

# Direct marketing detailed guidance

Guidance summary	3
About this guidance	4
Navigating this guidance	8
Identify direct marketing	10
Plan direct marketing	15
Collect information and generate leads	36
Respect people's preferences	45
Enforcement	52
Annex A: Glossary	55
Annex B: Wider regulatory framework	58

# Guidance summary

## Guidance summary

- Direct marketing is important. It can help you grow your businesses and further your aims, add value to the customer experience and increase trust and confidence in your brand or organisation.
- This guidance will help you do direct marketing responsibly. It is a practical guide for those conducting direct marketing or those involved in it. It explains what you have to do to comply with the law and gives you good practice recommendations. It covers the following steps:

### Step 1: Identify

Does what you want to do count as direct marketing? Remember, direct marketing covers promoting aims and ideals as well as selling products and services.

### Step 2: Plan

Take a data protection by design approach, planning how you will protect people's information from the start. Think about what information you want to use and how you want to get your direct marketing to people. And make sure you have a data protection reason ("lawful basis") for your direct marketing.

### Step 3: Collect

Collect information for direct marketing fairly and clearly explain to people how you plan to use their information.

### Step 4: Respect

Always respect people's preferences. People have an absolute right to object to or opt out of direct marketing at any time.

#### ■ [Latest updates](#)

**5 December 2022** - This guidance was published.

# About this guidance

This guidance covers the UK data protection regime which is the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR). It also covers the Privacy and Electronic Communications Regulations 2003 (as amended) (PECR), where this applies to direct marketing.

## In more detail

- [Who is this guidance for?](#)
- [Why is it important to get direct marketing right?](#)
- [What laws cover direct marketing?](#)
- [How should we use this guidance?](#)
- [What happens if we don't follow this guidance?](#)

## Who is this guidance for?

This guidance is for everyone who intends to conduct marketing directed to particular people and those more broadly involved in direct marketing. It supports and empowers responsible direct marketing, helping you develop positive, trusted relationships with your customers and supporters while protecting people from unwanted intrusion. It provides you with practical guidance on the law and good practice.

It is for you, if you use information with the intention to market, advertise, or promote products, services, aims or ideals. For example:

- commercial businesses marketing products and services;
- charities and third sector organisations fundraising or promoting aims and ideals;
- political parties fundraising or canvassing for votes;
- public authorities promoting commercial services or sending promotional messages that aren't necessary for public tasks or functions (eg messages from a local authority promoting its gym);
- organisations involved in buying, selling, or profiling personal information for direct marketing purposes; or
- telemarketing companies, lead generators, marketing agencies, and those providing advice on marketing campaigns.

It is likely that the majority of organisations, large and small, will at some stage use direct marketing to connect with customers or supporters or find new ones.

### Further reading

If you are involved in political campaigning, you can find tailored advice in our [guidance for the use of personal data in political campaigning](#).

If you are a public authority considering promotional messages necessary for your task or function, you

## Why is it important to get direct marketing right?

Direct marketing is important. It can help you grow your business or further your aims, and it can benefit competition across markets. It can add value to the customer experience, making people aware of new products and services that they may benefit from, giving them opportunities to take part in events or find out about important causes. When done responsibly direct marketing can also increase trust and confidence in your brand or organisation.

It is important to get direct marketing right so you maintain these benefits. Bombarding your customers with direct marketing messages they don't want can alienate them and damage relationships.

When organisations don't get things right, direct marketing can cause nuisance or anxiety or other harm. Ofcom research published in 2019 found that 83% of those who received any type of sales calls found them annoying and 11% found them distressing, both of which were increases on its previous research (see the further reading box for more information).



In some cases direct marketing can result in significant harm. For example, someone in financial difficulties who is regularly targeted with direct marketing for high interest loans might sign up for these offers and potentially incur more debt. This is harmful for the people affected, can undermine the important role direct marketing plays in the UK economy, and create negative perceptions. For example, Gambling Commission research in 2019 on consumer attitudes towards gambling advertising found that people perceived that those at most risk of problematic play were being targeted with the advertising (see the further reading box for more information).

The rules are not there to stop you from engaging in direct marketing. They are there to make sure you think about the privacy of those who will be affected by your activity. The law enables good direct marketing practices to happen for the benefit of all involved.

The benefits for you in following the guidance may include:

- greater trust in you by the public and your customers in how you use people's information for direct marketing purposes;
- greater confidence within your organisation that you are engaging in direct marketing responsibly and in a way that complies with the law;
- economic benefits from effective, responsible direct marketing; and
- better protection for people from unwanted or nuisance marketing.

### Further reading

- [Ofcom research on nuisance calls 2019](#) 
- [Gambling Commission research on consumer attitudes towards gambling advertising 2019](#) 

## What laws cover direct marketing?

Where direct marketing uses personal information, it is covered by the UK data protection regime. This is set out in the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR).

Where direct marketing is carried out using electronic marketing messages (eg phone calls or electronic mail such as emails or text messages), it is also covered by the Privacy and Electronic Communications Regulations 2003 (as amended) (PECR). PECR also covers cookies and similar technologies. In some ways it has a broader application than data protection law, as it can apply even if you are not using any personal information.

There are other rules and industry standards affecting direct marketing that are regulated by other bodies. For more information see [Annex B](#).

### **What is a legal requirement in this guidance and what is good practice?**

This guidance covers what you must do to comply with data protection law and PECR. Where we use the word “must”, this means that the law requires you to do something (so it is a legal requirement).

Where we use the word “should”, this isn't a legal requirement but is what we expect you to do to comply effectively with the law. You should follow this unless you have a good reason not to (good practice). If you take a different approach, you must be able to demonstrate that this complies with the law. Where we use the word “could”, this refers to an option(s) that you may want to consider to help you comply (good practice). We have highlighted these words throughout the guidance for ease of reference.

### **How should we use this guidance?**

This guidance helps you understand what you need to do at each stage of your direct marketing:

#### **Step 1: Identify**

#### **Step 2: Plan**

#### **Step 3: Collect**

#### **Step 4: Respect**

It explains the steps you are likely to go through as part of your direct marketing activities. It starts with a section about identifying what is direct marketing to help you decide if what you want to do is covered. Further sections cover planning your marketing activities, collecting information, and respecting people's preferences. There is a [Glossary](#) to help you understand the terms we use in the guidance.

The guidance is designed to set out the main things you need to consider or do when you carry out direct marketing. However, we know some of you may want more detail about particular areas, so we have included “further reading” boxes. These boxes do not form part of the guidance but highlight where to find more detail if you want it.

Also, our website has further practical direct marketing resources and tools to help you.

### Further reading

- [The Guide to Data protection](#)
- [The Guide to PECR](#)
- For other direct marketing tools and resources, see our [direct marketing guidance and resources page](#).
- For how to make an enquiry, see the [contact us](#) section of our website.

## What happens if we don't follow this guidance?

If you don't follow this guidance you may find it more difficult to show that your direct marketing complies with data protection law and PECR.

We can take action against you if you send direct marketing or use personal information in a way that infringes the UK GDPR, DPA 2018 or PECR. For more information, see the [Enforcement](#) section.

As long as you can demonstrate that you found another way to comply with the law, you will not receive a penalty if you fail to adopt our good practice recommendations.

# Navigating this guidance

## Identify direct marketing

- What is direct marketing?
- What are direct marketing purposes?
- What are service messages?
- How can we decide if what we want to do is direct marketing?

## Plan direct marketing

- Why it is important to plan our direct marketing activities?
- What type of information do we want to use?
  - Can we use special category data for direct marketing?
  - Can we use children's information for direct marketing?
- What direct marketing activity do we want to do?
  - Can we use 'live' calls for our direct marketing?
  - Can we use automated calls for our direct marketing?
  - Can we use electronic mail (including emails and texts) for our direct marketing?
  - Can we use post to send our direct marketing?
  - Can we use online advertising for our direct marketing?
  - Can we use social media for our direct marketing?
  - Is there any information we must give people when we send direct marketing to them?
  - Can we share information for direct marketing purposes?
- Can we work with others on our direct marketing?
- How do we decide what our data protection reason ("lawful basis") is for direct marketing?
  - How does consent apply to direct marketing?
  - How does legitimate interests apply to direct marketing?
- How do we make sure the information we use for direct marketing is accurate?
- How long should we keep information for direct marketing purposes?

## Collect information and generate leads

- What is collecting information and generating leads for direct marketing?
  - What do we need to tell people if we collect their information directly from them?
  - What do we need to tell people if we collect their information from other sources?
  - Can we use publicly available personal information for direct marketing purposes?
-



- Can we find out additional contact details for people from other sources?
- Can we get new contact details for people from other sources, if their details are no longer correct?
- Can create profiles of people for direct marketing?
- What do we need to consider when buying or renting information for direct marketing?

