlighted in the summary section at the beginning of this code and in the 'at a glance' boxes at the start of each section – but you need to read the full section in order to understand the detail.

How should charities and not-for-profits use this code?

In general the direct marketing rules are the same for charities and not-for-profit organisations as for private and public sector organisations. Therefore you need to read all the sections of the code that relate to your activities. Where relevant, any issues that are specific to your sector are discussed along with examples.

Further reading outside this code
See our separate guidance on:
The Guide to Data protection
The Guide to PECR

Does the code apply to us?

At a glance

This code applies if you process personal data for direct marketing purposes.

Direct marketing includes the promotion of aims and ideals as well as advertising goods or services. Any method of communication which is directed to particular individuals could constitute direct marketing. Direct marketing purposes include all processing activities that lead up to, enable or support the sending of direct marketing.

In more detail

What is the definition of direct marketing?

The definition of direct marketing is in section 122(5) of the DPA 2018:

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

This definition also applies for PECR. This is because regulation 2(2) of PECR provides that any undefined expressions have the same meaning as in the UK data protection regime (formerly the Data Protection Act 1998, now the DPA 2018).

Relevant provisions in the legislation

PECR – see Regulation 2(2)
DPA 2018 – see Schedule 19 paragraph 430 and paragraph 432(6)

What are direct marketing purposes?

GDPR and PECR do not define the term 'direct marketing purposes', but clearly it is intended to be wider than simply sending direct marketing communications. The focus is on the purpose of the processing, not the activity. Therefore, if the ultimate aim is to send direct marketing communications, then all processing activities which lead up to, enable or support sending those communications is processing for direct marketing purposes, not just the communication itself.

Therefore, if you are processing personal data with the intention that it is used for communicating direct marketing by you or a third party you are processing for direct marketing purposes. For example, if you are collecting personal data from various sources in order to build up a profile on an individual – such as the products they buy, the services they like to use, or the causes they are likely to support – with the intention that this is used to target advertising at them, whether by you or by a third party. Other examples include:

- lead generation;
- list brokering;
- data enrichment;
- data cleansing, matching or screening;
- audience segmenting or other profiling; and
- contacting individuals to ask them for consent to direct marketing.

Disclosing the data to third parties for them to use for their own direct marketing also constitutes direct marketing purposes.

Example
A hotel sends an email to its previous guests asking them if they would like to consent to receiving its special offers and discounts. Whilst this email does not itself contain any of these discounts or offers, it is still being sent for direct marketing purposes.

Direct marketing purposes include trying to generate leads by sending mass texts, emails or automated calls or cold-calling numbers registered with the Telephone Preference Service (TPS), even if these messages do not contain any sales or promotional material. Therefore if you intend to do this you must ensure that you have complied with PECR.

What is 'advertising or marketing material'?

The DPA 2018 and PECR do not clarify what is meant by 'advertising or marketing material'. However it is interpreted widely and covers any advertising or marketing material, not just commercial marketing. For example it includes the promotion of aims and ideals as well as advertising goods or services. This wide interpretation acknowledges that unwanted, and in some cases nuisance, direct marketing is not always limited to commercial marketing.

This is a long standing interpretation which was supported by an Information Tribunal in 2006:

Example
The Scottish National Party (SNP) made a series of automated campaigning calls to selected Scottish voters in the lead-up to the 2005 general election. PECR states that automated direct marketing calls can only be made with prior consent, but the SNP claimed that the rules on direct marketing did not apply to them - only to commercial organisations. The case went to the Information Tribunal.

In the Scottish National Party v Information Commissioner (EA/2005/0021, 15 May 2006), the Tribunal agreed that the direct marketing rules in PECR and the (now superseded) Data Protection Act 1998 covered the promotional activities of both commercial and not-for-profit organisations, and so political parties had to comply with PECR when carrying out campaigning calls.

All promotional material falls within the definition. Examples of material promoting aims and ideals could be about:

- fundraising;
- political parties or candidates; or
- the use of public services.

Often it is very obvious that a message contains advertising or marketing material but sometimes it is not as clear cut. In these circumstances the tone, content and the context of the message is likely to be important. The question is whether the communication is:

- promotional in nature – does it advertise goods or services or otherwise promote the organisation itself or its interests?; or
- more neutral and informative in nature – does it seek simply to provide information the individual needs in the context of the existing relationship?

You should think about why you want to communicate with individuals – for example to try to influence thought or behaviour, or encourage an action as this will help you in deciding if the message is direct marketing. See the section What are service messages? for further information.

What type of 'communications' are covered?

The definition of direct marketing covers any means of communication, although PECR rules only apply to specific types of electronic communication (eg phone calls, emails, text messages, in-app messaging, push notifications).

Online behavioural advertising and some types of social media marketing are not classed as electronic mail under PECR but these are still direct marketing communications.

The definition is designed to be technology neutral and is therefore not limited to traditional forms of direct marketing such as telesales or mailshots, but can extend to online marketing, social networking or any other emerging channels of communication or approach.

Any background processing that takes place to enable or target those communications is also processing for direct marketing for purposes. See the section above What are direct marketing purposes? for further information.

What does 'directed to' mean?

The key element of the definition is that the marketing material must be 'directed to' particular individuals. For example:

- personally addressed post;
- calls to a particular telephone number;
- emails sent to a particular email account;
- online advertising that is targeted to a particular individual; and
- advertising on social media that is targeted to a particular individual.

Indiscriminate blanket marketing does not therefore fall within this definition of direct marketing. For example, leaflets delivered to every house in an area, magazine inserts, or adverts shown to every person who views a website.

Your marketing material is still 'directed to' particular individuals if you process their personal data behind the scenes, then remove their name from

the resulting mailing. Omitting names from the marketing material you send does not stop it from being direct marketing.

What is 'solicited' and 'unsolicited' marketing?

There is no restriction on sending 'solicited' direct marketing – that is, marketing material that the person has specifically requested. PECR rules only apply to 'unsolicited' direct marketing messages, and the GDPR does not prevent you providing information which someone has asked for. So, if someone specifically asks you to send them particular marketing material, you can do so.

Example
An individual submits an online form to a double glazing company requesting a quote. By sending this quote to the individual the company is responding to the individual's request, and so the marketing is solicited.

If someone specifically signs up to a service for the sole purpose of receiving marketing within certain defined parameters, we accept that messages sent within the parameters of that service are solicited. For example, some types of loyalty schemes or offer schemes.

If the direct marketing has not been specifically requested, it is unsolicited and the PECR rules apply. This is true even if the customer has 'opted in' to receiving marketing in general from you.

Example
When they requested the quote for double glazing, the individual also ticked a box opting in to receiving information about future home improvement offers from the company. A few months later, the company sends an email with details of a new offer.

This is unsolicited marketing, because the customer did not contact the company to specifically request information about that particular offer. However, this does not mean that the company should not have sent details of the new offer. They can do so because the individual has consented to receiving these offers.

An opt-in means that the individual is happy to receive further marketing in future, and is likely to mean that unsolicited marketing is lawful. But it is still likely to be unsolicited marketing, which means the PECR rules apply. See the section on Sending direct marketing messages for further information.

Is market research direct marketing?

Market research will not constitute direct marketing if you contact individuals to conduct genuine market research (or you contract a research firm to do so). For example your purpose is to use market research to make decisions for commercial or public policy, or product development and there is no direct marketing purpose involved. However, you still need to comply with other provisions of the GDPR, and in particular ensure you process any individually identifiable research data fairly, transparently, securely and only for research purposes.

What is 'sugging'?
If your market research is for a direct marketing purpose (ie to ultimately send direct marketing communications to individuals) it will constitute direct marketing. You cannot avoid the direct marketing rules by labelling your message as a survey or market research, if you are actually trying to sell goods or services, or to collect data to help you (or others) to contact people for marketing purposes at a later date. This is sometimes referred to as 'sugging' (selling under the guise of research). If the call or message includes any promotional material, or collects data to use in future marketing exercises, the call or message is for direct marketing purposes. You must say so, and comply with the direct marketing rules.

Do not claim you are simply conducting a survey when your real purpose (or one of your purposes) is to sell goods or services, generate leads, or collect data for marketing purposes - this is likely to infringe the GDPR when you process the personal data. If you call a number registered with the TPS, sent a text or email without consent, or asked someone else to do so you may breach PECR.

Unless the individuals' contacted agreed to this and all communications comply with PECR, you must not ask market research firms you employ to:

- promote your products (this includes asking the research firm to use your goods/services as a way to incentivise participation); or
- give you the research data for future sales or marketing purposes.

If during a genuine market research project you discover errors in your customer database, you can use the research data to correct these errors without breaching the GDPR or PECR. This is consistent with the obligation under the GDPR accuracy principle to ensure personal data is accurate and up to date. However, you should not deliberately use market research as a method of keeping your customer database updated.

Further reading outside this code

More information on market research, including professional standards for research projects and mixed-purpose projects, is available on the Market Research Society (MRS) website.

What are 'service messages'?

The term 'service message' is not used in the GDPR or PECR but it is a way of describing a communication sent to an individual for administrative or customer service purposes. For example contacting a customer to:

- remind them how to contact you in case of a problem;
- check that their details are correct; or
- update them on your terms and conditions.

In these examples there is no advertising or marketing occurring and no promotional material being transmitted.

Example
A bank makes a telephone call to a customer about the administration of their bank account. The purpose of the call is simply to advise the customer that there is a problem with one of their standing orders. Therefore the call does not constitute direct marketing.

You must be able to justify that a message is a service message and not an attempt to promote or advertise for it to fall outside of the direct marketing definition. Care must be taken over the content and tone.

In order to determine whether a communication is a service message or a direct marketing message, a key factor is likely to be the phrasing, tone and context.

If a message is actively promoting or encouraging an individual to make use of a particular service, special offer, or upgrade for example, then it is likely to be direct marketing. However if the message has a neutral tone and simply informs the individual for example of a benefit on their account then these are more likely to be viewed as a service message.

Example
An individual holds a credit card which has variable balance transfer rates. The card provider wants to email the individual to tell them that the rate is changing for a limited period. Obviously the card provider needs to tell their customer about this.

If the card provider emails the individual simply telling them this information, then this is more likely to be viewed as a service message. However if the message actively encourages the individual to make use of the rate change offer then this is likely to fall within the definition of direct marketing as the card provider is promoting the rate in order to gain further business from the individual.

Example
A mobile network provider sends a text message to a customer that states that they are reaching their monthly data limit and advises what the data charges are under its terms and conditions if the customer exceeds the limit. Because this message is purely informative about their account, it is likely to be viewed as service message.

However if, for example, the mobile network provider also uses the message to encourage the customer to take up a special offer to buy more data, then this constitutes direct marketing.

You may need to send the individual a renewal or end of contract notice. These are unlikely to constitute direct marketing if neutrally worded and not actively promoting or encouraging the individual to renew or take on a further contract with you.

However, it is important to understand that you cannot avoid the direct marketing rules by simply using a neutral tone. For example a message from a supermarket chain sent to an individual saying 'Your local supermarket stocks carrots' is clearly still promotional despite the use of a neutral tone.

If the service message has elements that are direct marketing then the marketing rules apply, even if that is not the main purpose of the message.

Example
During a call about the administration of their account the bank also decides to outline its mortgage products. Although the main purpose of the call is for administration, because the call is also being used by the bank to promote other products and services, it now falls within the definition of direct marketing.

Are regulatory communications direct marketing?

The term 'regulatory communications' is often used to describe situations where a statutory regulator asks or requires the industry it regulates to send out specific communications to consumers (in sectors such as finance,

insurance, telecoms and utilities). For example about new initiatives or to promote competition in the market.

Regulators have the interests of consumers in mind when asking particular sectors to send these communications. However, it is important to remember that the direct marketing provisions of the GDPR and PECR may apply to communications that are sent to meet a regulatory objective, comply with a licence condition or meet a wider public policy initiative.

The content and context of the message is likely to determine whether it is direct marketing, regardless of the wider public policy objective behind it. If the communication actively promotes the initiative, by highlighting the benefits and encouraging consumers to participate, it will constitute direct marketing.

The normal rules apply to your proposed method of communication. You should check phone numbers against the TPS and you should not send direct marketing to people who have issued objections.

Examples of when a 'regulatory communication' might not constitute direct marketing includes information that you have been asked to inform customers about that is:

- in a neutral tone, without any encouragement or promotion;
- is given solely for the benefit of the individual; and
- is against your interests and your only motivation is to comply with a regulatory requirement (eg the regulator is requiring you to tell people that they should consider using your competitors' services).

However this always depends on a case by case basis taking into account the particular circumstances.

See the sections on What is 'advertising or marketing material'? and What are 'service messages'? for further information.

Can public sector communications be direct marketing?

The public sector is also capable of carrying out promotional activities. Just because your motivation might be to fulfil your statutory functions rather than for profit or charity, you can still engage in promotional activity. If, as a public body, you use marketing or advertising methods to promote your interests, you must comply with the direct marketing rules. For example, direct marketing in the public sector can include:

- a GP sending text messages to patients inviting them to healthy eating event;
- a regulator sending out emails promoting its annual report launch;
- a local authority sending out an e-newsletter update on the work they are doing; and
- a government body sending personally addressed post promoting a health and safety campaign they are running.

This is not an exhaustive list. It is important therefore that if you are a public body planning a promotional campaign you ensure that you are compliant with the GDPR and PECR.

However not everything you send to meet a public policy initiative will be direct marketing.

Example
A regulator wants to send an email to individuals promoting their new online complaints tool.

Whilst this email is ultimately to further the regulator's statutory function it is still direct marketing, therefore they must comply with the direct marketing rules.

However if the regulator sends an email in response to an individual's query which also includes information about its complaint service, this is unlikely to be considered marketing of that complaints service. This is because the context is different and the regulator is providing important objective information in response to the individual about their right to complain.

Whether or not the messages you send constitute direct marketing is likely to depend on the context and content of the messages. For example a text message sent by a hospital to confirm an individual's appointment is not caught by PECR because it is purely a service message not a direct marketing message.

A key thing to remember is whether the message is advertising or promoting something. Often this comes down to the tone of the communication.

Example

Scenario A
A GP sends the following text message to a patient:

'Our records show you are due for x screening, please call the surgery on 12345678 to make an appointment.'

As this is neutrally worded and relates to the patient's care it is not a direct marketing message but rather a service message.

Scenario B
A GP sends the following text message to a patient:

'Our flu clinic is now open. If you would like a flu vaccination please call the surgery on 12345678 to make an appointment.'

This is more likely to be considered to be direct marketing because it does not relate to the patient's specific care but rather to a general service that is available.

See the section What are 'service messages'? for further information.

It is important to remember that you must be transparent when collecting people's details and clearly explain what you will use their data for. This applies regardless of whether the message you send contains direct marketing or not.

Are fundraising and campaigning messages direct marketing?

Yes, direct marketing is not limited to the sale of good and services, it also includes fundraising, campaigning and promotional activities. This means that the activities of not-for-profit organisations such as charities and political parties are covered by the direct marketing rules.

Examples include:

- a university contacting its alumni to ask for donations;
- a charity appeal asking individuals to become supporters or leave a legacy donation;
- a political party contacting particular individuals to seek their votes; and
- a civil society group contacting people to encourage them to write to their MP or attend a public meeting or rally.

You still need to ensure that you comply with the GDPR and PECR rules even if you are contacting existing supporters.

Further reading outside this code
See our separate guidance on:
Draft framework code of practice for the use of personal data in political campaigning

Planning your marketing: DP by design

At a glance

A key part of the GDPR is accountability and you must be able to demonstrate your compliance. You must consider data protection and privacy issues upfront when you are planning your direct marketing activities. Depending on your direct marketing activity you may be required to conduct a DPIA.

Generally speaking the two lawful bases most likely to be applicable to your direct marketing purposes are consent and legitimate interests. However if PECR requires consent then in practice consent will be your lawful basis under the GDPR. If you intend to process special category data for direct marketing purposes it is likely that the only Article 9 condition available to you will be 'explicit consent'.

In most cases it is unlikely that you will be able to make using an individual's data for direct marketing purposes a condition of your service or buying your product.

It is important to keep personal data accurate and up to date. It should not be kept for longer than is necessary. Children's personal data requires specific protection in regard to direct marketing.

In more detail

Why is it important to plan our direct marketing activities?

It is important to plan your direct marketing activity before you start so that you can build in data protection and PECR. It is hard to retrofit GDPR and PECR into your direct marketing activities once you have started the processing and you may find that you are infringing on the direct marketing rules by not having planned properly. This in turn may also harm your reputation and your relationship with your customers or supporters. Therefore it makes good business sense to properly plan ahead.

A key part of GDPR is accountability. You are responsible for ensuring that your direct marketing practices are compliant and you must be able to demonstrate your compliance. You are likely to need to:

- adopt data protection policies;
- take a 'data protection by design and default' approach;
- maintain documentation of your processing activities;
- have written contracts with organisations that process personal data on your behalf; and
- carry out data protection impact assessments (DPIAs) (see the section Do we need to conduct a DPIA? for more information).

You must be clear which legislation applies to your direct marketing activities so you can follow all the relevant rules. In some cases only the GDPR or only PECR will apply, but in other circumstances both may apply. For example, if you are processing personal data when sending direct marketing by electronic message or when using cookies (or similar technologies) for direct marketing purposes.

Further reading outside this code
See our separate guidance on:
Accountability and governance

What is data protection by design?

The GDPR requires you 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 when you are planning your direct marketing activities. You need to as a minimum ask yourself the following questions:

- Who is your target audience? Is it particular groups of individuals, is it business contacts?

- Are you a controller or a joint controller? Do you intend to use a processor to send direct marketing on your behalf?
- How will you ensure that your direct marketing activity is lawful, fair to individuals and your purposes transparent? (lawfulness, fairness and transparency principle)
- What specified direct marketing purposes do you intend to collect this data for? (purpose limitation principle)
- What personal data is actually necessary and proportionate for your direct marketing activity? (data minimisation principle)
- How will you ensure the accuracy of the data that you are using for your direct marketing activity? (accuracy principle)
- How long will it be necessary for you to keep the data for your direct marketing purposes? (retention principle)
- How will you ensure that appropriate security measures are taken with regard to the data you want to use for direct marketing purposes? (security principle)
- Will any of the personal data be transferred overseas?
- How will you implement and support individuals' rights?

Thinking about these questions will help your direct marketing to be compliant with the GDPR.

Relevant provisions in the legislation
GDPR – see Article 25 and Recital 78

Further reading outside this code
See our separate guidance on:
Data Protection by design and default
Principles

Are we responsible for compliance?

In most situations it is likely to be obvious that you are the controller and have responsibility for complying with data protection. However it is common in the direct marketing context to work with third parties and this can be beneficial to you – but you do need to ensure that your collaboration with others is compliant with the GDPR and PECR.

In particular you need to be clear who in the relationship is the controller and what your responsibilities are. It is also important that any work you do with third parties is lawful, fair and transparent.

In some instances you might choose to use a processor to assist with your processing for direct marketing purposes. A processor acts on your behalf

under your authority and in line with your instructions. You are the data controller in this situation.

For example, you might use a processor to screen your telephone marketing list against the TPS or to print and send your postal marketing to the people on your customer list.

If you use a processor you must comply with the GDPR rules on controllers and processors. For example you must choose a processor that provides sufficient guarantees that they implement appropriate technical and organisational measures to ensure their processing meets GDPR requirements.

The GDPR and PECR do not prevent you from conducting joint direct marketing campaigns with third parties. However you and the third party need to be clear about your responsibilities under the legislation.

You need to be clear who the controller is, if you and the other party are both processing the personal data. If you are joint controllers then you must arrange between yourselves who takes primary responsibility for complying with the GDPR – but remember that all joint controllers remain responsible for compliance with the controller obligations which means action can be taken against any of you. You need to have a transparency agreement that sets out your agreed roles and compliance responsibilities.

If you are planning electronic communications as dual branding promotion with a third party, you still need to comply with PECR even if you do not have access to the data that is used. Both you and the third party are responsible for complying with PECR.

Example
A supermarket decides to support a particular charity at Christmas and sends out a marketing email to its customers promoting the charity's work. Whilst the email is promoting the charity, it also constitutes marketing by the supermarket itself as it is promoting its values.

Although the supermarket is not passing the contact details of its customers to the charity it still needs to ensure there is appropriate consent from its customers to receive direct marketing promoting the charity. Where possible it would be good practice for the supermarket to screen against the charity's suppression list.

Relevant provisions in the legislation
GDPR – see Article 26, 28, 82, 83 and Recitals 79 and 146

Further reading outside this code

See our separate guidance on:
Controllers and processors
Contracts and liabilities between controllers and processors
The Guide to PECR

Do we need to complete a DPIA?

A data protection impact assessment (DPIA) enables you to analyse your processing and help you identify and minimise the data protection risks. It is an integral part of the accountability requirements of GDPR.

DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability and building trust and engagement with individuals.

Article 35 of the GDPR says you must do a DPIA if you plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

The ICO has compiled a list of processing operations where a DPIA is required as these are 'likely to result in a high risk'. Many of these operations that require a DPIA are relevant to the direct marketing context:

- large scale profiling;
- data matching – eg for direct marketing;
- invisible processing – eg list brokering, online tracking by third parties, online advertising, re-use of publicly available data;
- tracking the geolocation or behaviour of individuals – eg online advertising, web and cross device tracking, tracing services (tele-matching, tele-appending), wealth profiling, loyalty schemes; and
- targeting children or other vulnerable individuals for marketing and profiling.

Some of these processing operations require a DPIA automatically. Others require a DPIA if they occur in combination with any other criterion from the European guidelines on DPIAs. There are nine of these criteria that may act as indicators of likely high risk processing.

If your direct marketing activity includes processing of a type likely to result in high risk, you must do a DPIA before you begin the processing. You therefore need to carry it out in the early stages of developing a project,

prior to processing personal data. You may need to consult with the ICO and so should build in time for potential consultation to your project plan.

You do not need to submit all DPIAs to the ICO for prior consultation. However, you must consult with the ICO if your DPIA identifies a high risk and you are not able to take measures to reduce this risk.

The DPIA is a dynamic document and you should review and update it to ensure it reflects any changes to your project. The review process does not stop once processing personal data commences. You should periodically review the DPIA at suitable intervals during longer term projects to ensure it remains an accurate assessment of the processing undertaken, the risks and the mitigations in place.

Good practice recommendation
Even if there is no specific indication of likely high risk in your direct marketing activity, it is good practice to do a DPIA for any major new project involving the use of personal data.

Relevant provisions in the legislation
GDPR – see Article 35 and Recitals 84, 89, 90, 91, 92, 93, and 95

Further reading outside this code
See our separate guidance on:
DPIAs

See also:
EDPB Guidelines on Data Protection Impact Assessment (DPIA)

How do we decide what our lawful basis is for direct marketing?

You must decide and document your lawful basis before you start processing personal data for direct marketing purposes. There are six lawful bases for processing in the GDPR. The most appropriate basis to use depends on your direct marketing activity, the context and your relationship with the individual.

It is likely to be obvious to you that certain lawful bases do not apply to your direct marketing. For example vital interests does not apply in a direct marketing context. For other lawful bases it may not be as clear.

If you have a contractual relationship with the individual you might be able to apply the contract lawful basis to your direct marketing. However it is important to remember that this lawful basis only applies to processing that

is necessary for the performance of that contract. It does not apply if the processing for direct marketing purposes is necessary to maintain your business model or is included in your terms and conditions for business purposes beyond delivering the contractual service.

For example, just because you may be able to rely on the contract lawful basis to process an individual's address to supply them with goods, does not mean that you can also use this basis to send direct marketing to them or profile them based on their purchases.

If you are a public authority you might be able to use public task for your direct marketing if you can demonstrate that the processing is necessary for a specific task or function set down in law.

Generally speaking the two lawful bases that are most likely to be applicable to your direct marketing purposes are consent and legitimate interests. However it is important to remember that neither of these lawful bases are the 'easy option' and both require work.

Your choice between these two bases is likely to be affected by a number of factors including whether you want to give individuals choice and control (consent) or whether you want to take responsibility for protecting the individual's interests (legitimate interests). However, the first thing you need to consider is PECR.

PECR requires consent for some methods of sending direct marketing. If PECR requires consent, then processing personal data for electronic direct marketing purposes is unlawful under the GDPR without consent. If you have not got the necessary consent, you cannot rely on legitimate interests instead. You are not able to use legitimate interests to legitimise processing that is unlawful under other legislation.

If you have obtained consent in compliance with PECR (which must be to the GDPR standard), then in practice consent is also the appropriate lawful basis under the GDPR. Trying to apply legitimate interests when you already have GDPR-compliant consent would be an entirely unnecessary exercise, and would cause confusion for individuals.

The table below lists different methods of sending direct marketing and whether PECR requires consent:

Marketing method	**Does PECR require consent?**
'Live' phone calls to TPS/CPTS registered numbers	✓

'Live' phone calls to those who have objected to your calls	✓
'Live' phone calls where there is no TPS/CTPS registration or objection	✗
Automated phone calls	✓
Emails/texts/in app/in-platform direct messaging to individuals – obtained using 'soft opt-in'	✗
Emails/texts/in-app/in platform direct messaging to individuals – without 'soft opt-in'	✓
Emails/text messages to business contacts (corporate subscribers)	✗
Post	✗ (not covered by PECR)

See the section below on How does consent apply to direct marketing? for further information.

If PECR does not require consent, legitimate interests may well be appropriate. Likewise legitimate interests may be appropriate for 'solicited' marketing (ie marketing proactively requested by the individual). See the section below on How does legitimate interests apply to direct marketing? for further information.

Good practice recommendation
Get consent for all your direct marketing regardless of whether PECR requires it or not. This gives you the benefit of only having to deal with one basis for your direct marketing as well as increasing individuals' trust and control. See the section How does consent apply to direct marketing? for the requirements of consent.

In order to be accountable, if you rely on consent you must keep appropriate records of the consent and if you rely on legitimate interests you must document how it applies to your processing.

Relevant provisions in the legislation
GDPR – see Article 6(1)(a), 6(1)(b), 6(1)(e) and 6(1)(f)

Further reading outside this code
See our separate guidance on:

Lawful basis for processing
Consent
Contract
Public task
Legitimate interests
The use of cookies and similar technologies

See also EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects

How does consent apply to direct marketing?

The consent lawful basis is about giving people choice and control over how you use their data.

The GDPR defines consent in Article 4(11) as:

"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"

Individuals can withdraw consent at any time. You must make it as easy to withdraw consent to direct marketing as it was to give it. See the section What do we do if someone withdraws their consent? for further information.

Remember you do not automatically have an individual's consent to process their personal data for direct marketing purposes just because you have a pre-existing relationship with them – for example because they are your customer, previously donated to your cause, or are one of your alumni.

Example
An individual sees a charity appeal in a newspaper and decides to donate £5 by text message. However the fact that the individual has decided to donate on this occasion (and provided their telephone number to the charity as a result) does not mean that the charity has their consent to use their details to contact them about future campaigns. The charity cannot therefore use the individual's details for direct marketing purposes.

If you want to rely on consent to process the individual's personal data for direct marketing purposes you must meet all the elements of valid consent.

Freely given

The individual must:

- have genuine choice and control over whether or not to consent to their personal data being used by you for direct marketing purposes;
- be able to refuse consent to direct marketing without detriment; and
- be able to withdraw consent at any time.

You should not coerce or unduly incentivise people to consent to direct marketing. However in the marketing context there is usually some inherent benefit to individuals if they consent to marketing, eg discounted products or access to special offers. But you must be careful not to cross the line and unfairly penalise those who refuse consent to your direct marketing.

Example
Joining a retailer's loyalty scheme comes with access to money-off vouchers. Clearly there is some incentive for people to consent to marketing. However the fact that this benefit is unavailable to those who do not sign up doesn't amount to a detriment for refusal.

You must also be careful if you make consent for marketing a condition of accessing a service or benefit. For more information see the section Can we make our services conditional on the individual receiving direct marketing?.

Specific and informed
Your request for consent for direct marketing must cover:

- the name of the controller who wants to rely on the consent – this includes you and any third party controllers who are relying on the consent for direct marketing;
- the purposes of the processing – you need to be specific about your direct marketing purposes;
- the types of processing activity – where possible you should provide granular consent options for each separate type of processing (eg consent to profiling to better target your marketing or different methods of sending the marketing), unless those activities are clearly interdependent – but as a minimum you must specifically cover all processing activities; and
- the right to withdraw consent at any time – we also advise you should include details of how to do so.

You must clearly explain to people in a way they can easily understand that they are consenting to direct marketing. The request for consent needs to be prominent, concise, in plain language, and separate from your privacy information or other terms and conditions.

Whilst PECR takes its definition of consent from the GDPR it also reinforces the need to be specific and informed by requiring that the consent is to 'such communications'. For example you cannot make an automated call unless that person has consented to receiving that type of communication from you.

Unambiguous indication
It must be obvious that the individual has consented to you processing their personal data for direct marketing purposes. It must be a clear, affirmative act, where the individual takes a deliberate and specific action to agree to your direct marketing purpose.

Example
An airline's privacy policy states that they send direct marketing material to individuals who buy a flight from them. In order to submit the online form, individuals must tick a box to say that they have read that policy.

However confirmation that the individual has read the privacy policy does not constitute an unambiguous indication that the individual has consented to receive direct marketing. Therefore the airline is not able to rely on consent as their lawful basis.

Pre-ticked opt-in boxes are banned under the GDPR. You cannot rely on silence, inactivity or default settings – consent must be separate, freely given, unambiguous and affirmative. Failing to opt-out of direct marketing is not valid consent.

Relevant provisions in the legislation
GDPR – see Article 4(11), Article 6(1)(a), Article 7, Recital 32, 42, and 43

Further reading outside this code
See our separate guidance on:
Consent

See also:
European Data Protection Board (EDPB) Guidelines on consent

How does legitimate interests apply to direct marketing?

If you do not need consent under PECR, then you might be able to rely on legitimate interests for your direct marketing purposes if you can show the way you use people's data is proportionate, has a minimal privacy impact and is not a surprise to people or they are not likely to object to what you are doing.

The legitimate interests lawful basis is made up of a three-part test:

- Purpose test – is there a legitimate interest behind the processing?
- Necessity test – is the processing necessary for that purpose?
- Balancing test – is the legitimate interest overridden by the individual's interests, rights or freedoms?

We refer to this test as a legitimate interests assessment (LIA). You must objectively consider whether legitimate interests apply to your direct marketing purposes.

Recital 47 of the GDPR says:

> "…The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest."

It is important to note that the GDPR says that direct marketing **may** be a legitimate interest. It does not say that it is always a legitimate interest and it does not mean that you are automatically able to apply this lawful basis to your direct marketing. Whether you can apply it depends on the particular circumstances.

The fact that direct marketing 'may be regarded' as a legitimate interest is likely to help you demonstrate the purpose test, as long as the marketing is carried out in compliance with e-privacy laws and other legal and industry standards.

You still need to show that your processing passes the necessity and balancing tests. You may also need to be more specific about your purposes for some elements of your processing in order to show that processing is necessary and to weigh the benefits in the balancing test. For example, if you use profiling to target your marketing.

It is sometimes suggested that direct marketing is in the interests of individuals, for example if they receive money-off products or offers that are directly relevant to their needs. This is unlikely however to add much weight to your balancing test, and we recommend you focus primarily on your own interests and avoid undue focus on presumed benefits to customers unless you have very clear evidence of their preferences.

In some cases direct marketing has the potential to have a significant negative effect on the individual, depending on their personal circumstances. For example, someone known or likely to be in financial difficulties who is regularly targeted with direct marketing for high interest loans may sign up for these offers and potentially incur further debt.

When looking at the balancing test, you should also consider factors such as:

- whether people would expect you to use their details in this way;
- the potential nuisance factor of unwanted marketing messages; and
- the effect your chosen method and frequency of communication might have on vulnerable individuals.

Example
A theatre wants to send details of its programme of summer performances by post to people who have attended events there in the past and have not previously objected to receiving direct marketing from it.

The theatre's purpose of direct marketing to increase its revenues is a legitimate interest.

The theatre considers it is necessary to process the name and address details for this purpose and that posting the programme is a proportionate way of achieving this.

The theatre determines that the impact of this postal marketing on the individuals is likely to be minimal but it includes details within the mailing about how to opt-out.

Given that individuals have the absolute right to object to direct marketing, it is more difficult to pass the balancing test if you do not give individuals a clear option to opt out of direct marketing when you initially collect their details (or in your first communication, if the data was not collected directly from the individual). The lack of any proactive opportunity to opt-out in advance would arguably contribute to a loss of control over their data and act as an unnecessary barrier to exercising their data protection rights.

Other examples of when it is very difficult for you to pass the balancing test include:

- processing for direct marketing purposes that you have not told individuals about (ie invisible processing) and they would not expect; or
- collecting and combining vast amounts of personal data from various different sources to create personality profiles on individuals to use for direct marketing purposes.

Remember if PECR requires consent then in practice it is consent and not legitimate interests that is the appropriate lawful basis.

Relevant provisions in the legislation
GDPR – see Article 6(1)(f) and Recital 47

Further reading outside this code
See our separate guidance on:
Legitimate interests

See also:
Article 29 Working party (which has been replaced by the EDPB) Opinion 06/2014 on the notion of legitimate interests of the data controller – whilst this was written under the previous data protection framework it is still useful guidance.

Can we make our services conditional on the individual receiving direct marketing?

In most cases it is unlikely that you can make using an individual's data for direct marketing purposes a precondition of entering into a contract to buy your product, use your services or support your cause etc.

If the direct marketing is not necessary for the performance of that service or contract then the consent will be invalid because it is not freely given.

Example
A train company has signs in its carriages saying that free wifi is available for its passengers.

In order to access the wifi the passenger is required to provide their name, email address and telephone number. There is a notice at the bottom of the sign up process which says:

□ I understand that by submitting my details I am agreeing to receive marketing from the train company.

If the passenger does not tick the box they cannot access the 'free' wifi – in other words accessing the wifi is conditional on them receiving electronic direct marketing.

It is not necessary for the train company to collect these details for direct marketing purposes in order to provide the wifi, therefore the consent is not valid.

If you believe that your processing of personal data for direct marketing purposes is necessary for the service, then you may be able to rely on the contracts lawful basis. However you still need consent if you want to send certain types of electronic marketing under PECR.

If you are considering legitimate interests as your lawful basis you must be able to demonstrate how making your service conditional on direct marketing is actually necessary and proportionate and how this impacts on the individual's rights and freedoms. See the section How do we decide what our lawful basis for processing is? for further information.

There may be occasions when making direct marketing a condition of service is necessary for that service. For example, a retail loyalty scheme that is operated purely for the purposes of sending people marketing offers, is likely to be able to show that the direct marketing is necessary for that service. But you need to be upfront and clear about this purpose and ensure that the consent individuals provide when signing up meets the GDPR standard. If on the other hand your loyalty scheme allows people to collect points when they shop, which they can then redeem against future purchases, you cannot require them to consent to marketing messages in order for them to collect these points.

Relevant provisions in the legislation
GDPR – see Article 6(1)(a) and Article 7(4), Article 6(1)(b), and Article 6(1)(f)

Further reading outside this code
See our separate guidance on:
Consent guidance

Can we use special category data for direct marketing?