## Respect people's preferences

- Why is it important to respect people's preferences?
- What do we do if someone objects to our direct marketing?
- What do we do if someone opts out of our direct marketing?
- What do we do if someone withdraws their consent?
- What are direct marketing suppression lists?
- What do we do if someone asks us to delete their information?

## Enforcement

- What is the role of the ICO?
- How does the ICO deal with complaints?
- What are the ICO's enforcement powers?

# Identify direct marketing

## At a glance

Not everything you want to do will be considered direct marketing. But it is important to check if it is, so you can comply with all the relevant rules.

Direct marketing includes promoting your aims and ideals, as well as advertising your products or services. This means it includes fundraising and campaigning.

Direct marketing is not just about sending messages. It can include activities that lead up to, enable or support you sending direct marketing (such as targeting and profiling).

## In more detail

- [What is direct marketing?](#)
- [What are direct marketing purposes?](#)
- [What are service messages?](#)
- [How can we decide if what we want to do is direct marketing?](#)

## What is direct marketing?

The definition of direct marketing is taken from the DPA 2018 and is also used in PECR. The DPA 2018 says direct marketing means:



“the communication (by whatever means) of advertising or marketing material which is directed to particular individuals”

This definition is sector neutral which means any type of organisation can engage in direct marketing. However, if a public authority can demonstrate that the promotional message it is sending is necessary for its task or function, then this doesn't count as direct marketing (see the further reading box).

The definition breaks down as follows:

- **Advertising or marketing material**

This is interpreted widely and covers any advertising, promotions or marketing material. It includes:

- commercial marketing of products and services; and
- promotion of aims and ideals such as fundraising, political campaigning or corporate initiatives that promote community or charitable work.

Contacting people to conduct genuine market research is not direct marketing. However, if your market

research messages include promotional material, or if the research is ultimately being carried out for you or others to send direct marketing to the people involved, then this is direct marketing. This is sometimes referred to as 'sugging' (selling under the guise of research).

- **Communication (by whatever means)**

Any type of communication that you might decide to use for your direct marketing. For example:

- emails or text messages;
- phone calls;
- post;
- online behavioural advertising; or
- social media marketing.

It can also cover any type of non-traditional or emerging types of communication or approach.

- **Directed to particular individuals**

This means that the marketing material must be "directed to" a particular person or categories of people. 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 user (eg based on browsing history, purchase history or login information); and
- advertising on social media that is targeted to a particular person (eg by using direct messaging or tagging a particular person into an advertising post).

Marketing is not "directed to" if it is indiscriminate blanket marketing. For example:

- leaflets delivered to every house in an area;
- magazine inserts;
- online adverts shown to everyone who views a website; or
- an advertising post on social media that is broadcast to all followers of the account or all users of the platform.

However, simply removing someone's name from the marketing material doesn't stop it from still being directed to that person.

## Further Reading

 [Relevant provisions in PECR – see Regulation 2\(2\)](#) 

External link

 [Relevant provisions in DPA 2018 – see Section 122\(5\) \(definition\), Schedule 19 paragraph 430 and paragraph 432\(6\)](#) 

### Further reading

If you are a public authority, see our [guidance on direct marketing and the public sector](#).

## What are direct marketing purposes?

Direct marketing is wider than just sending messages to people. It includes all the activities you do with people's information that lead up to, directly enable or support sending your direct marketing messages. The focus is on why you are doing something rather than the activity itself.

For example:

- building a profile on someone with the intention of using this to target them with advertising;
- generating leads for advertising purposes (eg cold calling people);
- data cleansing, matching or screening for direct marketing;
- list brokering;
- sharing data with third parties for them to use for their own direct marketing; and
- contacting people to ask them for consent to direct marketing.

### 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 doesn't contain any of these discounts or offers, the hotel is still sending it for direct marketing purposes.

## What are service messages?

Data protection law and PECR don't stop you from telling your customers important information that they need to know as part of their relationship with you.

This type of communication is often referred to as a 'service message'. It covers messages that aren't promotional but are for administrative or customer services purposes, such as messages to:

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

### Example

A gym makes a telephone call to a customer. The purpose of the call is simply to advise the customer that their monthly membership payment hasn't worked. Therefore, the call doesn't count as direct marketing.

If your service message has elements that are direct marketing, even if that is not the main purpose of your message, then it will count as direct marketing. However, if your service message contains general branding or logos, this doesn't count as direct marketing.

### Example

During the call to a customer about the problems with their payment, the gym also outlines its personal training services. Although the main purpose of the call is for administration, because the gym is also using the call to promote its services, it now falls within the definition of direct marketing.

How can we decide if what we want to do is direct marketing?

In most cases, it will be clear to you that what you want to do is direct marketing. However, if you are unsure you **should**:

- think about why you want to use the information (eg are you using it so that you can build a profile on someone to send them marketing or for anything else that supports you sending direct marketing?);
- think about why you want to communicate with people (eg are you trying to influence their behaviour?); and
- look at whether the content is promotional (eg does it advertise products or services or promote you or your interests?).

If you want to send a message that actively promotes or encourages people to make use of a particular service, special offer, or upgrade, then it is likely to be direct marketing.

If you have a relationship with a person, the phrasing, tone and context are likely to be a key factor in whether the message you want to send is direct marketing. For example, if a message has a neutral tone and simply gives information that they need to know as part of their relationship with you this is more likely to be a service message.

### Example

A mobile phone company needs to tell their customer that they are reaching their monthly data limit.

---

The company sends a text message to the customer about this, advising what the charges will be if the customer exceeds the limit and signposting to further information:

"You are approaching your monthly data limit. Any data that you use over your allowance will be charged at XX. For more information including your data bundle options go to [company.com](https://company.com)."

Because this message is about their account and purely informative and neutral in tone, it is likely to be a service message.

However, if the company used the message to encourage the customer to take up a special offer to buy more data, then this would be direct marketing. For example:

"You are approaching your monthly data limit. Any data that you use over your allowance will be charged at XX. But don't worry, as we have a special data offer just for you. For more information and to see your exclusive offer go to [company.com](https://company.com)."

Other examples of when a message may not be direct marketing include:

- factual information reminding customers of a benefit on their account but not encouraging them to use the benefit (eg reminding customers that their bank account includes free travel insurance);
- advising customers in a factual way of the options available to them at the end of their contract without encouraging or promoting one option over another; and
- automatic renewal notices that are worded neutrally and don't encourage customers to renew.

However, simply using a neutral tone doesn't necessarily avoid messages being direct marketing. This is because the context in which you send the message is also important. For example, a message sent to a person by a supermarket which says "Your local supermarket stocks leading brands" is clearly still promotional, despite the neutral tone. In this context, the purpose of the message is to promote the supermarket.

# Plan direct marketing

## At a glance

Planning your direct marketing before you start means that you can make sure it complies with the law. It is important to think about:

- what type of information you want to use;
- what you want to do with the information;
- who is responsible for compliance when you work with others;
- what your data protection reason ("lawful basis") will be; and
- how you will ensure the information is accurate and not kept for longer than you need it.

## In more detail

- Why it is important to plan our direct marketing activities?
- What type of information do we want to use?
  - Can we use special category data for direct marketing?
  - Can we use children's information for direct marketing?
- What direct marketing activity do we want to do?
  - Can we use 'live' calls for our direct marketing?
  - Can we use automated calls for our direct marketing?
  - Can we use electronic mail (including emails and texts) for our direct marketing?
  - Can we use post to send our direct marketing?
  - Can we use online advertising for our direct marketing?
  - Can we use social media for our direct marketing?
  - Is there any information we must give people when we send direct marketing to them?
  - Can we share information for direct marketing purposes?
- Can we work with others on our direct marketing?
- How do we decide what our data protection reason ("lawful basis") is for direct marketing?
  - How does consent apply to direct marketing?
  - How does legitimate interests apply to direct marketing?
- How do we make sure the information we use for direct marketing is accurate?
- How long should we keep information for direct marketing purposes?

## Why is it important to plan our direct marketing activities?

You **should** plan your direct marketing activity before you start so that you can build-in data protection and

PECR compliance. It is hard to retrofit legal requirements once you have started your activity and it may be costly. You may find that not planning properly means you are infringing the law. This may harm your reputation and your relationship with people. It may also result in us taking action against you.

In general, the data protection rules covering direct marketing are the same as when you use people's information for any reason (the main difference is people have an absolute right to object to direct marketing).