Special category data is specifically defined in the GDPR. It is recognised as more sensitive and in need of more protection (eg racial or ethnic origin, political opinions, religious beliefs, health data or sexual life). If you want to use this type of data for your direct marketing purposes you must have a special category condition from Article 9 of the GDPR as well as having an Article 6 lawful basis for the processing.

There are ten conditions for processing special category data in the GDPR itself and the DPA 2018 contains additional conditions. These conditions are narrow to cover very specific circumstances and none of them relate specifically to direct marketing. In practice the only condition available for processing special category data for direct marketing purposes is 'explicit consent'.

Therefore if you do not have the individual's explicit consent you cannot process their special category data for direct marketing purposes.

Explicit consent is not defined in the GDPR, but must meet the usual GDPR standard for consent. In particular, it must be freely given, informed, specific, affirmative (opt-in) and unambiguous, and able to be withdrawn at any time. In practice, the extra requirements for consent to be 'explicit' are likely to be that it:

- must be confirmed in a clear statement (whether oral or written), rather than by any other type of affirmative action;
- must specify the nature of the special category data; and
- should be separate from any other consents you are seeking.

Special category data can be a particular issue if you are trying to better target your direct marketing by profiling individuals. If you are profiling for direct marketing purposes on the basis of special category data, you need explicit consent for that profiling – including drawing inferences about people's likely race, ethnicity, politics, beliefs, health or sexual orientation from other data. You also need to be careful that these assumptions about people do not lead you to process inaccurate, inadequate or irrelevant personal data.

Example
A supermarket wants to promote its baby club. It decides to use its loyalty card data to predict which of its customers might be pregnant in order to send them messages about its baby club.

Because the supermarket does not have its customers explicit consent to do this, it has infringed the GDPR.

Simply holding a list of customer names will not trigger Article 9, even if those names are associated with a particular ethnicity or religion – unless you specifically target marketing on the basis of that inference. Likewise if you could infer special category data from your customer list due to the nature of the products you sell – eg you are a company selling disability aids – this will not trigger Article 9 unless you hold specific information about the individual's condition or specifically target marketing on the inference of their health status.

Relevant provisions in the legislation
DPA 2018 – see Sections 10, 11 and Schedule 1
GDPR – see Article 9 and Article 9(2)(a), and Recital 43

Further reading outside this code
See our separate guidance on:
Special category data
Consent

How do we keep personal data we use for direct marketing accurate and up to date?

The accuracy principle of the GDPR requires that personal data is accurate and where necessary kept up to date. This is important for direct marketing.

For example you need to accurately record:

- the data that you have been provided with eg contact details;
- the source of that data;
- which methods of direct marketing the individual has consented to;
- objections, opt-outs, withdrawals of consent; and
- people's details on suppression lists.

You need to have a process for considering challenges that individuals may make to the accuracy of the data you hold about them. Individuals have a specific right under the GDPR to have inaccurate data rectified. See the section What do we do if someone tells us their data is inaccurate? for further information.

You must take reasonable steps to ensure that personal data you hold for direct marketing purposes is not factually incorrect or misleading. It is reasonable to rely on the individual to tell you when they change address or other contact details. It may be sensible to periodically ask individuals to update their own details, but you do not need to take extreme measures to ensure people's contact details are up to date such as using tracing services. See the section Can we use data cleansing and tracing services? for further information.

Example
A retailer sends direct marketing by post to an individual. The marketing is returned to the retailer marked with the words 'no longer at this address'.

The retailer complies with the accuracy principle by making a note on the individual's record to say that the address is no longer correct.

It is important that any suppression lists you use are kept up to date. For example ensure that you use the most recent version of the TPS to screen telephone numbers t before making live direct marketing calls.

You should have a policy to periodically review and update the data you hold for direct marketing purposes.

Relevant provisions in the legislation
GDPR – see Article 5(1)(d)

Further reading outside this code
See our separate guidance on:
Accuracy

How long should we keep personal data for direct marketing purposes?

The GDPR does not specify how long you should keep personal data for direct marketing purposes. However the storage limitation principle says that you must not keep it for longer than you need it.

Therefore it 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 direct marketing purpose to keep it.

In order to comply with the documentation requirements of the GDPR you are likely to need a policy that sets your retention periods. Also, you need to tell people how long you will store their personal data or the criteria you used to determine the period, to meet one of the requirements of the right to be informed.

You need to remember that if you are relying on consent to send direct marketing that consent does not last forever. How long consent remains valid depends on the particular circumstances including:

- the context in which it was given;
- the nature of the individual's relationship with you; and
- the individual's expectations.

PECR is also clear that consent is only 'for the time being' which implies that consent lasts as long as the circumstances remain the same. The question is whether it is still reasonable to treat it as an ongoing indication of that individual's wishes. Depending on the circumstances it is likely to be harder to rely on consent as a genuine indication of wishes as time passes.

Consent for a one-off message, or consent that is clearly only intended to cover a short period of time or a particular context, does not count as ongoing consent for all future direct marketing.

Example

A retailer collects email addresses from individuals who have specifically asked to be kept up to date about a new product launch.

Once the product has been launched the retailer needs to consider whether it is still necessary for them to keep these email addresses given that the specific reason that these were provided has now ended. The consent that individuals gave for the product launch does not cover sending direct marketing about other products.

If you obtained an individual's consent via a third party to send direct marketing they may be happy to hear from you at the time they gave their consent. However they are unlikely to expect to start receiving your messages at a much later date. This may be different in very specific cases where the circumstances clearly indicate that the individual would expect to start receiving marketing from you at a particular time in the future. For example consent given via a third party to receive your offers on seasonal products or annually renewable insurance services.

Good practice recommendation
When sending direct marketing to new customers on the basis of consent collected by a third party we recommend that you do not rely on consent that was given more than six months ago.

Remember individuals' can withdraw their consent at any time. If the individual withdraws their consent, you must stop any of the processing for direct marketing purposes that was based on that consent. See the section What do we do if someone withdraws their consent? for further information.

Individuals can also opt-out or unsubscribe from receiving your direct marketing messages. If this happens, you cannot send any further direct marketing messages to them.

Individuals can object to you using their personal data for direct marketing. If this happens, you must stop that processing. See the section on Individual rights for more information.

If you no longer need the personal data for your direct marketing purposes you should erase (delete) or anonymise it (ie so it is no longer in a form that allows the individual to be identified).

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

Relevant provisions in the legislation
GDPR – see Article 5(1)(e), Article 13 and 14, and Article 30

Further reading outside this code
See our separate guidance on:
Storage limitation
Consent
Legitimate interests
What is personal data?

Can we use children's personal data for direct marketing?

You are not necessarily prevented from using children's personal data for direct marketing purposes. The normal rules apply – for example, you must be transparent, comply with all the data protection principles and you must comply with PECR, if you are sending electronic communications.

The GDPR does highlight children's personal data as requiring specific protection especially for direct marketing. Recital 38 says:

"Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child…."

The GDPR also says that you must explain your direct marketing purposes in a way that a child understands. Recital 58 says:

"…Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand."

If a child gives you their personal data, such as an email address, or information about their hobbies or interests, then they may not realise that you will use it to market them, and they may not even understand what marketing is and how it works. This may lead to them receiving direct marketing that they do not want. If they are also unable to critically assess the content of the marketing then their lack of awareness of the consequences of providing their personal data may make them vulnerable in more significant ways. For example, they may be influenced to make unhealthy food choices, or to spend money on goods that they have no use for or cannot afford.

So, if you wish to use a child's personal data for direct marketing you need to think about if and how you can mitigate these risks and take into account their reduced ability to recognise and critically assess the purposes behind your processing and the potential consequences of providing their personal data to you. You should not exploit any lack of understanding or vulnerability.

Advertising standards stipulate that marketing targeted directly at or featuring children should not contain anything that is likely to result in their physical, mental or moral harm and must not exploit their credulity, loyalty, vulnerability or lack of experience. For example some adverting industry standards ban or limit direct marketing of certain types of products to services (eg gambling, high fat, salt or sugar foods in adverts aimed at children).

Whilst you are not prevented from profiling children for the purposes of direct marketing you need to take particular care if you do so to ensure that any marketing they receive as a result of your profiling complies with advertising standards and is not detrimental to their health or wellbeing.

The EDPB Guidelines on Automated Individual decision-making and Profiling state:

"Because children represent a more vulnerable group of society, organisations should, in general, refrain from profiling them for marketing purposes. Children can be particularly susceptible in the online environment and more easily influenced by behavioural advertising. For example, in online gaming, profiling can be used to target players that the algorithm considers are more likely to spend money on the game as well as providing more personalised adverts. The age and maturity of the child may affect their ability to understand the motivation behind this type of marketing or the consequences."

You should also note that the child's right to object to your processing their personal data for direct marketing also extends to any profiling that is related to that direct marketing. So if the child (or someone acting on their behalf) asks you to stop profiling for this purpose, then you must do so.

You must complete a DPIA if you intend to target children (or other vulnerable individuals) for direct marketing purposes. See the section Do we need to complete a DPIA? for further information.

Further reading outside this code
See our separate guidance on:
Children
Draft Age appropriate design code of practice

DPIAs

See also:
EDPB Guidelines on Automated Individual decision-making and Profiling

Sector specific guidance on marketing to children eg Advertising Standards Authority

Generating leads and collecting contact details

At a glance

Transparency is a key part of the GDPR and as part of this individuals have the right to be informed about your collection and use of their personal data for direct marketing purposes.

If you collect data directly from individuals you must provide privacy information at the time you collect their details. If you collect personal data from sources other than the individual (eg public sources or from third parties) you must provide privacy information within a reasonable period of obtaining the data and no later than one month from the date of collection. Your privacy information must be in clear and plain language and easily accessible.

If you are considering buying or renting direct marketing lists you must ensure you have completed appropriate due diligence.

In more detail

What is lead generation?

There are a number of ways that you may decide to generate leads and seek contact details to use for your direct marketing purposes. For example from:

- the individuals who buy your products and services or support your cause (ie people who have a direct relationship with you);
- third parties who sell or rent lists of contact details; or

- publicly available sources.

Whichever method you wish to use, you must ensure that your processing is fair, lawful and transparent. This includes giving individuals appropriate privacy information about what you intend to do with their data.

What do we need to tell people if we collect their data directly from them?

Transparency is a key part of the GDPR and as part of this individuals have the right to be informed about your collection and use of their personal data for direct marketing purposes.

Article 13 of the GDPR contains a list of the information that you must provide to individuals if you collect their personal data directly from them. For example you must:

- explain why you are using people's personal data (eg to send postal marketing, profile people's buying habits and interests etc);
- tell people who the third parties are that you intend to share their data with or the specific categories that they fall into if applicable;
- tell people what your retention periods are for the data that you are using for direct marketing purposes;
- say which lawful bases you are relying on for your direct marketing;
- say what the legitimate interests are if you are using legitimate interests as your lawful basis;
- tell people about the right to withdraw consent if you are relying on consent as your lawful basis;
- provide details about any solely automated decisions (including profiling) that have legal or similarly significant effects which you intend to make; and
- tell people what rights they have under the GDPR (including the right to object to your direct marketing).

You must provide this privacy information to individuals at the time you collect their details. If at later date you want to process for purposes other than those which you initially collected the data for you need to give individuals further privacy information (assuming the new purposes are fair and lawful.

See the section below How do we tell people that we want to use their personal data for direct marketing? for further information.

Relevant provisions in the legislation

GDPR – see Article 5(1), and Article 13

Further reading outside this code
See our separate guidance on:
Right to be informed

What do we need to tell people if we collect their data from other sources?

If you collect personal data indirectly, ie from sources other than the individual, you must still be transparent and comply with the right to be informed. Other sources could include publicly available data, third parties such as data brokers, or other organisations that you work with.

Article 14 of the GDPR contains a list of the information you must provide to individuals if you have not collected their personal data directly from them. In general these requirements are the same as when you collect the data directly from the individual but you also need to provide:

- details of the categories (types) of the individual's personal data that you have collected (eg contact details, interests, ethnicity etc); and
- the source of their personal data (eg the name of the third party, the name of the publicly available source).

You must provide privacy information to individuals within a reasonable period and at the latest within a month of obtaining their data.

If you plan to use the personal data you obtain to send direct marketing to the individual it relates to, or to disclose to someone else, the latest point at which you must provide the information is when you first communicate with the individual or disclose their data to someone else. However it is important to remember that the one month time limit still applies in these situations. For example, if you plan on disclosing an individual's personal data to someone else for direct marketing purposes two months after obtaining it, you must still provide that individual with privacy information within a month of obtaining the data.

Example
A travel company obtains a list of contact details from Company Z.

Three weeks after obtaining the data the travel company sends out its brochure to the people on the list along with details of its privacy information which includes the types of information it holds (names and addresses) and details of the source of the individual's personal data (Company Z).

There are a number of exceptions to Article 14 requirements. The majority are unlikely to be applicable in a direct marketing context but the following 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.

Individual already has the information
To rely on the exception that the individual already has the information, you must be able to demonstrate and verify what information they already have. You must ensure that they have been provided with all of the information listed in Article 14 – you must provide anything that you are unsure about or that is missing.

Disproportionate effort
If you want to rely on the disproportionate effort exception, you must 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's not proportionate to put significant resources into informing individuals. However the more significant the effect the processing has on the individual then, the less likely you are to be able to rely on this exception.

You are unlikely to be able to rely on disproportionate effort in situations where you are collecting personal data from various sources to build an extensive profile of an individual's interests and characteristics for direct marketing purposes. Individuals will not reasonably expect organisations to collect and use large volumes of data in this way, especially if they do not have any direct relationship with them. If individuals do not know about such extensive processing of their data they are unable to exercise their rights over it.

If you determine that providing privacy information does involve a disproportionate effort, you must record your reasoning in order to demonstrate your accountability. Even if disproportionate effort correctly applies, the GDPR still requires you to publish the privacy information (eg on your website).

Good practice recommendation
If it is relatively easy for you to inform individuals and in context it is useful to them, you should always do so, even if the effect of the processing on individuals is minor.

If you do not actively tell people about your processing it results in 'invisible processing'. Therefore you must carry out a DPIA before you start. See the section Do we need to complete a DPIA? for further information.

Further information on publicly available personal data is in the section Can we use publicly available personal data for direct marketing purposes?.

Relevant provisions in the legislation
GDPR – see Article 14

Further reading outside this code
See our separate guidance on:
Right to be informed

How do we tell people that we want to use their data for direct marketing?

The privacy information you provide to individuals must be concise, intelligible, in clear and plain language, and easily accessible. This applies regardless of how you collect the personal data for direct marketing purposes (eg online, over the phone, in person).

You should tailor your privacy information to your audience – so think about who your customers, supporters, contacts etc are and what they are likely to understand.

You need to clearly explain the purposes for which you want to process the individual's personal data for. Vague terms such as 'marketing purposes', 'marketing services' or 'marketing insights' are not sufficiently clear. These terms are wide and potentially cover all sorts of processing for direct marketing purposes such as sending direct marketing messages, profiling or analysing individual's behaviours.

If you find it difficult to explain what you will be doing with people's personal data, or you do not want to be transparent because you think they might object to that processing, then this is a clear sign that you should rethink your intended purpose or processing.

Example
A charity wants to conduct wealth profiling of its supporters to determine their financial standing so they can target their campaigns appropriately. It includes the following statement in its privacy information:

'We analyse our supporters and the donations they have made. Some of the results from this analysis provide us with an indication of the likely donations we may receive in the future.'

This statement is vague and not clear what purpose the charity is using the data for. It does not explain to supporters that the charity wants to profile their financial standing to decide who has capacity to donate more money or who might leave a legacy.

As the statement is not sufficiently transparent any processing based on this statement infringes the GDPR.

There is no set way that you should provide your privacy information. You can consider whichever method suits the way you are collecting the data. For example, you might consider 'just in time notices' in an online context or have layered notices. The key point is that you should be upfront about your direct marketing processing.

Any unusual or unexpected processing ought to be at the forefront of any layered privacy information. For example as it is highly unlikely that your customers or supporters etc expect you to collect additional data on them from other sources, this should therefore clearly be brought to the individual's attention.

Further reading outside this code
See our separate guidance on:
Right to be informed

See also:
EDPB Guidelines on Transparency

Can we use publicly available personal data for direct marketing purposes?

The term 'publicly available' can refer to information sourced from various places, including:

- the open version of the electoral register;
- Companies House;
- social media; and
- press articles or 'rich' lists.

You might seek personal data from publicly available sources to find new customers or supporters, or to add to the profile or data you already hold about individuals.

The GDPR does not prevent you from collecting and using personal data from publicly available sources for direct marketing purposes. However you should not assume that such data is 'fair game'. The GDPR and PECR still apply and once you have collected this data you are a controller for it and you must comply.

For example, you must meet the transparency requirements of the GDPR and provide people with privacy information (unless you are relying on an exception). See the section what do we need to tell people if we collect their data from other sources? for further information.

You must also ensure that your processing of personal data is fair, taking into account the source of the data. You must consider whether what you intend to do with the data is unexpected to individuals. For example you cannot assume that simply because an individual has put their personal data into the public domain, they are agreeing to it being used for direct marketing purposes. An individual 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 your direct marketing 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 personal data for direct marketing purposes.

You must also comply if you are collecting personal data from publicly available sources in order to package it up and make it available to other organisations for them to use for direct marketing purposes you still need to comply with the GDPR. This means you are required to provide privacy information about your processing to the individuals whose data you collect. You must provide this within a month of obtaining the data or before you disclose their data to others, whichever is soonest.

If you collect people's contact details from publicly available sources and then send electronic marketing you may breach PECR. See the section on Sending direct marketing messages for further information.

What do we need to consider when buying or renting direct marketing lists?

Many organisations, including data brokers, offer direct marketing lists for sale, rent or on license.

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

You must be very careful about using these lists and undertake proportionate due diligence.

Due diligence when buying data could include ensuring you have certain details as described below:

- **Who** compiled the data – was it the organisation you are buying it from or was it someone else?
- **Where** was the data obtained from – did it come from the individuals directly or has it come from other sources?
- **What** privacy information was used when the data was collected – what were individuals told their data would be used for?
- **When** was the personal data compiled – what date was it collected and how old is it?
- **How** was the personal data collected – what was the context and method of the collection?
- **Records** of the consent (if it is 'consented' data) – what did individuals' consent to, what were they told, were you named, when and how did they consent?
- **Evidence** that the data has been checked against opt-out lists (if claimed) – can it be demonstrated that the TPS or CTPS has been screened against and how recently?
- **How** does the seller deal with individuals' rights – do they pass on objections?

A reputable third party should be able to demonstrate to you that the data is reliable. If they cannot do this, or if you are not satisfied with their explanations, you should not use the data.

You may wish to have a written contract in place confirming the reliability of the personal data, as well as making your own checks. The contract should give 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.

Your own compliance

You need to be clear how your use of the list complies with the GDPR. For example, can you can demonstrate what your lawful basis is for processing the list.

You also need to screen the lists that you obtain against your own suppression lists. This ensures you do not contact anyone who has already said they object or want to opt-out of your direct marketing (unless they have given you consent that overrides their previous objection). See the Individual rights section for further information on suppression.

Once you have obtained the data, you must comply with the right to be informed and provide people with your own transparency information detailing anything they have not already been told. See the section What do we need to tell people if we collect their data from other sources? for further information.

You also must be prepared to deal with any inaccuracies or complaints arising from your use of the data. If you receive complaints from individuals whose details came from a particular source, this might suggest that the source is unreliable and you should not use it.

Relevant provisions in the legislation
GDPR – see Article 6(1)(a), and Article 14

Further reading outside this code
See our separate guidance on:
Consent
The right to be informed

Can we ask our existing customers to give us contact details of their friends and family?

You cannot escape your GDPR and PECR obligations by asking existing customers or supporters to provide you with contact details for their friends and family to use for direct marketing purposes. In practice it is very difficult to comply with the GDPR when collecting details for direct marketing purposes in this way or to demonstrate your accountability.

For example you have no idea what the individual has told their friends and family about you processing their data and you would not be able to verify whether these contacts actually gave valid consent for you to collect their data. If you want to do this you need to very carefully plan how you will demonstrate accountability and compliance – in practice this is likely to be difficult in most circumstances.

If you use contact details collected in this manner to send electronic direct marketing you are likely to breach PECR. For example, you would not have

valid consent to send direct marketing emails, texts (the soft opt-in would not apply) or to make automated calls or to override a TPS registration.

Profiling and data enrichment

At a glance

Profiling and enrichment activities must be done in a way that is fair, lawful and transparent. If you are considering using profiling or enrichment services you must ensure you have completed appropriate due diligence.

If you are carrying out solely automated decision making, including profiling, that has legal or similarly significant effects on individuals then there are additional rules in the GDPR that you must comply with. If you want to profile people using their special categories of data you must have their explicit consent to do this.

If you use non-personal data such as assumptions about the type of people who live in a particular postcode to enrich the details you hold about an individual it will become personal data.

In most instances, buying additional contact details for your existing customers or supporters is likely to be unfair unless the individual has previously agreed to you having these extra contact details.

You are unlikely to be able to justify tracing an individual in order to send direct marketing to their new address – such tracing takes away control from the individual to be able to choose not to tell you their new details.

In more detail

What does profiling and data enrichment mean?

Profiling is where the behavioural characteristics of individuals are analysed to find out about their preferences, predict their behaviour, make decisions about them or classify them into different groups or sectors.

Data enrichment is where you find out more data on individuals to add to the profile that you already hold on them.

Profiling and data enrichment can be very useful for direct marketing and there are often clear business benefits. For example, knowing more about your customers and supporters can help you tailor your direct marketing messages in order to get better response rates.

However you must ensure that any profiling or enrichment that you do, or that you buy from third parties (such as data brokers), complies with the GDPR and, where applicable, PECR.

Can we use profiling to better target our direct marketing?

Profiling is defined in Article 4(4) as:

> "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."

Profiling is not necessarily restricted to facts about individuals. Profiling for direct marketing purposes often involves predictions, inferences or assumptions about individuals.

Profiling might occur in direct marketing in the following circumstances:

- analysing loyalty card data to decide what new products to suggest to a customer;
- identifying high net-worth individuals in order to send them fundraising material about legacy donations;
- predicting what products an individual might buy based on their online browsing history;
- applying assumptions about an individual's personal circumstances based on their postcode;
- combining online and offline data to build up a picture of an individual's interests; and
- segmenting customers into different categories based on perceived characteristics.

Profiling can help you to target your messages to people who are more likely to buy your product or support your cause. But it can potentially pose significant risks to the rights and freedoms of individuals because:

- they might not know it is happening or fully understand what is involved;
- it might restrict and undermine the individual's freedom to choose;
- it might perpetuate stereotypes; or
- it might cause discrimination.

You can profile aspects of an individual's personality, behaviour, interests or habits in order to use this for direct marketing purposes, but you must still comply with the direct marketing rules and where applicable the rules on automated decision-making.

You must be transparent and clearly explain to individuals what you will be doing. You also need to make sure the processing is fair and lawful as well as ensuring the personal data you hold as part of the profile is accurate and not excessive for your purpose.

It is important to remember that you cannot profile individuals on the basis of their special categories of data without their explicit consent. See the section Can we use special category data for direct marketing? for further information.

If explicit consent is not required and you are considering using legitimate interests as your lawful basis, you need to give careful consideration to the three-part test. It is unlikely that you will be able to apply legitimate interests for intrusive profiling for direct marketing purposes. This type of profiling is not generally in an individual's reasonable expectations and is rarely transparent enough.

Remember, if you want to engage in 'large-scale profiling' or 'wealth profiling' you are required to complete a DPIA before your start processing. See the section Do we need to complete a DPIA? for further information.

Solely automated decisions

Article 22 of the GDPR has rules to protect individuals if you are carrying out solely automated decision-making including profiling that has legal or similarly significant effects on individuals. The profiling that you undertake for direct marketing purposes is only caught by Article 22 if there is no human involvement and there is a legal or similarly significant effect on the individual.

Automated profiling is likely to occur in online behavioural advertising because this happens without human involvement.

Whilst the majority of direct marketing based on solely automated profiling is unlikely to have a legal or 'similarly significant effect', there could be situations where it does for example:

- profiling to target vulnerable groups or children;
- targeting individuals known to be in financial difficulty with marketing about high interest loans;
- targeting known problem gamblers with adverts for betting websites; or
- using profiling to effectively 'price-out' individuals of owning a particular product by giving them a much higher price than other people.

If Article 22 is engaged you need the individual's explicit consent to profile for direct marketing purposes.

Further reading outside this code
See our separate guidance on:
Rights related to automated decision making including profiling

See also:
EDPB Guidelines on Automated individual decision-making and Profiling

Relevant provisions in the legislation
GDPR – see Article 4(4) and Article 22

Can we enrich the data we already hold?

Enrichment is where you use other sources such as data brokers or publicly available data to find out more information about your customers or supporters to add to a profile on them.

Examples of enrichment include obtaining information about:

- an individual's interests and buying habits;
- customer segmentation (the type of customers you have);
- postcode data (eg assumptions or census data about the type of people who live in a certain area); and
- enriching online data with offline data (and vice versa).

It is important to remember that if non-personal data such as postcode data is added to the details you hold about the individual it will become personal

data. This means that you must comply with the GDPR. For example, you must ensure that this processing is transparent, fair and lawful.

You need to be careful that the enrichment is not unfair to individuals. It is unlikely that individuals will anticipate you seeking to learn more about them using enrichment or indeed understand what enrichment is.

If you are considering enrichment you need to check what you have previously told individuals about using third parties or public sources to gather extra data to create or expand a profile on them. Likewise if the data held by the third party is personal data, you need to check what that third party told people about selling that data to you. You are not able to enrich the personal data you hold if you and the third party (where applicable) did not tell people about this.

You must have explicit consent from the individual for processing if any of the data is special category data. See the section Can we use special category data for direct marketing? for further information.

As enrichment is profiling, you should also read the section Can we use profiling to better target our direct marketing?.

Can we match or append data?

Data matching or appending is where you match the data you already hold on individuals with other contact details that you did not already have. For example, buying phone numbers for your customers to add to the address details that you already hold. These additional contact details are usually obtained from third parties, such as data brokers.

In most instances, buying additional contact details for your existing customers or supporters is likely to be unfair, unless the individual has expressly agreed.

This is likely to be true no matter how clearly you explain it in your privacy information that you might seek out further personal data about individuals from third parties. This is because it removes people's choice about what channels you can contact them on for direct marketing purposes.

Individuals use different email addresses as a way of managing their data and relationships, including as a means to limit or to manage the direct marketing they receive. By getting that information from a third party, you may be going directly against their wishes.

You cannot assume that an individual wants you to contact them by other channels or has forgotten to give you the data. Even if they had forgotten, they still would not reasonably expect you to contact them via contact details they never gave you. It must be for the individual to choose what contact details they give you.

If an individual has consented via a third party for you to have their additional contact details to use for direct marketing then you are able to match this to what you already hold about them. However you need to make sure that the consent is valid.

See the section What do we need to consider when using profiling or enrichment services? for further information.

Can we use data cleansing and tracing services?

Some organisations such as data brokers offer data cleansing and tracing services for direct marketing purposes. For example, these services are used for:

- removing the contact details of people who are deceased from a marketing list;
- removing contact details that are out of date; and
- tracing the new addresses of individuals.

Data cleansing that removes deceased records from your database is unlikely to be a problem under the GDPR (assuming this information is accurate) because the GDPR only applies to living individuals. Likewise removing out of date contact details helps you comply with the accuracy and data minimisation principles. However tracing is very difficult to do for direct marketing purposes in a way that is compliant.

Often you may become aware that an individual's contact details are no longer correct but they have not told you of the change. For example, because your direct marketing material is being returned to sender due to the individual no longer living there, their email address is no longer valid or their phone number is no longer in service.

There is no requirement for people to tell you when they have changed contact details so that you can continue using their data for direct marketing purposes.

However in some cases individuals may express a wish for their updated contact details to be shared. For example, the individual may have moved house and made clear to a third party data source, by ticking a box or some

other positive action, that they wanted the source to inform further third parties of the change of address. In this instance you are able to continue to market them at the new address (assuming your initial collection of the data at the old address was compliant). If there's no evidence of a recent expectation that their updated contact details would be shared, it is highly likely that the 'tracing' will be unfair and unlawful.

You cannot assume that an individual has simply forgotten to tell you that they have changed their details. Even if they had previously consented to your direct marketing at their old address, this consent is not transferrable to a new address that they have not given you. Likewise under PECR, consent is non transferrable – it is specific to receipt of calls or texts to a particular telephone number, or messages to a particular email address.

Tracing an individual for direct marketing purposes takes away control from people to be able to choose not to tell you their new details. Your commercial interests in continuing to market them do not outweigh this. Therefore you are unlikely to be able to justify this processing under legitimate interests.

Whilst the GDPR requires you to keep personal data up to date 'where necessary', your processing must always be fair. The actions you take to update contact details must be reasonable and proportionate. It will be difficult to justify taking intrusive steps such as tracing to keep contact details used for direct marketing up to date.

It is not necessary to trace individuals, because it is more reasonable in a direct marketing context to rely on individuals to inform you of changes to their details.

Example
A university sends fundraising newsletters by post to the last address that they held for their alumni. Some of the alumni graduated a number of years ago. A large number of the mailings are returned to the university because the address details are now incorrect.

The university decides to use a data broker to 'cleanse' its alumni database and provide up to date address details. The university then sends its newsletters to the new addresses.

The university has infringed the GDPR by taking this action Because it is unfair to trace individuals in these circumstances and it takes away their control. The university's legitimate interest in raising money does not outweigh the rights of the alumni to choose not to share their new address.

If you already hold other contact details for communication with the individual, you could consider using these to remind them how they can keep

their details updated with you. But you must be very careful to check that this contact is fair, lawful and transparent, as well as complying with PECR (where applicable).

See the section How do we keep personal data we use for direct marketing accurate and up to date? for more information on complying with the accuracy principle.

Relevant provisions in the legislation
GDPR – see Article 5(1)(d)

Further reading outside this code
See our separate guidance on:
Accuracy
The right to be informed

What due diligence do we need to consider when using profiling or enrichment services?

You are responsible for ensuring compliance with the GDPR and PECR. It is not enough to simply accept a third party's assurances that the data they are supplying to you is compliant. You must be able to demonstrate your compliance and be accountable.

As part of your planning stage you should do appropriate due diligence before you use profiling or enrichment services. Due diligence could include having answers to the following questions:

- what is the third party's approach to transparency – do people know that the company has their data?
- what sources of data is the third party using – is using these sources fair?
- what does the third party's DPIAs say – have they completed any?
- when was the data compiled – how old is the data?
- records of the consent (if it is 'consented' data) – what did individuals consent to, what were they told and how did they give consent?
- is any of the data special category data?

A reputable third party should be able to demonstrate to you that the data is compliant. If they cannot do this, or if you are not satisfied with their explanations, you should not use the data.

It is important to remember that before you obtain data on your customers or supporters via such services you must ensure that undertaking this activity is compliant with the GDPR. For example:

- have you told people about using profiling or enrichment services?
- have you been sufficiently transparent about this and is it fair to do this?
- what lawful basis are you relying on and do/can you meet the requirements of that basis?

Relevant provisions in the legislation
GDPR – see Article 14

Sending direct marketing messages

At a glance

No matter which method you use for sending direct marketing messages the GDPR will apply when you are processing personal data.

The direct marketing provisions in PECR only apply to live and automated calls, electronic mail (eg text and emails) and faxes. The electronic mail 'soft opt-in' only applies to the commercial marketing of products and services, it does not apply to the promotion of aims and ideals.

PECR may apply differently to business to business marketing. PECR may still apply even if you ask someone else to send your electronic direct marketing messages.

In more detail

Why does the type of message matter?

The methods you use to contact individuals as part of your direct marketing campaign may vary. However the GDPR rules are the same no matter what method you choose to communicate with people. For example, you still need to tell people that you are processing their data and what for, and have a lawful basis for the processing in place, prior to contacting them.

In contrast the direct marketing rules in PECR vary depending on your chosen method of contacting individuals and can also be different if you are

contacting your business contacts. The rules can also be different if you are promoting aims and ideals rather than selling products and services.

Direct marketing by post

Direct marketing by post is not covered by PECR. But you must still comply with the GDPR if you are processing personal data as part of your campaign.

If you conduct a mail drop addressed to 'the householder' or 'the occupier' this is unlikely to constitute direct marketing because it is not directed to a particular individual. However you cannot use this as a way to get around the GDPR. If you process an individual's data to target them with advertising, merely omitting that individual's name from the final marketing communication does not prevent the processing being for direct marketing purposes. A name on an envelope is not the sole factor when determining whether someone's personal data has been processed to allow the marketing material to be 'directed to' that particular individual.

Before you start your postal direct marketing campaign you need to consider for example:

- Do people know that you intend to use the data for direct marketing by post?
- Have you screened the contact details against your suppression list of people who have previously opted out of your direct marketing?
- Do you have a process for dealing with people who exercise their right to object to direct marketing?

Good practice recommendation
Unlike live telephone calls and faxes there is no statutory preference service for direct marketing by post where individuals can register their objection to such contact. However we recommend that you screen individual's names and addresses against the mail preference service (MPS) prior to sending out the direct marketing.

You should also be aware that screening against the MPS is a requirement under some industry codes.

Direct marketing by 'live' calls

Direct marketing by 'live' telephone call (where there is a live person who is speaking) is covered by different provisions of PECR depending on what the call is about.

In general the PECR rules on making live marketing calls are that you:

- cannot call numbers registered with the Telephone Preference Service (TPS) or the Corporate Telephone Preference Service (CTPS) unless the subscriber has consented to your marketing calls;
- cannot call the number of a subscriber who has previously objected to your calls;
- must say who is calling (eg the name of your organisation);
- must allow your number (or an alternative contact number) to be displayed to the person receiving the call; and
- must provide your contact details or a Freephone number if asked.

In short you can call numbers that are not registered on the TPS or CTPS without the subscriber's consent, but only if there is no previous objection.

There are however specific stricter rules for direct marketing calls about claims management services and pension schemes which are dealt with below.

If you want to call a number registered with the TPS or CTPS you must have the subscriber's consent in order to override their general objection to direct marketing calls.

Example
A utility company collects an individual's contact details verbally. During the conversation the company asks the individual if they would like to receive direct marketing telephone calls from it. The individual verbally agrees to such calls.

Assuming the consent is valid, the utility company does not need to screen this number against the TPS or their own 'do not call' lists because the individual has consented to receive such calls.

It is not enough that someone simply failed to object to past calls, or failed to take positive steps to opt-out of your calls. For example, you cannot assume that failing to click on an unsubscribe link, or not replying to an email inviting them to opt-out, is notification that they do not object. They must have taken a proactive step to 'notify' you that they wish to receive direct marketing calls from you.

Example
A travel insurance company collects contact details using an online form and provides a tick box for individuals to use if they wish to opt-out of their live direct marketing calls.

The company screens the phone numbers of those who did not opt-out against the TPS and its own 'do not call list'. It discovers that a small percentage of these numbers are registered with the TPS or have previously told the company they do not want their calls.