You **must** take a 'data protection by design' approach when planning your direct marketing campaign or activity. For example, you **should** consider:

- what type of information you want to use (eg is it personal information, special category data or children's information?);
- what direct marketing activity you want to use the information for;
- who is responsible for compliance when you work with others;
- what data protection reason ("lawful basis") applies to your activity; and
- how will you ensure the information is accurate and not kept longer than you need it.

You **must** also be aware of whether any additional rules apply to the information you want to use or to the activity you want to carry out. You **must** be clear which legislation applies to your direct marketing activities so you can follow all the relevant rules. In some cases only data protection law or only PECR will apply, but in other circumstances all may apply.

## Further Reading

 [Relevant provisions in the UK GDPR – see Article 5\(2\), Article 25 and Recital 78](#) 

External link

### Further reading

- [Data Protection by design and default](#)
- [Accountability and governance](#) guidance and [Accountability Framework](#) (to help you demonstrate your compliance)

## What type of information do we want to use?

You **should** think about what type of information you want to use for your direct marketing activity before you start. This will help you know which rules apply.

For example, if you want to use personal information, then you **must** comply with data protection law. Personal information can simply be someone's name and address but it is also broader. It covers distinguishing between people and singling them out. For example, in the direct marketing context, personal information covers:

- a person's email address;



- a business email address if this identifies a person (eg [\[email protected\]](#)); and
- online identifiers such as cookie IDs, IP addresses or advertising IDs.

If you want to use contact details, such as a phone number or electronic mail address (eg email address), then PECR applies (as well as data protection law if your marketing involves using personal information).

### Further reading

If you want to find out more about personal information, see our guidance on [what is personal data?](#)

## Can we use special category data for direct marketing?

Special category data includes information about people's racial or ethnic origin, political opinions, religious beliefs, health or sexual life. It is more sensitive and therefore the law requires a higher standard of protection. This means that you **must** have a special category condition, as well as a data protection reason ("lawful basis") to use the information.

You **should** have "explicit consent". This is because it is unlikely that any other special category condition applies.

Explicit consent has to meet the usual standard for consent (see [How does consent apply to direct marketing?](#)). However, the key difference, is that people **must** agree in a clear statement to you using such information rather than an 'affirmative action'. You **must** also specify the type of special category data you want to use and your explicit consent request **should** be separate from any other consents.

You may be using special category data if you are trying to better target your direct marketing by profiling people. For example, drawing inferences about people's race, political opinions or health from other information.

## Further Reading

 [Relevant provisions in the DPA 2018 – see Sections 10, 11 and Schedule 1](#) 

External link

 [Relevant provisions in the UK GDPR – see Article 9 and Article 9\(2\)\(a\), and Recital 43](#) 

External link

### Further reading

- [Special category data](#)
- If you are a political party, see our [guidance for the use of personal data in political campaigning](#).

## Can we use children's information for direct marketing?

Direct marketing to children has significant potential for harm. Other regulators have rules that specifically

protect children from advertising (see the further reading box). Therefore, you **should** be very careful when you plan such a campaign.

You **must** take into account the risks to children of using their information for direct marketing and think about how you can mitigate these. For example, children might:

- not realise that you want to use their information for direct marketing (this may lead to them getting direct marketing that they don't want);
- not understand what direct marketing is or how it works (this may mean they don't recognise when something is direct marketing);
- lack awareness of the consequences of giving you their information;
- be unable to critically assess the content of direct marketing (eg they may be influenced to make unhealthy food choices or spend money on things they can't afford).

You **should** also comply with advertising standards and make sure that your direct marketing is not detrimental to a child's health or wellbeing.

If you're providing online services that are likely to be accessed by children, you **should** read the ICO's Children's code.

## Further Reading



[Relevant provisions in the UK GDPR – see Recital 38 and 58](#)

External link

### Further reading

- [Children and the UK GDPR](#) (for more guidance on using their information)
- The Children's code ([Age appropriate design code of practice](#))
- See also sector-specific guidance on marketing children. For example, the [Advertising Standards Authority](#) enforces the [CAP code](#) which includes specific rules to protect children from advertising.

## What direct marketing activity do we want to do?

You **should** think about what direct marketing activity you want to carry out, before you collect the information. For example, do you want to:

- make [live marketing phone calls](#) or [automated marketing phone calls](#);
- send direct marketing by [electronic mail](#) or by [post](#);
- use [online advertising](#) or [social media marketing](#); or
- [share information](#) for direct marketing with other organisations?

Being clear about what you want to do with the information before you start means that you can follow all the relevant rules. This includes providing any information [you must give people at the time of your](#)

You **must** also think about what information is necessary and proportionate to use for your activity and how you will make sure the activity is fair to people.

- **Can we use 'live' calls for our direct marketing?**

'Live' direct marketing calls are when a person is speaking live on the telephone. Direct marketing by live calls is covered by different provisions of PECR, depending on what the call is about. The live call rules protect individual and corporate subscribers (see the [Glossary](#) for definitions).

Live calls can be a useful direct marketing method, allowing you to speak directly to people and discuss your promotions with them. However, some people find live direct marketing calls intrusive or a nuisance. For example, Ofcom nuisance calls research in 2019 found that 82% of people receiving live sales calls found these annoying (see the further reading box). Therefore, you **must** make sure you understand how to comply. For example:

- **Be clear what your live marketing call will be about.**

There are different rules in PECR for live calls depending on what you are marketing. However, for most types of marketing you can make live calls if:

- there is no objection to your calls; and
- the number isn't registered on the Telephone Preference Service (TPS) or the Corporate Telephone Preference Service (CTPS).

### **Example**

A company has a list of telephone numbers that it wants to use to make live marketing calls about its products.

In order to comply with PECR, it checks the numbers against the TPS and CTPS registers and against its own 'do not call' list. It doesn't make calls to any numbers that it finds on the register or its own list. It calls the remaining numbers.

However, there are stricter rules for direct marketing calls about claims management services and pensions. For claims management services marketing calls, you **must** have consent.

For pension scheme marketing calls:

- you **must** be a trustee or manager of a pension scheme or authorised by the Financial Conduct Authority; and
- the person you are calling **must** have consented to your calls or your relationship with them **must** meet strict criteria (see the further reading box).

- **Understand what the TPS and CTPS are.**

The TPS and CTPS registers are statutory registers that act as a way to let people record a general objection to receiving live direct marketing calls that you **must** respect. You can only call a number on these registers if the subscriber has specifically told you they want your live marketing calls.



- **Be considerate to people.**

You **should not** make calls to people that would unduly distress them 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 anti-social hours.

Remember, if you are using personal information, you **must** comply with data protection law as well as PECR (see [What type of information do we want to use?](#)).


For details on the information you **must** give people when making live marketing calls, see [Is there any information we must give people when we send direct marketing to them?](#).

## Further Reading

 [Relevant provisions in PECR – see Regulations 21, 21A, 21B, and 26](#) 

External link

### Further reading

- If you need more detailed information on making live calls, including on pension scheme calls and claim management services calls, see our [guidance on direct marketing using live calls](#).
- If you want to make live marketing calls to other businesses, see our [guidance on business-to-business marketing](#).
- [Ofcom research on nuisance calls 2019](#) 

## Can we use automated calls for our direct marketing?

Direct marketing by automated telephone calls are made by an automated dialling system that plays a recorded message. The automated marketing call rules in PECR protect individual and corporate subscribers (see the [Glossary](#) for definitions).

You may be considering automated marketing calls as a cheaper alternative to live calls. However, the rules are stricter as many people find such calls very intrusive and sometimes disturbing. For example, Ofcom research from 2019 on nuisance calls found that 84% of people found recorded sales calls annoying and 14% found this type of call distressing (see the further reading box).

You **must** have consent to make automated marketing calls. General consent for direct marketing, or even consent for live calls, is not enough. The consent **must** specifically cover automated marketing calls from you. (See [How does consent apply to direct marketing?](#))

You don't need to check against the TPS or CTPS because you **must not** make the call without consent, even if the number is not on these lists.

Remember, you **must** comply with data protection law as well as PECR if you are using personal information (see [What type of information do we want to use?](#)).


For details about the information you **must** give people when making automated marketing calls, see [Is there any information we must give people when we send direct marketing to them?](#).

## Further Reading

 [Relevant provisions in PECR – see Regulation 19](#) 

External link

### Further reading

- [The Guide to PECR: Telephone marketing](#)
- If you want to make automated marketing calls to other businesses, see our [guidance on business-to-business marketing](#).
- [Ofcom research on nuisance calls 2019](#) 

## Can we use electronic mail (including emails and texts) for our direct marketing?

Electronic mail means any electronically stored messages (eg emails, text messages, picture or video messages, voicemails, and direct messaging on social media). In particular, emails and text messages are a popular, cost-effective way to deliver marketing messages to people.