Because failing to opt-out does not constitute consent to receive live direct marketing calls, this does not override the TPS registration or objection. The travel insurance company does not make the calls to these numbers.

If someone you have called in the past subsequently registers their number with TPS or CPTS, you cannot make any more direct marketing calls to them from that point. Even if they have not specifically objected to your calls before, registering with TPS acts as a general objection which you must respect. You can only call that TPS registered number again if the subscriber has already specifically consented to receive your direct marketing calls. If so, the fact that they later register with TPS does not override that specific consent, and you may continue to call them (assuming that they do not withdraw their consent for your calls).

Example
A charity has called an individual in the past to fundraise. The individual has never specifically objected to receiving the calls nor did they specifically consent to the direct marketing calls.

When undertaking its regular screening against the TPS the charity notices that the individual has now registered their number on the list. The charity might be confident in light of its past relationship with the individual that they would not object to further calls, however it will breach PECR if it continues to make direct marketing calls to that individual.

You also need to comply with the GDPR if you are processing personal data when making the calls. For example because you know the name of the person you are calling. See the section on Planning your marketing: DP by design for further information.

In line with the purpose limitation principle, and in order to ensure fairness, you cannot make a direct marketing call to a number that you originally collected for an entirely different purpose.

Example
A bank records information about some of the individuals who are shareholders of its corporate account customers. It collects and holds this information to comply with its duties under anti-money laundering regulations. Unless the bank has obtained their prior consent, it is unfair to use this information to make marketing calls inviting those individuals to open personal accounts with the bank.

In order to be fair to individuals you should not make calls to them which would unduly distress people or cause them other unjustified harm. Be particularly careful if you are aware that someone is elderly or vulnerable, or if the nature of the direct marketing call might cause offence or stress. You should avoid frequent redialling of unanswered numbers or making calls at antisocial hours.

You must make sufficient checks of third parties and give them clear instructions if you outsource any part of your telephone marketing campaign, such as asking someone else to screen the numbers against the TPS or to make the calls on your behalf. You still retain responsibility for complying with PECR and the GDPR. See the section on Planning your marketing: DP by design for further information.

If an individual tells you they do not want your calls anymore you must respect this and suppress their details by adding it to your 'do not call list'. See the section What are direct marketing suppression lists? for more information.

Calls management calls
The rules on live direct marketing calls about claims management services are stricter than other types of direct marketing calls (with the exception of pension scheme calls).

This means the following services in relation to making a claim:

- advice;
- financial services or assistance;
- acting on behalf of, or representing, a person;
- the referral or introduction of one person to another; or
- the making of inquiries.

The term 'claim' means a claim for compensation, restitution, repayment or any other remedy or relief in respect of loss or damage or in respect of an obligation, whether the claim is made or could be made:

- by way of legal proceedings;
- in accordance with a scheme of regulation (whether voluntary or compulsory); or
- in pursuance of a voluntary undertaking.

You can only make direct marketing calls about claims management services if the person you are calling has specifically consented to your calls. This means that unlike other types of direct marketing calls there is no need to check against the TPS or CTPS, because you must have consent. For more

information on consent see the section How does consent apply to direct marketing?.

If you have consent to make these calls then you must also:

- say who is calling (eg the name of your organisation);
- allow your number (or an alternative contact number) to be displayed to the person receiving the call; and
- provide contact details or a Freephone number for your organisation if asked.

Pension scheme calls
The rules on live calls for direct marketing of pension schemes (eg occupational pensions or personal pensions) are very strict. This type of call is banned except in specific circumstances.

Regulation 21B says that direct marketing of pension schemes includes:

- marketing a product or service to be acquired using funds held, or previously held in a pension scheme;
- offering advice or another service that promotes, or promotes consideration of, withdrawing or transferring funds from a pension scheme; or
- offering advice or another service to enable the assessment of the performance of a pension scheme (including its performance in comparison with other forms of investment).

You can make live direct marketing calls about pension schemes, if you meet all the requirements of the specifically defined exception.

For the exception to apply, firstly you must be a trustee or manager of an occupational or personal pension scheme or authorised by the Financial Conduct Authority (FCA).

Secondly you must either have the individual's consent to receive the calls or your relationship with the individual must meet strict criteria, as follows:

- you have an existing client relationship with the person you are calling (this doesn't include a relationship that you have established primarily in order to allow you to make such a call);
- that person might reasonably envisage such a call from you; and
- you gave them a chance to opt-out of such calls when you collected their details and in every communication you send them.

For more information on consent see the section How does consent apply to direct marketing?.

In order for you to be fair and transparent you should say who is calling (eg the name of your organisation) and allow your number (or an alternative contact number) to be displayed to the person receiving the call. You should also provide contact details or a Freephone number for your organisation if asked.

Relevant provisions in the legislation
PECR – see Regulation 21 and Regulation 24, Regulation 21A (as inserted by section 35 of the Financial Guidance and claims Act 2018) and Regulation 21B

Further reading outside this code
See our separate guidance on:
The Guide to PECR

Direct marketing by automated calls

Direct marketing by automated telephone call is covered by Regulation 19 of PECR. These are calls made by an automated dialling system that plays a recorded message.

You can only make this type of call if you have consent. General consent for direct marketing, or even consent for live calls, is not enough. The consent must specifically cover automated calls from you.

There is no need for you to screen against the TPS or CTPS because it makes no difference whether or not a number is registered with a preference service. You cannot make that call without the subscriber's consent, even if the number is not on these lists.

PECR also requires that your automated call must:

- say who is calling (eg the name of your organisation);
- allow your number (or an alternative contact number) to be displayed to the person receiving the call; and
- provide your contact details or a Freephone number.

You also need to comply with the GDPR if you are processing personal data when making the calls. For example because you know the name of the person you are calling. See the section on Planning your marketing: DP by design for further information.

If you intend to buy a 'consented' list of telephone numbers to use for automated calls, you need to undertake appropriate due diligence. See the

section What do we need to consider when buying or renting direct marketing lists? for further information.

Relevant provisions in the legislation
PECR – see Regulation 19 and Regulation 24

Further reading outside this code
See our separate guidance on:
The Guide to PECR

Direct marketing by electronic mail (including emails and texts)

Direct marketing by electronic mail is covered by Regulation 22 of PECR. Electronic mail is defined in Regulation 2 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 means it covers any electronically stored messages. For example email, texts, picture or video messages, voicemail messages, in-app messages and direct messaging on social media.

Currently the most commonly used forms of electronic mail are email and text messages. However the guidance on these two types is also relevant to any form of electronic mail.

In general under PECR, direct marketing by electronic mail requires that you have the individual subscriber's consent. However there is an exception to this known as the 'soft opt-in'.

If you intend to rely on consent you must ensure that it is specific to the individual receiving that particular type of electronic mail from you (for example specific consent for emails or specific consent for text messages). If you are intending to send direct marketing text messages it is important to remember that consent to use their phone number for live or automated calls does not cover direct marketing by text message.

See the section How does consent apply to direct marketing? for further information.

Example

An individual is buying a pair of jeans from a high street retailer. At the end of the payment the shop assistant asks the individual if they would like their receipt emailed to them. The individual agrees and gives their email address.

Later that day the individual receives an email that contains an electronic receipt of their purchase.

However the following day the individual receives a further email promoting the retailer's footwear sale.

Whilst the first email was compliant because it did not contain any marketing, the second email is not. This is because the individual did not consent to their email address being used for direct marketing and no information was given to the individual about it being used for this purpose. There are also GDPR issues in terms of fairness and transparency.

Example
An individual uses their mobile phone to call a takeaway to verbally order a pizza. The takeaway advises the individual how much the order costs and how long it will take to be ready.

Shortly after the call the individual receives a text message from the takeaway thanking them for their order and telling them how to opt-out of its offers. The individual then receives multiple text messages offering discounts on pizzas.

The individual did not consent to their phone number being used to send direct marketing text messages and no information was given to the individual during the phone call about it being used for this purpose.

The takeaway is in breach of PECR by automatically opting the number into receiving direct marketing text messages.

If you want to rely on the soft opt-in instead of consent see the section on The soft opt-in for further information.

Regardless of whether you are relying on consent or the soft opt-in, you must not disguise or conceal your identity and you must provide a valid contact address or Freephone number for individuals to opt out or unsubscribe.

You must comply if an individual tells you they do not want direct marketing by electronic mail, for example if they unsubscribe or opt-out. You must make it easy for them to withdraw their consent or opt-out. See the section on Individual rights for further information.

If you intend to ask or 'instigate' someone else to send your electronic marketing, see the sections on Can we use third parties to send our direct marketing? and Can we ask individuals to send our direct marketing? for further information.

You also need to comply with the GDPR if you are processing personal data when sending the electronic mail. For example because you know the name of the person you are texting.

Because an email address identifies a unique user and distinguishes them from other users, it is personal data, therefore you also need to comply with the GDPR. For example, you must provide transparency information to people and have a lawful basis for the processing. See the section on Planning your marketing: DP by design for further information.

If you use 'tracking pixels' within your direct marketing emails then you need to be aware that:

- regulation 22 applies to the email itself; and
- if the pixel involves storing information, or accessing information stored, on the device used to read the email – such as its location, operating system, etc – then PECR's rules on cookies and similar technologies (Regulation 6) will also apply.

See the section on Online advertising and using other technologies for further information.

Further reading outside of this code
See our separate guidance on:
What is personal data?
Cookies and similar technologies

The 'soft opt-in'

The term 'soft opt-in' is not used in PECR, but it is commonly used to describe the exception to the consent requirement of Regulation 22.

Regulation 22(3) says:

"A person may send or instigate the sending of electronic mail for the purposes of direct marketing where—

(a) that person has obtained the contact details of the recipient of that electronic mail in the course of the sale or negotiations for the sale of a product or service to that recipient;

(b) the direct marketing is in respect of that person's similar products and services only; and

(c) the recipient has been given a simple means of refusing (free of charge except for the costs of the transmission of the refusal) the use of his contact details for the purposes of such direct marketing, at the time that the details were initially collected, and, where he did not initially refuse the use of the details, at the time of each subsequent communication."

The soft opt-in only applies to electronic mail (eg emails and texts), it does not apply to other methods of direct marketing. If you want to use the soft opt-in you must meet all of its requirements. It breaks down into five requirements;

1) You obtained the contact details;
2) In the course of a sale or negotiation of a sale of a product or service;
3) Your similar products and services are being marketed;
4) Opportunity to refuse or opt-out given when you collected the details; and
5) Opportunity to refuse or opt-out given in every communication.

These requirements are described in detail below.

1) **You obtained the contact details**
   You must have obtained the contact details directly from the individual. If the contact details were obtained by someone else then the soft opt-in does not apply.

Example
A restaurant chain is offered a list of individuals' mobile phone numbers which the third party claims are 'soft opt-in compliant'.

If the restaurant chain uses this list to send direct marketing text messages they will breach PECR. The soft opt-in does not apply because the restaurant chain did not obtain the contact details direct from the individuals. There is no such thing as a third party marketing list that is 'soft opt-in compliant'.

2) In the course of a sale or negotiation of a sale of a product or service
   The individual does not actually need to have bought anything from you to trigger the soft opt-in. It is enough if 'negotiations for a sale' took

place. This means that the individual should have actively expressed an interest in buying your products or services. For example, by requesting a quote or asking for more details of what you offer. There must be some form of express communication.

Example
A customer logs into a company's website to browse its range of products. This is not enough to constitute negotiations. But if the customer completes an online enquiry form asking for more details about a product or range of products, this could be enough.

The communication must be about buying products or services. It's not enough for the individual to send any type of query.

Example
A customer sends an online enquiry to ask if the company can order a particular product. This could constitute negotiations for a sale. But an enquiry asking if the company is going to open more branches in a particular location does not.

3) Your similar products and services are being marketed

You can only send electronic mail about your similar products or services. The key question is whether the individual reasonably expects direct marketing about your particular product or service. This is likely to depend on the context, including the type of business you are and the category of product.

Example
A customer buys bread and bananas online from a large supermarket chain. Afterwards they might reasonably expect emails about bread, fruit, and other groceries, but also a wide range of products including books, DVDs, kitchen equipment and other everyday goods commonly sold in supermarkets.

However, they are unlikely to expect emails about banking or insurance products sold under the supermarket brand. These products are not bought and sold in a similar context.

Because the soft opt-in applies to 'products and services' it can only apply to commercial marketing. This means that charities, political parties or other not-for-profit bodies are not able to rely on the soft opt-in for their campaigning or fundraising, even with existing supporters. In other words, you must have consent to send electronic mail promoting your aims or ideals.

4) Opportunity to refuse or opt-out given when you collected the details

You must give individuals a clear opportunity to opt-out of your direct marketing when you first collect their details. You cannot assume that individuals who engage with you are automatically happy to receive direct marketing from you in the future.

It must be simple to opt out. When first collecting a customer's details, this should be part of the same process. For example, your online forms should include a prominent opt-out box, and staff taking down details verbally should specifically offer an opt-out.

Example
An individual buys some trainers from an online shoe retailer and as part of the buying process provides their email address.

The retailer automatically adds this email address to their marketing database and the individual subsequently receives an email with a 10% discount code for their next purchase.

However these emails are not compliant with the soft opt-in. Even though the individual's email address was collected during the course of a sale and the marketing is for the retailer's similar products, the retailer did not give the individual an opportunity to opt-out of receiving direct marketing emails when it collected their details.

5) Opportunity to refuse or opt-out given in every communication

You must give individuals the chance to opt-out of every subsequent communication that you send.

It must be simple for individuals to change their mind and opt-out or unsubscribe. For example, in subsequent messages the individual should be able to reply directly to the message, or click a clear 'unsubscribe' link. In the case of text messages you could offer an opt-out by telling individuals to send a stop message to a short code number. This must be free of charge, apart from the cost to the individual of sending the message.

Example
A yoga studio sends its clients an email about forthcoming events. At the bottom of the email the studio provides the following information:

'If you don't want to receive these emails from us anymore please click here and we will unsubscribe you.'

Example

A hairdresser sends its clients a text message offering 30% off colour treatments. At the end of the text it says:

'To opt-out text STOP to 12345.'

Relevant provisions in the legislation
PECR – see Regulation 22(3)

Does the does the soft opt-in apply to fundraising or campaigning?

If you are fundraising or promoting aims and ideals, you need to take particular care when communicating by electronic mail. This is because the 'soft opt-in' exception only applies to commercial marketing of products or services. It does not apply to the promotion of aims and ideals eg campaigning or fundraising.

You might be able to use the soft opt-in for any commercial products or services you offer. But you are not able to send campaigning or fundraising texts or emails without specific consent, even to existing supporters.

Example
A charity has an online shop that sells various ethically sourced products. An individual buys some speciality teas from the online shop and when they provide their details they are given a clear upfront chance to opt-out of direct marketing by email.

If the individual doesn't tick the opt-out box the charity may be able to rely on the soft opt-in to send direct marketing emails about the products in its online shop (assuming the other soft opt-in criteria are met).

However the charity cannot send emails to the individual which were about fundraising because this is not covered by the soft opt-in.

Business to business marketing

Business to business (B2B) marketing is where you send direct marketing to another business or a business contact rather than to an individual in their personal capacity.

The GDPR still applies to B2B marketing if you are processing personal data. It is the PECR rules that may be different for B2B (when compared to contacting individuals). This depends on your chosen method of direct

marketing and the type of business you intend to contact (ie they are a corporate subscriber).

It is important to remember that not all types of businesses are classed as corporate subscribers under PECR. Sole traders and some types of partnerships constitute individual subscribers which means they have greater protections under PECR.

The table below shows when PECR applies to business contacts:

Marketing method	**Does PECR apply?**
'Live' phone calls to corporate subscribers	✓
'Live' phone calls to sole traders and some types of partnerships	✓
Automated phone calls to corporate subscribers	✓
Automated phone calls to sole traders and some types of subscribers	✓
Faxes sent to corporate subscribers	✓
Faxes sent to sole traders and some types of partnerships	✓
Electronic mail (eg mails/text messages) to corporate subscribers	✗
Electronic mail (eg mails/text messages) to sole traders and some types of partnership	✓

The PECR rules apply if you are intending to send direct marketing to your B2B contacts by live or automated call or by fax. It is important to remember, however, that some businesses (sole traders and some partnerships) register with the TPS, and others register with the CTPS. For live B2B calls, you therefore need to screen against both the TPS and the CTPS registers, as well as your own 'do not call' list. See the section Direct marketing by 'live' calls for further information.

You can send direct marketing faxes to corporate subscribers without their consent, but you cannot fax any number listed on the Fax Preference Service unless they have specifically said that they do not object to your faxes. You also cannot fax anyone who has told you not to. If you want to send marketing faxes to a sole trader you must have consent because the rules for individual subscribers are different. In practice for fax B2B marketing you need to:

- check if the business is an individual subscriber;
- screen against the Fax Preference Service;
- screen against your own do not fax lists; and
- include your name and contact address or Freephone number on all B2B direct marketing faxes.

The PECR rules on marketing by electronic mail (eg email and text messages) do not apply to corporate subscribers. This means you can send B2B direct marketing emails or texts to any corporate body. However you must still say who you are and give a valid address for the recipients to unsubscribe from your emails.

Good practice recommendation
It makes good business sense for you to keep a 'do not email or text' list of any businesses that object or opt out of your direct marketing by electronic mail, and screen any new B2B direct marketing lists against it.

Because sole traders and some partnerships are treated as individual subscribers you can only market them by electronic mail if they have specifically consented, or the 'soft opt-in' applies. See the section Direct marketing by electronic mail (including emails and texts) for further information.

If you are unsure whether the contact details belong to an individual subscriber or a corporate subscriber this puts you at risk of breaching PECR. To mitigate that risk you should treat the details as belonging to an individual subscriber and ensure that you comply with rules on electronic mail.