If you want to send direct marketing by electronic mail, you **must** do the following:

- **Be clear what type of subscriber you want to send messages to.**

There are two types of subscribers in PECR (individual and corporate). Some of the rules for electronic mail only protect individual subscribers (which includes sole traders and some types of partnership). So, if you want to send electronic mail marketing to corporate subscribers the PECR rules on having either consent or the 'soft opt-in' (see below) don't apply. (See the [Glossary](#) for more information on subscribers.)

- **Understand when you need consent.**

You **must** have consent to send electronic mail marketing to individual subscribers (unless the 'soft opt-in' applies, see below). If you want to rely on consent, you **must** ensure it is specific to the particular type of electronic mail you want to send. For example, consent specifically for emails or consent specifically for text messages; simply saying 'electronic mail' is not specific or informed enough.

It is important to remember that consent to use someone's phone number for live or automated marketing calls doesn't cover direct marketing by text message. (See the section [How does consent apply to direct marketing?](#))

---

### Example

A customer is buying a pair of jeans from a high street retailer. At the end of the payment the shop assistant asks them if they would like their receipt sent by email. The customer agrees and gives their email address.

Later that day the customer receives an email that contains an electronic receipt of their purchase. However, the following day they receive a further email promoting the retailer's footwear sale.

While the first email was compliant because it didn't contain any marketing, the second email is not compliant with PECR. This is because although the customer consented to their email address being used to receive an e-receipt, they didn't consent for it to be used for direct marketing. Consent for an e-receipt doesn't cover sending direct marketing. The retailer should have clearly and separately asked for consent to send direct marketing by email.

As no information was given to the customer about their email address being used for direct marketing purposes, there are also likely to be data protection issues (eg fairness and transparency).

- **Understand how to comply with the 'soft opt-in'.**

The term 'soft opt-in' is not used in PECR, but is commonly used to describe the exception in the law to the electronic mail consent requirement. Many organisations find that the soft-opt in is a good option to use to send electronic mail to their existing customers. However, if you want to use it instead of consent, you **must** meet all of its requirements. The soft opt-in breaks down into five requirements:

1. **You obtained the contact details** – you **must** have obtained the contact details directly from the individual subscriber you want to send electronic mail to.
2. **You did this during the course of a sale, or negotiation of a sale, of a product or service** – they **must** have bought something from you or have actively expressed an interest in buying your products or services (eg by asking for a quote or more details of what you offer).
3. **You are marketing your similar products and services** – you **must** be sending electronic mail about your similar products and services. This means you can't send messages about things that people wouldn't reasonably expect from you in that context and you can't send the marketing of other organisations.
4. **You provided an opportunity to refuse or opt-out when you collected the details** – you **must** give a clear, simple opportunity to opt-out of your electronic mail marketing at the time you first collect their details (eg an online form with a prominent opt-out box).
5. **You give an opportunity to refuse or opt-out in every subsequent communication** – you **must** give people a chance to unsubscribe or opt-out of every subsequent communication you send. It **must** be simple and free of charge for them to do so (apart from the cost to them of sending the message).

### **Example**

An online clothing retailer decides it wants to use the soft opt-in to send marketing emails to its customers.

It adds the following opt-out box to the customer purchasing journey:

☐ **Tick here if you don't want to receive marketing emails from us about our clothing ranges.**

The retailer doesn't send email marketing to customers who tick the box. Instead it sends marketing emails about its clothing ranges to those customers who didn't tick the opt-out box when they bought its products.

It includes the following information at the end of every email that it sends:

**If you no longer want to receive our marketing emails, please click [unsubscribe](#).**

If the customer clicks unsubscribe, it stops sending them marketing emails.

The retailer is complying with the soft opt-in requirements of PECR.

Currently, the soft opt-in only applies to commercial marketing of products or services. This means you **must** have consent if you want to send direct marketing about fundraising, campaigning or to otherwise promote your aims or ideals.

Remember, you **must** comply with data protection law as well as PECR if you are using personal information (see [What type of information do we want to use?](#)).

For details of the information you **must** give people when sending electronic mail marketing, see [Is there any information we must give people when we send direct marketing to them?](#).

## Further Reading

 [Relevant provisions in PECR – see Regulation 2\(2\) and 22](#) 

External link

### Further reading

- If you need more detailed information on sending electronic mail, including on using the soft opt-in, see our [guidance on direct marketing using electronic mail](#).
- If you want to send direct marketing by electronic mail to businesses, see our [guidance on business-to-business marketing](#).

## Can we use post to send our direct marketing?

Direct marketing by post is not covered by PECR. But you **must** still comply with data protection law, if you are using personal information as part of your campaign.

Before you start your postal direct marketing campaign, ask yourself these questions:

- Do people know that you want to use their information for postal marketing? (See [Collect information and generate leads](#).)
- Have you checked their contact details against your suppression list of people who previously opted out or objected to your direct marketing? (See [What are direct marketing suppression lists?](#))

- Do you have a process for dealing with people who object to your direct marketing? (See [What do we do if someone objects to our direct marketing?](#))
- Do you have a data protection reason ("lawful basis") for sending direct marketing by post? (See [How do we decide what our data protection reason \("lawful basis"\) is for direct marketing?](#))

You **should** check names and addresses against the Mailing Preference Service (MPS) before sending out direct marketing. Although this is not a statutory preference service, checking against the MPS is a requirement under some industry codes (eg the DMA's code, see [Annex B](#)).

### Further reading

- If you intend to send political campaigning messages by post, see our [guidance for the use of personal data in political campaigning](#).

## Can we use online advertising for our direct marketing?

When you are considering using online advertising for your direct marketing, remember that the information you can collect on people is wider than what they actively give you. For example, it can include information gained by observing how someone uses the online environment (such as the devices they use) and inferred information based on this (such as predictions about their interests). This inferred information can also be special category data (eg inferring that someone suffers from a particular condition because their browsing history contains particular medical websites).

People may not understand how online advertising works or how their information is used. As a result they are less empowered to make choices about how their information is used.

If you are considering online advertising you **must** do the following:

- **Get consent.**

In most cases online advertising involves using cookies or similar technologies. For example, anything used to store information or access information stored on a user's device, such as cookies, fingerprint techniques or tracking pixels. If you intend to use cookies or similar for your online advertising, you **must** comply with PECR by getting consent (see [How does consent apply to direct marketing?](#)). This is the case whether the cookie is your own or that of a third party. If your online advertising involves special category data, you **should** get explicit consent (see [Can we use special category data for direct marketing?](#)).

- **Tell people what you're doing.**

You **must** give people concise, easy to understand privacy information for online advertising. The volume of organisations involved in online advertising and the technical complexity make it difficult for people to understand why their information is being collected and who is using it. (See [Collect information and generate leads](#).)

Under PECR you **must** give users clear and comprehensive information about what the cookies etc actually do that you intend to use for your online advertising (see [Is there any information we must give people when we send direct marketing to them?](#)).

Remember, you **must** comply with data protection as well as PECR, if you are using personal information



(see [What type of information do we want to use?](#)).

## Further Reading


 [Relevant provisions in the UK GDPR – see Article 4\(1\) and Recital 30 \(personal data\), Recital 58 \(transparency\)](#) 

External link

 [Relevant provisions in PECR – see Regulation 6](#) 

External link

### Further reading

- [Guidance on cookies and similar technologies](#)
- [ICO Opinion on data protection and privacy expectations for online advertising proposals](#) 

## Can we use social media for our direct marketing?

Social media platforms process large amounts of personal information about their users, including their behaviour and interactions. The platforms may allow you to target people for direct marketing purposes using particular tools. One of the most common is known as “audiences”. This can involve targeting:

- your existing customers on the platform. For example, giving your customers’ contact details to the platform and it then checks its userbase and those who match are added to this audience; and
- people that look like your existing customers. For example, setting targeting parameters based on an existing audience (such as demographics or interests) and the platform finds its users who are similar.

The activities in social media targeting are complex and you **must** make sure that you comply with the law. For example:

- **Be clear what information you need to achieve your purpose.**

You **should** be clear about what information you want to use and why it is necessary. This applies to when you want to use your social media presence to target direct marketing at people and when you want to use the platform’s advertising services.

- **Ensure what you want to do is fair, lawful and transparent.**

You **must** ensure that your use of people’s information is fair to the people involved. You **must** be upfront and clear about what you want to do, particularly if people are unlikely to expect it to take place (eg people without social media accounts will not expect you to share their information with a platform they don’t use).

Research from Which? found that 79% of those questioned were unaware that a social media platform matches profiles to customer lists that have been uploaded by organisations (see the further reading box).