If you do not know the name of who you are sending direct marketing to at a business, then you are not processing personal data and the GDPR does not apply to your marketing. For example, you are sending your direct marketing by post addressed simply to 'the IT department' or your email to 'info@company.com'.

However the GDPR does apply wherever you are processing personal data. This means if you can identify an individual either directly or indirectly, the GDPR applies, even if they are acting in a professional capacity. For example, you must comply with the GDPR if you have the name and number of a business contact on file or their email address identifies them (eg initials.lastname@company.com).

If you collect an individual's contact details in their business capacity and you intend to send them direct marketing you must make them aware of this and have a lawful basis for the processing. Also if you intend to buy or sell a list of business contacts for direct marketing purposes you must ensure that the

list complies with the GDPR if individuals can be identified from it. See the section What do we need to consider when buying or renting a direct marketing lists? and Selling or sharing data for further information.

Example
A business conference organiser collects the email addresses of delegates as part of the sign up process. This process does not say what the email addresses are used for and no options are given.

After the event the organiser decides they want to use the list to send emails to delegates about future events and that they also want to sell on the delegate contact list to third parties.

In terms of GDPR, no transparency information was provided to delegates about their data being sold onto other organisations. Also, the delegates were not made aware that their details would be used for direct marketing.

In terms of PECR, if any of the email addresses belong to sole traders or some types of partnership these are classed as 'individual subscribers'. As no consent was sought and the requirements of the soft opt-in were not met the organiser is in breach of PECR if they send direct marketing emails to these types of subscribers.

Assuming PECR does not require consent, in many cases it is likely that legitimate interests will be the appropriate lawful basis for processing individuals' personal data in their business capacity for direct marketing purposes. But there is no absolute rule and you need to apply the three-part test.

The GDPR does not necessarily apply to your collection of other people's hard copy business cards but this depends on what you intend to do with this information.

Example
At an industry networking event some of the attendees share their business cards which each other.

One of the attendees takes the business cards back to their organisation and places them loose into their desk drawer. At this point the GDPR does not apply to these business cards even though these have people's names on them. This is because the GDPR only applies to business cards if you intend to file them or input the details into a computer system.

One of the other attendees takes the business cards back to their organisation and adds them to their business contacts database. The GDPR applies to the personal data they have added to their marketing database

therefore the organisation needs to ensure they comply with the GDPR.

Individuals have the right to object to you processing their personal data for direct marketing purposes and the right to withdraw their consent to your processing. If an individual withdraws their consent or objects, you must stop processing their personal data as part of your B2B marketing. See the section on Individual rights for further information.

Relevant provisions in the legislation
PECR – see Regulation 19, 20, 21, 21A, 21B and 23

Further reading outside of this code
See our separate guidance on:
Legitimate interests (contains a section on using legitimate interests for business to business contacts)

Can we use third parties to send our direct marketing?

You might decide that you want to use the services of a third party to send your direct marketing on your behalf. You are not prevented from doing this, but you must ensure that you comply with the direct marketing rules.

Using third parties to send your direct marketing can take different forms, for example:

- you provide a third party with the contact details of your customers and ask them to do it on your behalf; or
- you ask a third party to use their own marketing lists to send your direct marketing content to individuals (sometimes known as 'hosted marketing').

Although in both these forms you are not physically sending the marketing yourself, this does not mean that you stop being responsible for compliance.

PECR applies to the 'sender', 'caller', or 'instigator' of the direct marketing message. This means that PECR may still apply even if you do not send the electronic message yourself or you do not hold the contact details that your direct marketing messages are sent to.

The term 'instigator' is not defined in PECR; however you are likely to be instigating if you encourage, incite, or ask someone else to send your direct marketing message.

Both you and the third party are responsible for complying with PECR. For example if Company A is encouraged by Company B to send its marketing emails then both companies require consent from the individual under PECR – Company A because they are the sender and Company B because they are the instigator.

In terms of responsibilities under the GDPR when using third parties to send your direct marketing, you may be joint controllers with the third party or there may be a controller/processor relationship. Whichever applies both of you have your own obligations and there are obligations around contracts and transparency arrangements, for example.

Further reading outside this code
See our separate guidance on:
The Guide to PECR
Controllers and processors

Can we ask individuals to send our direct marketing?

The direct marketing rules also apply to asking individuals to send your direct marketing 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.

Instigate does not necessarily mean that you have incentivised the individual to send your messages. Actively encouraging the individual to forward your direct marketing messages to their friends without actually providing a reward or benefit still means that you are instigating the sending of the message and you therefore need to comply with PECR.

Direct marketing emails and text messages require consent (the 'soft opt-in' does not apply in this situation) and you must be able to demonstrate this consent. As you have no direct contact with the people you are instigating the individual to send the direct marketing to, it is impossible for you to collect valid consent.

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

Example
An online retailer operates a 'refer a friend' scheme where individuals are given 10% off their orders if they participate. The individual provides their own name and email address and the retailer automatically generates an

email containing its marketing for the individual to send to their friends and family.

The retailer is instigating the direct marketing therefore they have responsibility for complying with the PECR rules. Because the retailer does not have the consent of the friends and family these emails 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, for example.

Relevant provisions in the legislation
PECR – see Regulation 22

Online advertising and new technologies

At a glance

Individuals may not understand how non-traditional direct marketing technologies work. Therefore it is particularly important that you are clear and transparent about what you intend to do with their personal data.

Individuals are unlikely to understand how you target them with marketing on social media so you must be upfront about targeting individuals in this way.

If you are planning to use cookies or similar technologies for direct marketing purposes you must provide clear and comprehensive information to the user about these and gain their consent (which must be to the GDPR standard).

Regardless of what technology or contact method you consider, you still need to comply with the GDPR and PECR. If you are using new technologies for marketing and online advertising, it is highly likely that you require a DPIA.

In more detail

What do we need to know when using new technologies for direct marketing?

Using new technologies for direct marketing can be very beneficial to you in reaching new or existing customers and supporters, such as those available in the digital or online environment.

However, the tools, techniques and amount of personal data available differ substantially from traditional advertising methods. Additionally, the personal

data you collect is often wider than that an individual actively provides to you. For example:

- 'observed data' – personal data you can obtain via observing how an individual uses or interacts with a technology or an online environment (eg the devices they use, the content they have generated); and
- 'inferred data' – personal data that is inferred or derived from the data provided or observed (eg inferences about the characteristics and interests of the user).

Individuals may not understand how these non-traditional marketing technologies work or how their data is used. As a result, these methods and technologies can have a greater potential impact on individual rights. It is therefore particularly important that you are clear and transparent about what you intend to do with this data and how you are processing it.

The type and volume of processing that you can undertake in the online world, and the risks associated with that processing, mean you are also highly likely to have to conduct a data protection impact assessment prior to the processing. See the section Do we need to complete a DPIA? for further information.

Is all online advertising covered by the direct marketing rules?

Whether your online advertising is covered by the direct marketing rules depends on your particular circumstances.

If your online advertising does not involve the processing of personal data – ie it is not based on any interests, behaviours or other information about individuals – then the GDPR will not apply.

For example, if the advertising is non-targeted (ie the same marketing is displayed to everyone who visits your website) or contextual (ie targeted to the content of the page rather than the identity or characteristics of the visitor) then this will not constitute direct marketing because it is not 'directed to' an individual.

However, even if your online advertising does not involve processing personal data, Regulation 6 of PECR may still apply. For example, you need to comply with Regulation 6 if you store information, or access information stored, on user devices (eg through cookies or similar technologies) – whether you do this for the purposes of online advertising or any other reason.

In the vast majority of cases, online advertising involves the use of cookies and similar technologies and therefore PECR applies. Additionally, if you engage in behavioural advertising – for example by personalising adverts on the basis of things like an individual's browsing history, purchase history or login information – this will constitute direct marketing. This is because the decision to target that particular user with a specific advert is based on what you know, or perceive to know, about the interests and characteristics of that individual and the device(s) they use.

What do we need to know if we use cookies and similar technologies for direct marketing purposes?

PECR does not have specific rules on online or behavioural advertising. However, if online behavioural advertising uses cookies or similar technologies it is covered by Regulation 6.

When we say 'cookies' we mean cookies and similar technologies. This covers any means you use to store information, or access information stored, on a user's device, including:

- first-party and third-party advertising cookies;
- fingerprinting techniques;
- tracking pixels and plugins, including those from third parties (such as social media platforms and ad networks/adtech providers); and
- other third party tracking technologies.

You may already use some of the above on your own website or be managing your advertising campaigns through using cookies on other organisation's websites, or both, whether through your direct relationship with that other organisation or via intermediaries.

If you are planning to use cookies for direct marketing purposes (whether or not they are targeted on the basis of those users' personal data), you need to comply with Regulation 6 by:

- providing users with clear and comprehensive information about the cookies etc that you intend to use; and
- getting their consent (which must be to the GDPR standard).

Regulation 6 contains two exemptions from these requirements, which are:

- the use of the cookie is necessary for the transmission of a communication; and
- the cookie is 'strictly necessary' for the provision of the online service the user requests (such as cookies used for authentication or security purposes).

Neither of these exemptions apply to online advertising (as well as tracking technologies and social media plugins). This means that you need to get consent from your users or subscribers for any cookie that you use for these purposes – whether the cookie is yours, or that of a third party.

You also need to explain what the cookies you use are doing as well as having valid consent. If you do not do either of these you will breach PECR. There are no alternatives to consent in PECR for the use of cookies. See the section How does consent apply to direct marketing? for further information.

As consent must be both freely given and a genuine choice, you also need to be very careful if you are considering requiring your users to 'agree' or 'accept' the setting of cookies for advertising purposes before they can access the content of your online service (this is known as a 'cookie wall').

This is because consent cannot be bundled up as a condition of a service unless it is necessary for that service. In many circumstances a cookie wall is unlikely to be appropriate as it will not demonstrate that you have valid consent.

How does the GDPR apply to online advertising?

It is clear that the GDPR applies if you are processing personal data such as an individual's name, account name or other similar information in the context of online advertising. However, even if you are targeting a particular user without knowing this sort of information, you still need to comply.

This is because you are 'singling out' a particular user and profiling them, making that user 'identified or identifiable, directly or indirectly', particularly when compared to other information you or another person may obtain or possess.

For example, this means that you must ensure that your processing is fair, lawful and transparent – this is particularly important if you are seeking to match an individual's 'online' behaviours with their 'offline' life.

Recital 58 of the GDPR specifically says online advertising is an area where it is important that you provide individuals with concise, easy to understand transparency information (additional highlighting):

> "The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. **This is of particular relevance in situations where the**

proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising…"

You need to have a lawful basis for your processing. In many circumstances it is likely that consent will be the most appropriate because PECR requires you to obtain consent when using cookies or similar technologies.

Also, if any of the personal data you process is special category data – for example where you target an individual because you infer that they might suffer from a particular condition on the basis that their browsing history contains medical websites – then you need an Article 9 condition in order to process that data.

Where Article 9 applies, you need to obtain the individual's explicit consent. See the section Can we use special category data for direct marketing? for further information.

Relevant provisions in the legislation
GDPR – see Recital 58 and Article 9
PECR – see Regulation 6

Further reading outside this code
See our separate guidance on:
Cookies and similar technologies
Consent

See also our Update report into adtech and real time bidding

How does direct marketing using social media work?

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

- personal data users provide (eg their account profile information);
- personal data observed through use of the platform – social media platforms process personal data about how their users interact with the service, (eg their activity on the platform and the devices they use to access it, 'off platform' data collected by third-party websites that include the platform's plugins or other technolgies);
- personal data inferred or derived about the user (eg data created on the basis of data provided by individuals or observed by their use of

the service). For example, social media platforms can generate 'insights' based on provided and observed data which constitute inferences about the characteristics and interests of the user.

Social media platforms may enable the targeting of individuals for direct marketing purposes based on all of the above types, alone or in combination.

It is therefore important to understand that, when you decide to use your social media presence to target direct marketing at individuals or use the platform's advertising services and technologies, many different data sources are likely to be used for this purpose. You need to be very clear about what data you will be using and why.

This type of targeted advertising on social media does not fall within the definition of electronic mail in PECR. However, if you use direct messaging on a social media platform, this is covered by Regulation 22 because this does constitute electronic mail. See the section Direct marketing by electronic mail (including emails and texts) for further information.

Can we target our customers or supporters on social media?

Social media platforms offer 'list-based' targeting tools that allow you to display direct marketing to users of the platform. This list-based targeting is where you upload personal data you already have to the platform (such as a list of email addresses). The platform then matches this data with its own user base. 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.

You must be transparent and clearly inform individuals 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 direct marketing.

You must be upfront about this processing. Individuals are unlikely to expect that this processing takes place, therefore you should not bury information about any list-based tools you use on social media within your privacy information. It is likely that consent is the appropriate lawful basis for this processing as it is difficult to see how it would meet the three-part test of the legitimate interests basis. However you will still need to ensure you also meet transparency requirements.

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, including by using list-based tools.

See the sections on Planning your marketing: DP by design, Generating leads and collecting contact details, and Profiling and data enrichment for further information.

Can we target people on social media who are similar to our customers or supporters?

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

These audiences 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 already target).

When you create this sort of audience, the social media platform uses data it has about other users of its platform to find people who match the interests and behaviours of people you already target with your marketing.

Additionally, the widespread use of social media plugins and tracking pixels on other websites can result in users being added to this sort of audience. So you need to be aware that this can take place and you must demonstrate that you have considered the data protection implications.

From a data protection perspective, these activities 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). Therefore it is likely that both you and the platform are joint controllers for this activity.

However, you may 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 transparency information to individuals. Particularly because this type of audience can change according to people's behaviour or interests.

You also need to inform individuals who have provided information to you that you intend to process their data to create these other audiences and ensure that you have a valid lawful basis.

If individuals have objected to the use of their personal data for marketing purposes, you also must not use their data for the creation of a 'lookalike' audience.

How are other technologies used in direct marketing?

There are a number of different ways to reach individuals with direct marketing, and in some cases these are increasingly popular. This section looks briefly at some of these and other emerging methods of direct marketing. It is not designed to be an exhaustive list. Regardless of what technology or contact method you consider, you still need comply with the GDPR and PECR.

You should also remember the use of new technologies, particularly where they are used for marketing and online advertising, is highly likely to require a DPIA – see the section Do we need to complete a DPIA? for further information.

Direct marketing on subscription TV, on-demand and 'over the top' (OTT) services

We use the term 'subscription TV' to cover any service that requires the user to subscribe, whether it is free or paid for. This includes online services that deliver content over the internet instead of traditional means (known as 'over the top' or OTT services) whether or not they require a set-top box, as well as on-demand or 'catch-up' services (which may also be a feature of a wider subscription TV service). These services may be entirely subscription-based, ad-supported, transactional (where the user pays for individual pieces of content), or a combination.

In many cases subscription TV involves profiling, such as to personalise the service towards the user. This can simply involve making programme recommendations based on analysis of the content the user accesses. However, profiling can also be more extensive and can involve combining and matching personal data from other sources and the use of cross-device tracking. For example when a user accesses the service on devices like their smart TV, desktop computer or via a mobile app.

Many providers have direct marketing services that are similar to those offered by social media platforms. Such as where you can provide a list of your customers or supporters and the provider shows your advert on their service to those who are also their customer, or you ask the provider to show your adverts to their subscribers who 'look like' your customers or supporters. The data protection issues are the same as using social media to target marketing, so you need to be transparent, fair and lawful. See the

section How does direct marketing using social media work? for further information.

You also need to assess whether PECR applies to your service, and take steps to comply. For example, the above type of targeted advertising on subscription TV does not fall within PECR's definition of electronic mail, so Regulation 22 does not apply. However, other PECR provisions may apply, depending on your service's circumstances.

Direct marketing using facial recognition or detection

Whilst facial recognition and detection technologies can be deployed in a number of circumstances, in the marketing context they generally involve billboards or digital screens in public spaces and retail establishments.

Facial recognition and detection involves processing biometric data. Facial recognition seeks to identify or verify a specific individual, whilst facial detection seeks to distinguish between different categories of individuals.

Biometric data is special category data when it is processed specifically 'for the purpose of uniquely identifying a natural person'. It is the end purpose of the processing which determines whether it is special category data, not whether the deployment has the technical capability to uniquely identify an individual.

It is unlikely that you will be able to use facial recognition technology to display direct marketing to specific individuals. It will be very difficult to comply with the lawfulness, fairness and transparency requirements of the GDPR when using the technology for this purpose.

Additionally, as facial recognition uses biometric data for the purposes of uniquely identifying an individual it constitutes special category data (whether this is for targeting them with direct marketing or other reasons). In order to process special category data to uniquely identify individuals for direct marketing, you must have their explicit consent under Article 9 of the GDPR (the other Article 9 conditions will not apply).

Unlike facial recognition, facial detection is not necessarily seeking to identify an individual but rather is segmenting the audience into categories – eg seeking to detect people's age, gender, facial attributes, their mood etc – and then showing them an advert based on these characteristics. Even in cases where a facial template is stored briefly and then deleted, this processing is likely to be personal data so the GDPR applies. However, categorisation does not automatically trigger Article 9. This is because it may not involve processing for the purposes of uniquely identifying an individual, but rather for the purposes of distinguishing one 'category' of people from another.

You must still be careful when using such technology and be clear about how it works and what the capabilities are. For example, a facial detection system may have the technical capability for use as a facial recognition system as well, depending on its features. Similarly, a facial detection system can still fall into Article 9 in some circumstances, such as where it stores a template to track the individual across an area covered by various screens and billboards (eg in a shopping centre). This is because it is then being used for the purposes of uniquely identifying that individual by singling them out, profiling their behaviour and taking some sort of action based on that processing. You also need to be careful of 'function creep' and remember that the GDPR requires you to only process the minimum of personal data necessary for your purpose.

Relevant provisions in the legislation
GDPR – see Article 4(14) and Article 9

Further reading outside of this code
See our guidance on
Special category data

See also EDPB Guidelines 03/2019 on processing of personal data through video devices

Direct marketing and in-game advertising

In-game advertising is where adverts are shown in computer or video games. It can take different forms such as an advert on an in-game billboard or an advert whilst the game loads; in many cases, the type of advertising used depends on the type of game in question.

Not all in-game advertising is covered by the direct marketing rules. For example, in-game advertising that is built into the game (eg 'static' in-game advertising) where all users see the same advert and that advert is not based on any characteristics of the users will not be in scope.

However, other types of in-game advertising that is more targeted at particular users (eg 'dynamic' in-game advertising) may be caught by the GDPR, particularly where it uses things like the user's location and other information such as time of the day the user plays to tailor the advertising.

You need to be transparent and fair with users so that they are aware that you will be targeting them with marketing in this way.

If you are sharing information such as the profile of the user or device information with third parties for direct marketing purposes this must also comply with the direct marketing rules.

Additionally, if your in-game advertising involves storing information, or accessing information stored, on user devices – whether these are gaming devices, PCs, mobile apps or anything else – then you also need to consider whether Regulation 6 of PECR applies.

Further reading outside of this code
See our separate guidance:
Draft Age appropriate design code

Direct marketing and mobile apps

Advertising within mobile apps generally works in the same way as on websites, with the use of technologies to connect the app to advertisers and developers. As with the web there can be many types of mobile app marketing, from display ads to video ads etc.

As with online advertising, you must comply with Regulation 6 of PECR if you use cookies and similar technologies as part of in-app marketing – whether this is for contextual or personalised advertising. This means that you must provide users with clear and comprehensive information about your use of cookies for these purposes and gain their consent. See the section What do we need to know when using new technology for direct marketing? for further information.

Even if you are not using cookies, it is likely that consent will be the appropriate lawful basis under the GDPR for any behavioural advertising or profiling that you wish to engage in for the same reasons as online advertising more generally.

It is also important to remember that consent must be separate and cannot be bundled into your terms and conditions for the use of your mobile app, unless you can demonstrate that consent for marketing is necessary for the provision of your service. See the section How does consent apply to direct marketing? for further information.

You must also be transparent and upfront about any advertising or profiling for this purpose and clearly explain what you want to use the data for.

Relevant provisions in the legislation
PECR – see Regulation 6

Further reading outside of this code

See the Article 29 Working Party (now the EDPB) Opinion 02/2013 on apps on smart devices

Direct marketing and the use of advertising IDs

Device operating systems such as Android or iOS incorporate unique identifiers which can be used for marketing purposes. These are known as the 'Google Advertising ID' (ADID) on Android, the 'Identifier for Advertising' (IDFA) on iOS and the 'Advertising ID' on Windows 10.

Whilst often described as an 'anonymous identifier', an advertising ID forms an example of an 'online identifier' which Recital 30 of the GDPR states can be personal data.

When the advertising ID is enabled, your mobile app may access and use it for personalised advertising, similar to how online services use unique identifiers stored in cookies. App developers and ad networks can therefore link personal data they process with advertising IDs as a means of providing personalised advertising across their apps and services.

You should also note that advertising IDs can also be used in other types of online behavioural advertising, such as real-time bidding. For example, they can be included in the exchange of data that takes place in this ecosystem.

If you decide to use advertising IDs in your marketing, you need to know the specific details of how the different platforms use these identifiers, the information and controls they provide to individuals (and what you also provide), and how your use links to other advertising techniques. You also need to consider compliance with other relevant laws such as PECR.

Location-based direct marketing

Location-based marketing, sometimes known as geo-targeting, is where data is processed from a user's device that indicates the geographical location of that device, including GPS data or data about connection with local wifi equipment. This data can be used to target marketing.

If you are considering using location-based marketing techniques you must be transparent and clearly tell people about this type of tracking. You are also likely to need consent for this type of marketing as it will be difficult for you to demonstrate that you can meet the legitimate interests requirements, especially as it is unlikely to be in people's reasonable expectations that you will track their location in order to send adverts to them.

Additionally, PECR has rules on the use of location data. Regulation 14 applies to situations where a network or service collects information about

the location of a user's phone or other device. For example tracing the location of a mobile phone from data collected by base stations on a mobile phone network to determine where it is or was.

However, these rules do not generally include GPS-based location information from smartphones, tablets, sat-navs or other devices, as this data is created and collected independently of the network or service provider. It also does not include location information collected at a purely local level (eg by wifi equipment installed by businesses offering wifi on their premises).

Ultimately you must be clear about whether PECR applies and comply where required.

Relevant provisions in the legislation
PECR – see Regulation 14

Further reading outside of this code
See our separate guidance:
Guide to PECR – location data
Draft Age appropriate design code

Direct marketing and connected devices

The term 'connected devices' covers 'Internet of Things' (IoT) devices like smart TVs, connected cars and wearables. It also covers broader concepts like smart cities.

It is important to note that where personal data is processed by connected devices, the GDPR applies. This is also the case if you seek to undertake direct marketing to users of connected devices.

Also, Regulation 6 of PECR generally applies to connected devices as in most cases they meet the definition of 'terminal equipment'. This means that if your marketing involves storing or accessing information from a user's connected device, you must comply with the requirements of Regulation 6.

See the section Is all online advertising covered by the direct marketing rules? for further information.

You must ensure that your processing is transparent and that you have a valid lawful basis if you want to use the data gained from connected devices for direct marketing purposes, including profiling, or you want to send advertising to users via connected devices.

If any of the data you are processing is special category data you need the user's explicit consent to process this for direct marketing purposes.

What due diligence do we need to do when considering using new technologies for direct marketing?

In most instances you will not be the developer of marketing or advertising technologies but rather you will be buying it in or using it to show your adverts. Given you are likely to have obligations under the GDPR and PECR, depending on the context, you need to undertake appropriate due diligence.

Examples of the types of due diligence you may want to consider include:

- Are you clear about the capabilities and functionality of the technology?
- Are you confident that what the product developer or provider is telling you is correct?
- Has the product developer or provider taken a data protection by design approach when developing the technology or service?
- Has the product developer or provider conducted a DPIA? (Although this may not be an obligation placed on them, it is good practice to undertake a DPIA, and this can also assist you in meeting your own requirements in this area. If the developer or provider is also your processor, they can assist you with your own DPIA.)
- Is any of the data special category data, and if so, how are the GDPR's requirements met?

You also need to have done your own DPIA where required, as well as ensuring you meet the other requirements of the GDPR and PECR.

Selling or sharing data

At a glance

If you are planning on selling or sharing personal data for direct marketing purposes you must ensure that it is fair and lawful to do so. You must also be transparent and tell people about the selling or sharing.

In more detail

Do we sell or share data?

There is a large trade in personal data for direct marketing purposes. A core part of the business of some organisations, such as data brokers, is selling or licensing data for direct marketing purposes. However selling data is not limited to these types of organisation. If you are contemplating selling or licensing data to other organisations you must ensure that you do so in compliance with the GDPR, and where applicable, PECR.

Sharing data for direct marketing purposes is not necessarily done for any monetary gain but is still mutually beneficial to you and the organisation you share it with. Lack of monetary exchange when you share the data does not absolve you from complying with the GDPR and PECR.

You need to be careful if you are planning on selling or sharing data for direct marketing purposes because you are responsible for ensuring that it is fair and lawful to do so.

Can we sell or share data for direct marketing purposes?

You must ensure that you comply with the GDPR when selling or sharing data for direct marketing purposes.

If you obtain personal data from individuals with the intention of selling or sharing these details on, you must make it clear that you want to sell to third parties for direct marketing purposes.

Likewise if you obtain data from sources other than the individual, you must be transparent and tell people about your intention to sell or share the data. See the section on Generating leads and collecting contact details for further information.

If you are seeking to rely on an individual's consent, you must ensure that the consent was valid to sell or share their data for direct marketing purposes (eg specific, unambiguous, informed, freely given) and that you have clear records of it. You cannot infer that you have consent just because you are selling the list to organisations with similar aims or objectives to you. See the section How does consent apply to direct marketing? for more information.

Example
A charity sells its supporter database to another charity. The charity selling the list believes that its supporters would not mind being contacted by the other charity because it campaigns on the same issues.

Such an assumption does not override the GDPR. The charity should have made clear to its supporters that it wanted to sell their details to another charity and obtained their consent to do so.

You may be able to lawfully disclose data on the basis of legitimate interests. These might be your own interests, or the interests of the third party receiving the data, or a combination of the two.

Your focus is on justifying your disclosure when you carry out the three-part test. Although the third party's intentions and interests are directly relevant, your focus is on whether the disclosure itself is justified for that purpose. The third party is responsible for ensuring their own further processing is fair and lawful, including carrying out their own three-part test if they plan to rely on legitimate interests as their basis for processing.

As part of your balancing test you need to take into account the reasonable expectations of individuals when determining if legitimate interests applies to your sharing or selling of the data. For example:

- Do you have an existing relationship with the individual? If so, what is the nature of that relationship?
- Did you collect data directly from the individual?
- What did you tell individuals at the time?

- If you obtained the data from a third party, what did they tell individuals about reuse of the data by third parties for other purposes?
- How long ago was the data collected?
- Is your intended purpose and method obvious or widely understood?

You also need to look at the impact on individuals of your selling or sharing their data for direct marketing purposes. For example, will individuals have a loss of control over their data if you sell it?

As a safeguard when you first collect the details from individuals, you should include a clear, simple opt-out opportunity for people to use if they object to you sharing or selling their details to third parties.

You cannot always use legitimate interests to sell data for direct marketing purposes. For example, to sell unconsented data for email marketing.

If you want to sell a marketing list for use in telephone campaigns you should make clear to buyers whether you have pre-screened it against the TPS register, and if so on what date it was last screened.

It is important that you maintain records of how and when you collected the details and what individuals were told – this is part of your accountability requirements under the GDPR. You should be able to give buyers proper assurances about the data that you are selling and demonstrate to them that it is compliant with the GDPR and PECR.

If you receive erasure or rectification requests you may be required to pass these down the chain to the third parties who you have sold or shared the personal data with. See the Individual Rights section for further information.

Remember it is a criminal offence under the DPA 2018 to knowingly or recklessly disclose, or procure the disclosure of, personal data without the consent of the controller. This means that if you sell or offer to sell a marketing list of customers where you do not have the consent of the controller to do this, then you are committing a criminal offence.

Relevant provisions in the legislation
DPA 2018 – see section 170 (unlawful obtaining of personal data)
GDPR – see Article 6(1)(a), 6(1)(f), Article 13 and 14 and Article 30

Further reading outside this code
See our separate guidance on:
Draft data sharing code of practice

Can we offer data broking services?

Data broking services involve collecting data about individuals from a variety of sources, then combining it and selling it on to other organisations. Data broking can involve providing a variety of services for other organisations including:

- selling lists of contact details;
- selling copies of the open electoral register;
- enrichment;
- profiling;
- data matching;
- data cleansing and tracing; and
- screening services.

If you operate as a data broker you are still subject to the GDPR and the majority of the processing that you undertake is likely to be for direct marketing purposes.

In most instances data brokers do not collect the data directly from individuals or have any direct relationship with them. Data brokers instead rely on data collected from other sources such as publicly available data, third parties (eg competition websites or lifestyle survey companies), or buying data from other data brokers. Therefore it is particularly important that your processing is transparent, fair and lawful.

You need to ensure that you provide individuals with privacy information that clearly explains what you will be doing with their data, what the source of their personal data is and how they can exercise their rights including the right to object to direct marketing. You must provide this information to the individual within a month of collecting their data. See the section on Generating leads and collecting contact details for further information.

If third parties are collecting and sharing personal data with you for direct marketing purposes on the basis of consent, then you must ensure that the consent is valid (eg freely given, specific, informed, unambiguous, separate from terms and conditions etc).

Where data is shared with you for direct marketing purposes on the basis of consent, then the appropriate lawful basis for your subsequent processing for direct marketing purposes will also be consent. It is not appropriate to switch to legitimate interests for your further processing for direct marketing purposes. Switching to legitimate interests would mean the original consent was no longer specific or informed, and misrepresented the degree of control and the nature of the relationship with the individual. This misrepresentation and the impact on the effectiveness of consent withdrawal mechanisms

would cause a problem with the balancing test, meaning that it would inevitably cause the balance to be against you.

If you are considering collecting and subsequently processing using legitimate interests as your lawful basis, you need to objectively work through the three-part test (the legitimate interests assessment) prior to the processing and record the outcome. A key part of the balancing test is the reasonable expectations of individuals, and transparency will be vital. It is unlikely to be in people's reasonable expectations that you will be building extensive profiles on them in order to sell these to lots of other organisations.

Example
The European Article 29 Working Party (which has been replace by the EDPB) was of the view that consent should be required for data brokering. It stated in Opinion 03/2013 on purpose limitation:

"…when an organisation specifically wants to analyse or predict the personal preferences, behaviour and attitudes of individual customers, which will subsequently inform 'measures or decisions' that are taken with regard to those customers... free, specific, informed and unambiguous 'opt-in' consent would almost always be required, otherwise further use cannot be considered compatible. Importantly, such consent should be required, for example, for tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research."

The Working Party reiterated this view in its Opinion 06/2014 on the notion of legitimate interests of the data controller. Whilst both of these Opinions relate to the old data protection regime this view is still relevant.

See the sections How does consent apply to direct marketing? and How does legitimate interests apply to direct marketing? for further information.

Remember that you must have the individual's explicit consent if any of the personal data that you are processing is special category data or inferred special category data.

You must have a process in place to deal with individuals' rights including how you will notify the third parties that you have disclosed the data to when an individual has exercised a particular right. See the section on Individual rights for further information.

Further reading outside this code
See our separate guidance on:
Legitimate interests

See also:
Article 29 Working party (which has been replaced by the EDPB)
Opinion 03/2013 on purpose limitation
Opinion 06/2014 on the notion of legitimate interests of the data controller
(whilst written under the previous data protection framework these are still relevant guidance).

Individual rights

At a glance

As well as the right to be informed, the rights to objection, rectification, erasure and access are the most likely to be relevant in the direct marketing context.

The right to object to direct marketing is absolute. This means if someone objects you must stop processing for direct marketing purposes (which is not limited to sending direct marketing). You should add their details to your suppression list so that you can screen any new marketing lists against it.

In more detail

What rights do individuals have?

Individuals have a number of rights under the GDPR, including the right to:

- object;
- rectification;
- erasure;
- access;
- restriction; and
- data portability.

Some of these rights are very relevant in the direct marketing context. Two of them – the right to restriction and the right to data portability – are less likely to be relevant. However it is still important to be aware that these are

available for individuals to use. Our Guide to GDPR contains further details on these two rights, if you need to know more.

The rights to objection, rectification, erasure and access are discussed in further detail in this section of the code.

Individuals also have the right to be informed – see the Generating leads and collecting contact details section for further information. In addition there are rights about automated decision making. See the section Can we use profiling to better target our direct marketing? for further information.

Relevant provisions in the legislation
GDPR – see Articles 13 and 14, Article 22, Article 15, Article 16, Article 17, Article 18, Article 20, and Article 21

Further reading outside this code
See our separate guidance on:
Individual rights
Right to restrict processing
Right to data portability

What do we do if someone objects to our direct marketing?

Individuals have the right to object to your processing of their personal data for direct marketing purposes. Article 21(2) says:

"Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing."

This is an absolute right. If someone objects, you must stop processing their personal data for these purposes. There are no exemptions or grounds for you to refuse the objection.

This right covers any processing that is for direct marketing **purposes** which includes profiling – it is not limited to sending direct marketing. This means that you must stop using their data for any direct marketing purposes. For example, using people's data to create direct marketing insights into particular geographical location or disclosing the data to third parties for direct marketing purposes.

You must make individuals aware of their right to object to processing for direct marketing purposes. Article 21(4) says this must be 'at the latest' at

the time of your first communication with them. This right must be explicitly brought to the individual's attention, presented clearly and separately from other matters, and in plain language. It is also important to remember that the right to be informed (Articles 13 and 14) requires you to tell people of their right to object when you collect their details. See the section on Generating leads and collecting contact details for further information.

Individuals can exercise their objection right at any time. This means they can object straight away or in advance of you using their data for direct marketing purposes. It may also be possible for an individual to object via a third party opt-out service.

Good practice recommendation
Provide mechanisms for individuals to easily object to your direct marketing at the time you collect their details (where this is not already required or where you are not relying on consent to process).

This is supported by the EDPB Profiling Guidelines which say:

"In line with Article 12(2) controllers who collect personal data from individuals with the aim of using it for direct marketing purposes should, at the moment of collection, consider offering data subjects an easy way to indicate that they do not wish their personal data to be used for direct marketing purposes, rather than requiring them to exercise their right to object at a later occasion." (footnote 31)

It must be free of charge for individuals to object. The GDPR does not specify how a valid objection should be made and there is no form of words that individuals must use. This also means that an individual could object verbally as well as in writing, and the objection could be made to any part of your organisation. You need to have a process in place to recognise and deal with objections to processing for direct marketing purposes.

If you have any reasonable doubts over the individual's identity, you can ask them for further information, but only what is necessary for you to action their objection. For example you may need to confirm what their email address or phone number is, in order to stop processing these details for direct marketing purposes.

Whilst you must comply with an objection to your direct marketing, this does not automatically mean that you need to erase the individual's personal data. In most cases it is preferable to suppress their details. See the sections on What are direct marketing suppression lists? and What do we do if someone asks us to erase their data? for further information.