Some types of audience may include people that you don’t have any direct relationship with. You **should**

be satisfied that the platform has taken all necessary steps to tell people what is happening.

You also **must** be clear about which data protection reason ("lawful basis") applies. (See [How do we decide what our data protection reason \("lawful basis"\) is for direct marketing?](#))


- **Define roles and responsibilities between you and the platform.**

Although the platform may undertake most of the actual processing, you are instigating it. This is because you provided the original information and defined the targeting parameters you want it to use. In many cases, it is likely that you and the platform are joint controllers, as you are both deciding what the information is being used for.

## Further Reading

 [Relevant provisions in the UK GDPR – see Article 5, Article 6, Article 13 and 14, Article 24 and 26](#)   
External link

### Further reading

- If you need more detail on joint controllers, see our guidance on [controllers and processors](#).
- Which? Research Report September 2021 – [Are you still following me? Consumer attitudes to data collection methods for targeted advertising](#) .

## Is there any information we must give people when we send direct marketing to them?

Some of the activities that involve sending direct marketing have additional rules in PECR that say what you **must** do or tell people.

When you make live or automated direct marketing calls, you **must**:

- say who is calling (eg the name of your organisation);
- display your number (or an alternative contact number) to the person receiving the call; and
- provide your contact details or a Freephone number (for live calls this is only if you are asked for this information).

When you send electronic mail marketing, you **must**:

- not disguise or conceal your identity; and
- provide a valid contact address for people to opt out or unsubscribe.

For online advertising, if you use cookies or similar technologies, you **must** give people clear and comprehensive information about what you are using these for. This **should** also be easily available, for example when someone first accesses your website.

## Further Reading

 [Relevant provisions in PECR – see Regulation 24 \(calls\), 23 \(electronic mail\) and 6\(2\)\(a\) \(cookies\)](#) 

### Further reading

- [Direct marketing using live calls](#)
- [Direct marketing using electronic mail](#)
- [Cookies and similar technologies](#)

## Can we share information for direct marketing purposes?

Sharing information for direct marketing purposes can include:

- selling, licensing or renting data or contact details;
- sharing or transferring databases; or
- supplying information obtained from a variety of sources to other organisations to add to people's existing records or profiles.

If the ultimate aim is that the organisation receiving the information uses it to inform their direct marketing, then you are sharing it for direct marketing purposes.

If you are involved in the trade of information for direct marketing purposes (eg data brokers offering direct marketing services), you **must** assess the compliance risks of these activities and comply with data protection law and PECR. For example:

- **Tell people you want to share their information.**

You **must** make clear to people that you want to share their information with other organisations for direct marketing purposes (see [Collect information and generate leads](#)).

- **If you want to share using consent make sure it is valid.**

You **must** make sure that consent to share someone's information for direct marketing purposes is valid. For example, you can't infer you have consent just because you are sharing information with an organisation that has a similar aim to you. (See [How does consent apply to direct marketing?](#))

- **Be able to justify sharing using legitimate interests.**

If you want to use legitimate interests as your data protection lawful basis, you **must** look at whether people would reasonably expect you to share their information with others for direct marketing. You also **must** consider what the impact of sharing will have on people (eg will they have a loss of control over their information if you share it?). (See [How does legitimate interests apply to direct marketing?](#))

- **Give people a chance to opt out of the sharing.**

If you are not relying on consent, then as a safeguard when you first collect information from people, you **should** include a clear, simple opt-out opportunity. People can use this if they want to object to you sharing their details with other organisations for direct marketing.

- **Take PECR into account.**

If you want to share a marketing list for other organisations to use to send electronic marketing messages, you **must** take PECR into account. For example, you **should** ensure that lists of phone numbers for others to use for automated marketing calls have consent for that organisation to use for that purpose.

- **Be accountable.**

You **should** keep records of:

- your decision-making (eg why do you want to share the information);
- how and when you collected the information; and
- what you told people.

You **should** be able to demonstrate to those you share information with, or who use your direct marketing services, that you collected the information in compliance with data protection law and, where applicable, PECR.

## Further Reading

 [Relevant provisions in the UK GDPR – see Article 6\(1\)\(a\), 6\(1\)\(f\), Articles 13, 14, 19 and 30](#) 

External link

 [Relevant provisions in PECR – see Regulation 19, 21 and 22](#) 

External link

### Further reading

- [Data sharing code of practice](#)
- [Data sharing information hub](#)
- [Investigation into data protection compliance in the direct marketing data broking sector](#)

## Can we work with others on our direct marketing?

Often you will do your direct marketing activity within your own organisation without any input or assistance from others. However, sometimes it may be beneficial to work with others.

If you do work with others, you **must** be clear who has responsibility for ensuring compliance. This is an important part of keeping people's information safe and making sure you respect their preferences. Responsibility depends on a number of factors including:

- who is making the decisions about how people's information is being used;
- the relationship between the different parties involved; and
- the type of direct marketing that is taking place.

Working with others for direct marketing can take different forms. For example:

- **Using other organisations to help with your direct marketing.**

In many cases, from a data protection perspective you are likely to have responsibility for making sure your direct marketing complies. This makes you the controller. The organisation helping you is likely in most cases to be acting on your instructions, and is therefore the processor. For example, they might check your telephone marketing list against the TPS or print and send your postal marketing to your customers. (See the [Glossary](#) for definitions.)

- **Using other organisations to send your electronic marketing messages on your behalf.**

Responsibility for complying with PECR is with the “sender”, “caller” or “instigator” of the direct marketing message. You are likely to be instigating if you encourage, incentivise, or ask someone else to send your direct marketing message. This means that PECR may still apply to you, even if you don’t send the message yourself or you don’t hold the contact details that your messages are sent to.

Often both you and the organisation you ask to send your messages are responsible for complying with PECR. But this may be different if you are entering into an agreement with a marketing platform or using a webmail provider. In this case, you may be the sender for PECR purposes with the other party having no responsibility under PECR for your messages. You may wish to seek legal advice if you are not clear who has responsibility for compliance.

- **Conducting joint direct marketing campaigns with third parties.**

If you and the other party are both using people’s information for the same purpose, you are likely to have joint responsibility for ensuring your marketing complies with data protection law and be joint controllers (see the further reading box). If you are conducting a joint campaign that involves sending electronic direct marketing messages, you both **must** comply with PECR.

- **Asking your customers to send your direct marketing to their friends and family.**

This is often known as a ‘refer a friend’ campaign. You **must** comply with PECR, if you are instigating people to send or forward your marketing messages (eg you may need consent from the friends and family). (See the further reading box.)

## Further Reading

 [Relevant provisions in the UK GDPR – see Article 24, 26, 28, 82, 83 and Recitals 79 and 146](#)   
External link

### Further reading

- [Controllers and processors](#) (this includes joint controllers)
- If you need more detail on ‘refer a friend’ campaigns, see our [guidance on direct marketing using electronic mail](#).

How do we decide what our data protection reason (“lawful basis”) is for direct marketing?

You **must** have a valid data protection reason, if you want to use people's information for your direct marketing activity (known as a "lawful basis"). You **must** choose which is the most appropriate, depending on your direct marketing activity, the context and your relationship with the person.

In general, consent and legitimate interests are the two lawful bases most likely to apply to your direct marketing.

You **must** consider if PECR applies to your direct marketing activity. It applies if you want to send direct marketing messages by phone call, electronic mail (eg emails and texts) or use cookies and similar technologies for online advertising.

Sometimes you need consent under PECR to send your marketing. PECR uses the same standard of consent as data protection law. Therefore, if you have consent for PECR, then you have already done the work needed to meet the consent lawful basis (assuming you are processing people's information and need a lawful basis). You don't need to find an alternative lawful basis to cover sending that direct marketing message. (See [How does consent apply to direct marketing?](#))

If PECR doesn't require consent for sending electronic marketing, then legitimate interests may be appropriate for your activity. For example, sometimes you don't need consent under PECR to make marketing calls and send electronic mail marketing. (See [How does legitimate interests apply to direct marketing?](#))

Apart from sending electronic marketing (such as by phone, email, text etc), other direct marketing activities are not covered by the marketing provisions in PECR. Therefore, PECR won't affect your choice of lawful basis for those.

## Further Reading

 [Relevant provisions in the UK GDPR – see Article 6\(1\)\(a\), and 6\(1\)\(f\)](#) 

External link

### Further reading

- If you need more detail on lawful bases and direct marketing, see our guidance on [sending direct marketing: choosing your lawful basis](#).
- [Lawful basis for processing](#)

## How does consent apply to direct marketing?

If you want to ask people to give you consent for direct marketing, you **must** make sure it is:

- **freely given:** People **must** have genuine choice and control over whether or not to consent to your direct marketing. In many cases it is unlikely you can make consent for direct marketing a condition of your service. They **must** be able to refuse consent without detriment (there's usually some benefit of consenting to direct marketing, such as access to special offers, but it is important to avoid unduly incentivising people to consent). They **must** also be able to withdraw their consent at any time (see [What do we do if someone withdraws their consent?](#));

- **specific and informed:** Your request for consent **must** be prominent, in plain language and separate from your privacy information. It **must** clearly explain what the consent is for (eg to send direct marketing emails), who wants to rely on the consent (eg you or another organisation) and how people can withdraw consent; and
- **unambiguous:** It **must** be obvious that someone has consented to your direct marketing activity. This **must** be a deliberate and specific action by someone to agree (pre-ticked boxes or default settings do not show consent).

### Example

A company's privacy policy states that they send direct marketing material to people who buy a product from them. In order to submit the online form, customers must tick a box to say that they have read that policy.

However, consent must be freely given and separate from privacy information. Also, confirmation that customers have read the company's privacy policy doesn't constitute an unambiguous indication that they have consented to receiving direct marketing. Therefore the consent the company has isn't valid.

If the company wants to use consent, it needs to provide a clear, separate opportunity for customers to choose to consent to its direct marketing.

You **should** also be aware of the following:



- **Consent for your direct marketing could come via a third party.**

It is possible for people to consent to your direct marketing via a third party but you **must** make sure the consent was valid. We generally recommend that you **should not** use consent for direct marketing that was given via a third party more than six months ago (unless people would expect your marketing at a later date, eg seasonal offers). This is because people may be happy to hear from you around the time they gave consent but they're unlikely to expect to start getting your marketing at a much later date.

- **Consent for direct marketing does not last forever.**

How long consent for direct marketing lasts depends on the circumstances (such as people's expectations and their relationship with you). For example, consent for a one-off message, or consent that is clearly only intended to cover a short time or a particular context, doesn't count as ongoing consent for all your future direct marketing.

## Further Reading

 [Relevant provisions in the UK GDPR – see Article 4\(11\), Article 6\(1\)\(a\), Article 7, Recital 32, 42, and 43](#)   
External link

### Further reading

## How does legitimate interests apply to direct marketing?

If your direct marketing activity doesn't need consent under PECR, then you might be able to rely on the legitimate interests as your data protection reason ("lawful basis"). For example, if you can show the way you use people's information:

- 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.

Legitimate interests is made up of a three-part test (known as a legitimate interests assessment or LIA):

- **Purpose test:** Identify whether you have a legitimate interest to use people's information for your particular direct marketing activity (eg to increase your revenues or grow your business).
- **Necessity test:** Decide if using people's information in that way is necessary for your purpose. Consider if:
  - what you want to do is a targeted and proportionate way of achieving your purpose; or
  - if you could achieve it in some other way (eg is it necessary to send the direct marketing to all your customers or is it be more proportionate to only send it to a particular group?).
- **Balancing test:** Objectively balance the necessity of your interests against the interests and rights of the people your direct marketing activity will affect. Typically this will involve considering:
  - what type of information you want to use for your direct marketing activity (eg is it likely to be considered sensitive or private?);
  - whether people will expect you to use their information in this way; and
  - any impacts your direct marketing activity may have on people (eg the potential nuisance factor of unwanted messages, any harm those messages could cause or the effect the frequency of your contact method might have on them).

If you want to use legitimate interests for your direct marketing activity, you **should** give people a clear option to opt-out of your direct marketing when you initially collect their details. People have the right to object to direct marketing and an opt-out can provide a safeguard to ensure they keep control of their information and can easily exercise their right.

### Example

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

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 decides that the impact of this postal marketing on people is likely to be minimal but it includes details within the mailing about how to opt-out. In light of the above it decides that it can apply the legitimate interests lawful basis to send the mailing. It has complied with the requirement to have a lawful basis.

## Further Reading

 [Relevant provisions in the UK GDPR – see Article 6\(1\)\(f\) and Recital 47 \(legitimate interests\), and Article 21\(2\) \(right to object\) !\[\]\(c9cd5a1c35167a83f09a35036fe5dcbd\_img.jpg\)](#)

External link

### Further reading

- [Legitimate interests](#)

## How do we make sure the information we use for direct marketing is accurate?

It is important for your direct marketing that the information you use is good quality and accurate. Also data protection law requires that you **must** keep people's information accurate and where necessary up-to-date:

- **Record information accurately.**

You **must** ensure that you accurately record people's information for direct marketing. For example, you **should** accurately record:

- the information you have been provided with (eg contact details);
- the source of that information;
- which methods of direct marketing people have consented to;
- any objections, opt-outs, or withdrawals of consent; and
- people's details on suppression lists (see [What are direct marketing suppression lists?](#)).

- **Take steps to ensure that information is accurate.**

You **must** take steps to ensure people's information that you hold for direct marketing purposes is not factually incorrect or misleading.

It is reasonable to rely on people to tell you when they change address or other contact details. It **could** be sensible to periodically ask them to update their own details. However, you don't need to take intrusive steps to ensure their contact details for direct marketing are up-to-date, such as using tracing services to find their new details. (See [Can we get new contact details for people from other sources, if their details are no longer correct?](#))

## Example

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

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

- **Keep up-to-date suppression lists.**

You **should** make sure that any direct marketing suppression lists you use are kept up-to-date. This is so that you don't inadvertently use someone's information for direct marketing when they have made clear that they don't want this. For example, you **must** use the most recent version of the TPS to check phone numbers before making live marketing calls. (See [What are direct marketing suppression lists?](#))

- **Deal promptly with challenges to the accuracy of personal information.**

People may challenge the accuracy of the information you hold on them. They have a data protection right to have their inaccurate information corrected, so you **must** deal with any such request.

## Further Reading

 [Relevant provisions in the UK GDPR – see Article 5\(1\)\(d \(accuracy\) and Article 16 \(right to rectification\)](#)   
External link

### Further reading

- [Accuracy](#)
- [Right to rectification](#)

## How long should we keep information for direct marketing purposes?

You **must** only keep people's information for as long as you need it:

- **Be clear why you need to keep it.**

Data protection law doesn't have specific timescales for how long you need to keep people's information for direct marketing. This means you **should**:

- consider why you need to keep their information; and
- be able to justify why it is necessary for your direct marketing purpose to keep it.

You **should** keep a record of your retention periods. You also **must** tell people how long you will keep their information (this is one of the things you **must** tell them when you collect their information, see [Collect](#)

[information and generate leads](#)).

- **Don't keep information that you don't need.**

You **should** regularly review the information you hold, in order to reduce the risk that it has become irrelevant, excessive or inaccurate.

If you no longer need the information for direct marketing purposes, you **must** delete or anonymise it (ie so it is no longer in a form that allows someone to be identified). This is unless you need to keep a small amount for another purpose, such as a suppression list (eg where someone has unsubscribed from your marketing, see [What are direct marketing suppression lists?](#)).

### Example

A retailer is planning a new product range. It wants to generate interest so it decides to give people an opportunity to submit their email address on a 'coming soon' webpage, so they can keep up-to-date with the product launch.

The retailer also decides that many people may want to hear about its other products as well. Therefore it decides to include an opt-in box on the webpage, so that when people submit their email address they can also choose to tick a box to also get emails about the retailer's other products.

Once the retailer has launched the product, it is unlikely to still need to keep the email addresses of those who didn't also agree to its general marketing. However, this is different for those people that also opted into the retailer's general marketing emails, as they gave consent for wider marketing too.

## Further Reading

 [Relevant provisions in the UK GDPR – see Article 5\(1\)\(e\), Article 13 and 14, and Article 30](#)   
External link

### Further reading

- [Storage limitation](#)

# Collect information and generate leads

## At a glance

You **must** tell people that you want to collect and use their information for direct marketing purposes. You **must** be clear about what you want to do and your privacy information **must** be easy for people to understand.

Getting new information about people from other sources or by profiling their interests and habits can help target your direct marketing more effectively. But you **must** ensure that doing this is fair and tell people about it.

## In more detail

- [What is collecting information and generating leads for direct marketing?](#)
- [What do we need to tell people if we collect their information directly from them?](#)
- [What do we need to tell people if we collect their information from other sources?](#)
- [Can we use publicly available personal information for direct marketing purposes?](#)
- [Can we find out additional contact details for people from other sources?](#)
- [Can we get new contact details for people from other sources, if their details are no longer correct?](#)
- [Can create profiles of people for direct marketing?](#)
- [What do we need to consider when buying or renting information for direct marketing?](#)

## What is collecting information and generating leads for direct marketing?

There are a number of ways that you may decide to seek contact details and additional information to use for your direct marketing, including from:

- the people who buy your products and services or support your cause (ie people you have a direct relationship with);
- third parties who sell or rent lists of contact details or who can provide additional information on your customers; or
- publicly available sources.