An individual's most recent indication of their wishes about the receipt of your direct marketing is the most important. It is possible for an individual to change their mind about objecting to your direct marketing. For example, if an individual specifically withdraws their objection or in the future actively solicits direct marketing from you, then this would override their original objection. However failing to opt-out of your direct marketing at a later date (for example if you are using the electronic mail soft opt-in) does not override an individual's previous Article 21(2) objection.

Relevant provisions in the legislation
GDPR – see Article 21(2), 21(3), 21(4) and Recital 70, and Article 12, Article 13(2)(b) and Article 14(2)(c)

Further reading outside this code
See our separate guidance on:
Right to object

See also:
EDPB Guidelines on Automated individual decision-making and Profiling

What do we do if someone opts out of our direct marketing?

If someone opts out of your direct marketing, you must stop processing their data for the direct marketing purposes that the opt-out covers.

For example, if you are relying on the soft opt-in to send direct marketing emails to an individual and they use the 'unsubscribe' link within your email, you cannot send them any further marketing emails.

An opt-out of receiving direct marketing, such as the individual placing a tick in an opt-out box, has the same effect on your ability to use that method of contact as if the individual had issued an objection to direct marketing on that channel. This is because the individual is making it clear that they do not wish to be marketed to. However unlike an Article 21(2) objection, an opt-out is more likely to cover a specific method of contact or a particular direct marketing activity rather than being a general objection to all direct marketing purposes.

What do we do if someone withdraws their consent?

The GDPR gives people a specific right to withdraw their consent. They can choose to use this right at any time and it must be as easy for them to withdraw consent as it was to give it.

If an individual withdraws consent for their data to be used for direct marketing purposes, you must stop the processing that the consent covers immediately or as soon as possible. Whilst the withdrawal does not affect the lawfulness of your processing up to that point, you can no longer rely on consent as your lawful basis for direct marketing purposes.

You cannot swap from consent to another lawful basis for this processing at the point the individual withdraws consent. Even if you could originally have relied on a different lawful basis, once you choose to rely on consent you are handing control to the individual. It is inherently unfair to tell people they have a choice, but then continue the processing after they withdraw their consent.

This means that when an individual withdraws consent for you to use their data for direct marketing purposes, you cannot swap to legitimate interests in order to try to justify continuing the processing.

PECR refers to consent being given 'for the time being'. Therefore individuals can change their mind and decide that they no longer wish to consent to your electronic direct marketing communications.

The GDPR does not prevent a third party acting on behalf of an individual to withdraw their consent, but you need to be satisfied that the third party has the authority to do so. This leaves the door open for sectoral opt-out registers or other broader shared opt-out mechanisms, which could help individuals regain control they might feel they have lost. It might also help to demonstrate that consent is as easy to withdraw as it was to give.

Example
The Fundraising Regulator has set up the Fundraising Preference Service (FPS). The FPS operates as a mechanism to withdraw consent to charity fundraising. If an individual wishes to stop receiving marketing from particular charities, they can use the FPS to withdraw consent from those specific charities

Relevant provisions in the legislation
GDPR – see Article 7(3)

Further reading outside this code
See our separate guidance on:
Consent

What are direct marketing suppression lists?

Direct marketing suppression lists are a list of people who have told you that they do not want to receive direct marketing from you (eg by issuing an objection or unsubscribing). When someone tells you they do not want direct marketing from you, you should add them to your suppression list. Doing this, rather than simply deleting all record of the individual, means that you can screen any new direct marketing lists against it. This ensures that you do not send direct marketing to anyone who has asked you not to.

Suppression involves retaining just enough information about people to ensure that in future you respect their preference not to either receive direct marketing or have their data processed for direct marketing purposes.

Direct marketing suppression lists is not a concept in the GDPR or PECR, but if you do not use a suppression list you risk infringing the legislation by processing people's data for direct marketing purposes despite them having told you not to.

The GPDR does not prevent you from placing an individual onto a suppression list when they have objected to you processing their personal data for direct marketing purposes. The keeping of such a list is not in itself for direct marketing purposes, but in order to comply with your statutory obligations – so you will not infringe on the right to object by keeping one.

In fact in order to comply with the right to object it will be necessary for you to keep a suppression list to ensure that individuals' wishes and rights are complied with, so they do not receive direct marketing material from you in future or so that their data is not subsequently used for direct marketing purposes. Likewise if an individual has opted-out or told you not to send them electronic direct marketing messages you will breach PECR if you contact them again, therefore maintaining the suppression list is necessary to ensure that you comply.

The appropriate lawful basis for you to keep the minimum amount of an individual's data on a suppression list is likely to be 'necessary for compliance with a legal obligation' (Article 6(1)(c)).

You do need to clearly mark the data so that it is not processed for the direct marketing purposes the individual has objected to.

Example
An individual whose phone number is not on the TPS receives a live direct marketing call from a motor company. The individual asks the company not to call them again. In response the motor company simply deletes the individual's phone number.

A few months later the motor company buys in a list of telephone numbers that have been screened against the TPS. This list includes the individual number because it is not registered on the TPS. The motor company makes a further direct marketing call to the individual.

The motor company has breached PECR by calling the individual's number.

If the company had placed the number on a suppression list rather than simply deleting it, the breach would have been prevented. This is because screening the bought in list against the suppression list would have identified that there was an objection to receiving direct marketing calls on that number.

The TPS and CTPS registers are also types of suppression lists, and so too is the Mail Preference Service although this is not a statutory one, where individuals or organisations have actively registered an objection to receiving certain types of direct marketing.

You should not confuse direct marketing suppression lists which are used to record an individual's direct marketing objection with a screening list that you have decided to use to screen out certain people because they do not fit the particular direct marketing campaign that you or a third party are running.

Example
A lender decides they only want to send direct marketing to customers who have balances above a certain level. It screens out anyone with a balance that does not meet that threshold and creates a list of those people above it so it can use this again in future.

This is not a direct marketing suppression list because it is unrelated to an individual's wishes.

Relevant provisions in the legislation
GDPR – see Article 6(1)(c)

Further reading outside this code
See our separate guidance on:
Legal obligation

What do we do if someone tells us their data is inaccurate?

Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete – this is known as the right to rectification. They can do this verbally or in writing and you have one calendar month to respond to them.

Example
An individual regularly receives direct marketing from a travel company about cycling and walking holidays as they previously opted-in for information on these types of holidays. However the individual subsequently starts receiving direct marketing from the same company about holidays for the over 60's.

Because the individual is not over 60 (they are in fact in their 30's) they decide to contact the travel company and ask it to correct the inaccurate data about their age. The travel company corrects the data so it no longer indicates that the individual is over 60.

This right links to the accuracy principle. See the section How do we keep personal data we use for direct marketing accurate and up to date? for more information on accuracy.

If you are required to rectify the personal data, you may need to inform each recipient you have disclosed the data to, unless this proves impossible or involves disproportionate effort. If the individual asks you about who you have disclosed their data to, you need to tell them.

Example
A data broker receives a rectification request from an individual. The data broker corrects the incorrect data that it holds about the individual. It also informs the two organisations that it had sold the incorrect data to about the inaccuracy.

Relevant provisions in the legislation
GDPR – see Article 5(1)(d), Article 16, Article 19

Further reading outside this code
See our separate guidance on:
Right to rectification

What do we do if someone asks us to erase their data?

Individuals have the right to have their personal data erased (also known as 'the right to be forgotten'). This can include personal data processed for

direct marketing purposes. They can do this verbally or in writing and you have one month to respond to them.

This right is not absolute, it only applies in certain circumstances as listed in Article 17(1). The most relevant ones in a direct marketing context are likely to be if:

- you are relying on consent to process and the individual withdraws their consent;
- the personal data is no longer necessary for your direct marketing purpose; or
- the individual exercises their right to object to you processing their data for direct marketing purposes.

You must comply with the request if you receive an erasure request and any of the circumstances listed in Article 17(1) apply. There is an exception to this requirement, but you must be able to demonstrate that the processing is necessary for one of the reasons listed in Article 17(3). However these are narrow and are likely to be difficult to apply in the direct marketing context.

You do not need to automatically treat a withdrawal of consent or an objection to direct marketing as an erasure request. However in practice if someone withdraws their consent you no longer have a basis upon which to process for that purpose. So you are likely to need to erase that data (unless you need to keep a small amount for another purpose, such as a suppression list). Likewise if someone objects to the processing of their personal data for direct marketing purposes, you must stop that processing. Similarly, this is likely to mean that you may need to erase the data (unless you need a small amount for a suppression list).

Because we do not consider that a suppression list is processed for direct marketing purposes there would not be an automatic right to have the suppression list erased. Even if the right to erasure did arise, it is likely that you could show that Article 17(3)(b) applies because the processing of the suppression list to ensure that their wishes and rights are complied with is necessary for compliance with a legal obligation (ie the legal obligation not to use personal data for direct marketing purposes where someone has asked you not to). See the section What are direct marketing suppression lists? for further information.

Example
An individual contacts a company to issue an objection to direct marketing and at the same time asks it to delete their data. The company stops using the individual's data for direct marketing and erases all of it, apart from a small amount which it keeps on its suppression list. This prevents it from

using the individual's personal data for direct marketing purposes in the future.

There may be circumstances where reasons other than the right to erasure mean in practice that you need to delete or erase personal data. For example, if the circumstances change and you no longer have a lawful basis for processing the personal data, you discover that you hold excessive personal data, or the deletion is in line with your retention periods.

If you are required to erase personal data, you may need to inform each recipient you have disclosed the data to, unless this proves impossible or involves disproportionate effort. If the individual asks you about who you have disclosed their data to, you need to tell them.

Relevant provisions in the legislation
GDPR – see Article 17 and Recitals 65 and 66, and Article 19

Further reading outside this code
See our separate guidance on:
Right to erasure

What do we do if someone asks us for access to their data?

Individuals have the right of access to a copy of the personal data that you hold about them, which includes their data that you process for direct marketing purposes. Depending on what data you hold, this could include their contact details, online credentials, purchase history, or profile including any assumptions, categories or segments you have assigned to them (eg based on their location or behaviour).

Individuals can request access (which is commonly known as a 'subject access request') verbally or in writing. There are no set words that they must use to exercise this right but it must be clear that they are asking for their own personal data. You have one month to respond and in most cases you cannot charge a fee to deal with a subject access request.

Individuals are also entitled to other supplementary information about your processing of their personal data, however this largely corresponds to the information that you should provide in your privacy notice.

There are exemptions to this right, but whether any of these apply depends on the particular circumstances. See the section on Exemptions for further information.

Relevant provisions in the legislation
GDPR – see Article 15 and Recitals 63 and 64

Further reading outside this code
See our separate guidance on:
Right of access

Exemptions

At a glance

The DPA 2018 contains a number of exemptions from particular GDPR provisions and these add to the exceptions that are already built into certain GDPR provisions. There are no exemptions that specifically apply to processing for direct marketing purposes.

PECR contains very few exemptions. The two exemptions in Regulation 6 from the requirement to provide clear and comprehensive information and gain consent for cookies and similar technologies do not apply to online advertising, tracking technologies or social media plugins.

In more detail

What are exemptions?

If an exemption applies it means that you do not have to comply with the particular provision that the exemption discharges you from.

The DPA 2018 contains a number of exemptions from particular GDPR provisions. These add to and complement a number of exceptions already built-in to certain GDPR provisions. PECR also contain some limited exemptions.

You should consider exemptions on a case-by-case basis. You must be able to justify why you are relying on an exemption and ensure that you document this.

Are there any PECR exemptions that apply to direct marketing?

PECR contains very few exemptions and none generally apply to the rules on using electronic communications for sending direct marketing.

As discussed earlier in this code, Regulation 6 contains two exemptions to the requirement to provide clear and comprehensive information and gain consent for cookies and similar technologies. However neither of these exemptions apply for online advertising, tracking technologies and social media plugins. See the section Is all online advertising covered by the direct marketing rules? for further information.

Regulation 29 contains a law and crime exemption for 'communications providers', ie someone who provides or operates an electronic communications network or electronic communications service. It exempts communications providers from any of the rules in PECR if complying with that particular rule would breach a provision of another law. For example this exemption could be relevant if another law required a communications provider to send electronic direct marketing emails to individual subscribers.

If you are not a communications provider, you cannot use this exemption. So even if there is a law requiring you to send direct marketing, you must still comply with the PECR rules on sending electronic communications.

Relevant provisions in the legislation
PECR – see Regulation 6 and Regulation 29

Further reading outside this code
See our separate guidance on:
PECR exemptions

Are there any data protection exemptions that apply to direct marketing?

The DPA 2018 sets out a number of exemptions from some of the GDPR rights and provisions. Whether or not you can rely on an exemption generally depends on why you are processing the personal data.

Some exemptions apply simply because you have a particular purpose. Others only apply to the extent that complying with the GDPR would be likely to prejudice your purpose, or prevent or seriously impair you from processing personal data in a way that is required or necessary for your purpose.

The exemptions cover specific areas such as:

- crime, law and public protection;

- regulation, parliament and the judiciary;
- journalism, research and archiving;
- health, social work, education and child abuse;
- finance, management and negotiations;
- references and exams; and
- subject access requests where you hold information about other people.

There are no exemptions in the DPA 2018 that specifically apply to processing for direct marketing purposes. As previously discussed in the Individual rights section of this code, the right to object to direct marketing is absolute which means that you cannot exempt yourself from complying with such an objection.

Some of the provisions in the GDPR contain exceptions which set out when its requirements do not apply. In the case of Article 14, there are a number of exceptions to providing privacy information if the personal data has not been collected from the individual. See the section What do we need to tell people if we collect their data from other sources? for further information.

Relevant provisions in the legislation
DPA 2018 – see Schedules 2 to 4
GDPR – see Article 14(5)

Further reading outside this code
See our separate guidance on:
Exemptions guidance

Enforcement of this code

At a glance

The ICO upholds information rights in the public interest. We will monitor compliance with this code through proactive audits, will consider complaints and enforce the direct marketing rules in line with our Regulatory Action Policy. Adherence to this code will be a key measure of your compliance with data protection laws. If you do not follow this code, you will find it difficult to demonstrate that your processing complies with the GDPR or PECR.

In more detail

What is the role of the ICO?

The Information Commissioner is the independent supervisory authority for data protection in the UK.

Our mission is to uphold information rights for the public in the digital age. Our vision for data protection is to increase the confidence that the public have in organisations that process personal data. We offer advice and guidance, promote good practice, monitor and investigate breach reports, monitor compliance, conduct audits and advisory visits, consider complaints, and take enforcement action where appropriate. Our enforcement powers are set out in part 6 of the DPA 2018.

Our focus is on compliance with data protection legislation in the UK. In particular, to ensure that the direct marketing rules are adhered to.

Where the provisions of this code overlap with other regulators we will work with them to ensure a consistent and co-ordinated response.

How will the ICO monitor compliance?

We will monitor compliance with this code using the full range of measures available to us from intelligence gathering, using our audit or assessment powers to understand an issue, through to investigation and fining where necessary.

Our approach is to encourage compliance. Where we find issues we take fair, proportionate and timely regulatory action with a view to guaranteeing that individuals' information rights are properly protected.

How will the ICO deal with complaints?

If someone raises a concern with us about your compliance with this code or the way you have handled personal data or sent electronic messages in the context of direct marketing, we will record and consider it.

We will take this code into account when considering whether you have complied with the GDPR or PECR. In particular, when considering questions of fairness, lawfulness, transparency and accountability.

We will assess your initial response to the complaint, and we may contact you to ask some questions and give you a further opportunity to explain your position. We may also ask for details of your policies and procedures, your DPIA, and other relevant documentation. However, we expect you to be accountable for how you meet your obligations under GDPR and PECR, so you should make sure that when you initially respond to complaints from individuals you do so with a full and detailed explanation about how you use their personal data and how you comply.

If we consider that you have failed (or are failing) to comply with the GDPR or PECR, we have the power to take enforcement action. This may require you to take steps to bring your operations into compliance or we may decide to fine you. Or both.

What are the ICO's enforcement powers?

We have various powers to take action for a breach of the GDPR or PECR. We have a statutory duty to take the provisions of this code into account when enforcing the GDPR and PECR.

Tools at our disposal for data protection infringements include:

- assessment notices;
- warnings;
- reprimands;
- enforcement notices; and
- penalty notices (administrative fines).

For serious infringements of the data protection principles, we have the power to issue fines of up to €20 million or 4% of your annual worldwide turnover, whichever is higher.

We have several ways of taking action to change the behaviour of anyone who breaches PECR. These include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner can also serve a monetary penalty notice imposing a fine of up to £500,000 which can be issued against the organisation or its directors. These powers are not mutually exclusive. We will use them in combination where justified by the circumstances.

Relevant provisions in the legislation
DPA 2018 – see Part 6 Enforcement

Further reading outside this code
See our separate guidance on:
What we do
Make a complaint
Regulatory Action Policy

Annex A: Glossary

Glossary of terms

This glossary is included as a quick reference for key data protection and PECR terms and abbreviations used in this code.

Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Corporate subscriber	Corporate body with separate legal status - includes companies, limited liability partnerships, Scottish partnerships, and some government bodies.
CTPS	Corporate telephone preference service
DPA 2018	Data Protection Act 2018
DPIA	Data protection impact assessment
EDPB	European Data Protection Board (formally the Article 29 Working Party)
Electronic mail	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.
GDPR	General Data Protection Regulation
Individual subscriber	Individual customers (including sole traders) and other organisations (eg other types of partnership).

Joint controller	Where two or more controllers jointly determine the purposes and means of processing.
PECR	Privacy and Electronic Communications Regulations 2003
Personal data	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.
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
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.
Special category data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
Subscriber	A person who is party to a contract with a provider of public electronic communications services for the supply of such services.
TPS	Telephone preference service
User	Any individual using a public electronic communications service.