You may be seeking this information to:

- reach potential new customers (eg obtaining contact details for people you don't already have a relationship with);
- find new contact details for your existing customers (eg adding new contact channels for them); or
- profile your customers (eg analysing their behavioural characteristics to find out their preferences or predict their behaviour).

Whichever way you collect information or generate leads on potential or existing customers, you **must** ensure that what you want to do is fair, lawful and transparent. You **must** be open and honest.

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

Being transparent about what you're doing with people's information is a key part of data protection law. People have the "right to be informed" when you collect and use their personal information for direct marketing purposes.

There is a list of information in the UK GDPR that you **must** provide to people if you collect their information directly from them. For example, you **must**:

- explain why you want to use their information (eg to send postal marketing, to profile their buying habits);
- tell them if you intend to share their information with other organisations for direct marketing purposes; and
- make them aware of their data protection rights (including the right to object to direct marketing).

You **must** provide this privacy information to people at the time you collect their details. If, at a later date, you want to use the information for other activities, you **must** give them further privacy information (assuming the new things you want to do are fair and lawful).

Your privacy information **must** be in clear and plain language. It **should** be easy for people to understand what you are saying to them. You **should** tailor it to your audience (eg who are your customers and what are they likely to understand?) and use language and terms they will be familiar with and will understand. If you find it difficult to explain what you want to do, or you don't want to tell people because you think they might object, this is a sign that you **should** rethink your intended marketing activity.

There is no set way to provide your privacy information. The method depends on your audience and the way you collect the information (eg online, over the phone, by post). For example, you **could** consider:

- 'just in time notices' in an online context where a brief message appears at the point where people give you a particular piece of information that explains how you will use it for marketing; or
- a layered approach with a short notice giving key privacy information immediately and more detailed information elsewhere for those that want it.

The key point is that you **must** be upfront about your direct marketing and make the important information the most visible.

## Further Reading

 [Relevant provisions in the UK GDPR – see Article 5\(1\), and Article 13](#) 

External link

### Further reading

- If you need more detailed information on drafting and providing privacy information, see our [right to be informed](#) guidance.

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

It is particularly important to be transparent with people if you don't have a direct relationship with them. This is because people may have no idea that you collect their information from other sources to use for direct marketing unless you tell them.

There is a list of information in the UK GDPR you **must** provide to people if you don't collect their information directly from them. In general, this list is the same as when you collect people's information directly from them, and the requirements for this information to be clear and in plain language still apply. But you also **must** give them details about:

- the categories of their information you hold (eg contact details, interests); and
- the source of their information (eg the particular organisation it came from).

You **must** give people your privacy information within a reasonable period and at the latest within a month of obtaining their information (unless an exception applies, see below).

There are additional requirements if you plan to use the information to send direct marketing to the person it relates to, or to disclose it to someone else. In that case, the latest point at which you **must** provide your privacy information is when you first communicate with that person or disclose their information to someone else. But the one month time limit still applies, so it is a case of whichever is sooner.

## Example

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

Three weeks after obtaining the contact details, the company wants to send out its brochure to people on the list. It includes details of its privacy information, including the types of information it holds (names and addresses) and details of the source of the personal information (Company Z). The company has complied with the requirement to give people its privacy information.

In some cases you might not have to comply with these requirements, if you can rely on an exception. These exceptions are limited and many are unlikely to apply for direct marketing, but the following may be relevant:

- **The person already has the information.**

If you want to rely on this exception, you **must** be able to demonstrate and verify what privacy information people already have. You **must** ensure they have been provided with all the required information. You **must** provide anything that you are unsure about or is missing.

- **Disproportionate effort.**

If you want to rely on this exception, you **must** assess and document whether there is a proportionate balance between the effort involved for you to give privacy information and the effect of your direct marketing activity on people. The more significant the effect it has on people, the less likely you are to be able to rely on this exception.

If disproportionate effort applies, you still **must** publish your privacy information (eg on your website).

The right to be informed is a fundamental part of data protection law and this is an exception to the general obligation of transparency. You **should not** use it routinely across a range of activities, without considering the impact of each. As part of planning your direct marketing activities, you **should** take into account the transparency requirements that data protection law places on you (see [Plan direct marketing](#)).

## Further Reading

 [Relevant provisions in the UK GDPR – see Article 14](#) 

External link

### Further reading

- If you need more detail, including about exceptions, see our [right to be informed](#) guidance.

## Can we use publicly available personal information 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;
- websites and social media; and
- press articles or ‘rich’ lists.

You might be considering seeking people’s information from publicly available sources to find new customers or supporters, or to add to the profile or information you already hold about people. Data protection law and PECR don’t necessarily prevent you from doing this but there may be restrictions. For example, you **must** tell people that you have their information and what you want to do with it, as well as ensuring what you want to do is fair and lawful.

You **must** consider whether your direct marketing activities will be unexpected to the people whose information you are collecting from public sources. For instance, because someone’s social media page has not been made private or they are seeking a large audience for their social media post doesn’t mean that you are free to use their personal information for direct marketing purposes. They won’t expect you to do this.

## Can we find out additional contact details for people from other sources?

Finding out additional contact details for your customers or supporters from other sources for direct marketing is often known as data matching or appending (where you match information you already hold on people with other contact details that you didn’t have). For example, adding phone numbers for your customers to the address details you already hold. Often these additional contact details are bought from third parties, such as data brokers.

If you are considering this:

- **Let people choose if you can have their additional details.**

If people have consented to you having their additional contact details for direct marketing, then it is likely that you can match these with what you already hold.

If people have not agreed, then it is likely to be unfair in most cases to obtain such details for direct marketing. This is the case, even if you explain in your privacy information that you might seek out further information about people from third parties. This is because it removes people's choice about what channels you can contact them on for direct marketing.

For example, some people use different email addresses as a way of managing their information and relationships, including to limit or manage the direct marketing they receive. By getting an additional email address from another source, you may be going directly against their wishes.

- **Don't assume people want direct marketing by other channels.**

You can't assume someone wants you to contact them by other channels or has forgotten to give you the information. Even if they have forgotten, they still won't reasonably expect you to market them using details they never gave you or agreed to you having. People **must** be able to choose what contact details they give you.

Can we get new contact details for people from other sources, if their details are no longer correct?

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

If this happens, you **should** take into account the following:

- **People don't have to tell you when their contact details change.**

You can't assume someone has forgotten to tell you they have changed their details. Even if they had previously consented to your direct marketing at their old postal or email address, this consent is not transferrable to a new address that they didn't give you (it was specific to their old details).

However, if people express a wish for their updated contact details to be shared, you can continue to send marketing to them at the new address (assuming your initial collection of the information at the old address was compliant). They might do this by making it clear to a third party data source, by ticking a box, or some other positive action, that they wanted it to inform other organisations about a recent change of address.

- **Tracing people's new contact details for direct marketing isn't needed to maintain accuracy.**

You **should not** seek out new contact details from other sources or use the tracing services of other organisations for direct marketing. Your commercial interests in continuing to market people who have changed details are unlikely to outweigh their interests in this context. This is because it would be unfair to trace people in these circumstances as it takes away their control and right to choose not to share their new address.

You don't need to do this to comply with data protection accuracy requirements. (See [How do we make sure the information we use for direct marketing is accurate?](#))



If you have traced someone for a non-direct marketing purpose (such as non-payment of bills or fraud), this doesn't automatically mean that you can use these new details for direct marketing as well.

### 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 places a 'do not use' marker against the address details if the mailing has been returned, in order to comply with data protection law.

If the university had instead taken steps to trace the new addresses of their alumni, it would have risked infringing data protection law.

- **Make it easy for people to tell you when their details change.**

If people have an account with you, you **could** make it easy for them to proactively update their contact details within their account. Likewise, if you already hold other contact details, you **could** consider using these to remind people how they can keep their details updated. But you **must** check that this contact is fair, lawful and transparent, as well as complying with PECR, where applicable.

### Can we create profiles of people for direct marketing?

Profiling is where you look at people's interests, habits and behaviour, for example. Profiling for direct marketing often also involves predictions or assumptions about people. It can help you target your direct marketing messages to people who are more likely to buy your product or support your cause. It can also make your messages more relevant to the people that receive them.

Profiling can simply be realising that your customer likes a to buy a particular type of product from you and tailoring your marketing accordingly. But sometimes it can be more intrusive, for example due to the type of information used (eg health, financial), or the amount being gathered on someone.

If you're thinking about using profiling for your direct marketing it is important to do the following:

- **Be fair and tell people what you want to do.**

You **must** make sure the profiling is fair to people. For example, they are unlikely to anticipate you seeking to learn more about them and adding information from other sources to create a profile on them.

You **must** tell people about your profiling and clearly explain to them what you will be doing. This includes if you are going to use third parties or public sources to expand the profile on them. You **must** also ensure the information you hold for the profile is accurate and not excessive.

## Example

When a company collects a customer's information from them it provides them with the following information in order to meet its transparency obligations:

"We will use your purchase history to tell you about our offers and products that we think you will be most interested in."

This makes clear to customers that the company will be analysing the things they have previously bought and it will use that analysis to determine the content of the marketing messages they receive.

- **Ensure you have a lawful basis.**

You **must** have a data protection reason ("lawful basis") for your profiling activity. (See [How do we decide what our data protection reason \("lawful basis"\) is for direct marketing?](#))

If you are profiling people for direct marketing using their special categories of data, you are likely to need explicit consent. (See [Can we use special category data for direct marketing?](#))

- **Understand any potential risks.**

In many cases profiling for direct marketing can be positive, both for you and your customer. But it can potentially cause people harm and you **should** effectively address these risks. For example, it might perpetuate stereotypes if you make general assumptions based on the information you hold, or might cause discrimination if you exclude people from products or services based on your profiling.

- **Respect people's preferences.**

People have the right to object to direct marketing and this includes any profiling related to such direct marketing. You **must** comply with such an objection (see [What do we do if someone objects to our direct marketing?](#)).

- **Understand when the rules on solely automated decisions apply.**

There are data protection rules to protect people when you carry out solely automated decision-making, including profiling, that has legal or similarly significant effects on them. Solely automated means making a decision without any human involvement (eg using an algorithm to make the decision).

Solely automated decision making is likely to occur in online behavioural advertising because this happens without human involvement. However, the majority of direct marketing based on solely automated profiling is unlikely to have a legal or similarly significant effect, which means these rules don't apply. But there could be situations where it does, for example targeting known problem gamblers with betting adverts. (See the further reading box.)

## Further Reading

 [Relevant provisions in the UK GDPR – see Article 4\(4\) and Article 22](#) 

External link

## Further reading

- [Rights related to automated decision making including profiling](#)

What do we need to consider when buying or renting information from other sources?

Many organisations, including data brokers, offer information for direct marketing for sale, rent or on licence. For example, marketing lists of potential customers or new information for you to add to what you already hold on your customer. This can help you reach new customers or target your direct marketing more effectively to existing ones.

However, it is important to remember that you are responsible for ensuring compliance with data protection law and PECR. It is not enough to simply accept a third party's assurances that the information they are supplying to you is compliant.

This means that you **must** undertake proportionate checks and due diligence before you get the information. This helps you reduce the risk of infringing data protection law and PECR. For example, this **could** include ensuring you have certain details:

- **Who compiled the information** – was it the organisation you are buying it from or someone else?
- **Where was the information obtained from** – did it come from people directly or has it come from other sources? Is it fair that the third party uses these sources?
- **What privacy information was given** when people's information was collected – do people know the third party has their information and what were they told it would be used for?
- **When was the information compiled** – what date was it collected and how old is it?
- **Which type of information is it** – is any of it special category data?
- **How was the information collected** – what was the context and method of the collection?
- **What records of the consent are there** (if it is 'consented' information) – what did people consent to, what were they told, were you named, when and how did they consent?
- **What evidence is there that the information has been checked against suppression lists** (if claimed) – can it be demonstrated that the TPS has been checked against and how recently?
- **How does the seller deal with people's rights** – do they pass on objections?

A reputable third party **should** be able to demonstrate to you that the information it is supplying is reliable. You **should not** use the information if it cannot do this, or if you aren't satisfied with its explanations.

- **Your own compliance**

You **must** be clear how your use of the information complies. For example:

- You **must** be able to demonstrate what your data protection reason ("lawful basis") is for using people's information that is being provided to you.
- If you're getting a list of potential new customers or supporters, you **should** check the information against your own suppression lists, so you don't contact anyone who has previously asked you not to (unless they have given you consent that overrides their previous objection). (See [Respect people's preferences](#).)

- If you want to get more information on people, you **must** tell them that you want to do this.
- You **must** ensure that what you intend to do with the information is fair, reasonable and proportionate.
- Once you have obtained a list of potential customers or supporters, you **must** provide them with your own privacy information detailing anything they've not already been told. (See [What do we need to tell people if we collect their information from other sources?](#))

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

## Further Reading

 [Relevant provisions in the UK GDPR – see Article 6\(1\)\(a\) \(consent\) and Article 14 \(right to be informed\)](#)   
External link

### Further reading

- [Data sharing code of practice](#)
- [Data sharing information hub](#)
- [Organisations using the marketing services of data brokers](#)

# Respect people's preferences

## At a glance

It is important to respect people's preferences about direct marketing. People can object to you using their information for direct marketing and you **must** stop or not start using their information for this purpose.

People can also change their mind and can withdraw their consent or choose to opt-out of your direct marketing.

If someone no longer wants you to use their information for direct marketing purposes, you **should** put their details onto a suppression or 'do not contact' list, instead of deleting them. Doing this means you can check against your list so you don't use their information for direct marketing in future by mistake.

## In more detail

- [Why is it important to respect people's preferences?](#)
- [What do we do if someone objects to our direct marketing?](#)
- [What do we do if someone opts out of our direct marketing?](#)
- [What do we do if someone withdraws their consent?](#)
- [What are direct marketing suppression lists?](#)
- [What do we do if someone asks us to delete their information?](#)

### Why is it important to respect people's preferences?

Many people will be happy for you to use their information for direct marketing purposes, but some might not want you to do this, or they may change their mind.

It is important to respect people's preferences to maintain good relationships with your customers and supporters. It is also important because the law gives people rights about whether they want you to use their information for direct marketing. You **must** comply if someone exercises these rights.

People can:

- object to your direct marketing;
- opt-out or unsubscribe;
- withdraw their consent to your direct marketing; and
- ask you to delete their information.

## Further Reading

 [Relevant provisions in the UK GDPR – see Chapter III Articles 12, 17, and 21 \(rights Article 7\(3\) \(withdrawing consent\)\)](#) 

External link

## Further reading

- [Individual rights](#)
- [Consent](#)

## What do we do if someone objects to our direct marketing?

People have a legal right to object to you using their information for direct marketing purposes.

If someone objects, you **must** stop using their personal information for direct marketing. There are no reasons that you can use to refuse their objection.

This right covers any use of people's information for direct marketing purposes, including profiling. For example, using people's information to try to infer what products or services people in a particular geographical location might be interested in or disclosing their information to third parties for direct marketing purposes.

It is important to take the following actions:

- **Make people aware that they can object.**

You **must** make people aware that they can object to your direct marketing. You **must** clearly bring this to their attention, presenting it separately from other matters, using plain language.

You **must** tell people about this right "at the latest" at the time of your first communication with them. However, remember that as part of people's separate right to be informed, you also have to tell them that they can object (eg at the time you collect their details) (see [Collect information and generate leads](#)).

People can object at any time. This means they might want to object straight away or before you use their information for direct marketing.

- **Make it easy for people to object.**

It is good practice to give people an easy way to object. They **should** be able to do this at the time you collect their details (if this is not already required or you are not relying on consent to use their information). It **must** be free of charge for them to object.

- **Recognise when someone is objecting.**

There is no form of words that people must use to object to your direct marketing. People can object verbally, as well as in writing, and this might be directed to any part of your organisation. Therefore, you **should** have a process in place to recognise and deal with direct marketing objections.

If someone objects and you have any reasonable doubts about their identity, you can ask them for more information, but only for what is necessary for you to action their objection. For example, you may need to confirm their email address or phone number, in order to stop using these details for direct marketing.

- **Respect their objection.**

While you **must** comply with an objection to your direct marketing, this doesn't automatically mean you

need to delete their information. In most cases it is preferable to suppress their details. (See [What are direct marketing suppression lists?](#) and [What do we do if someone asks us to delete their information?](#))

If someone has objected to your direct marketing, you can't contact them at a later date to ask if they've changed their mind. This contact would still be for direct marketing purposes that they have specifically objected to. However, you may be able to remind people about their direct marketing preferences, if the reminder forms a minor and incidental addition to a message that you are sending anyway. The content **must** be for another purpose and not include marketing material. For example, an annual statement that includes a message at the end saying how they can update marketing preferences (but not encouraging them to change their mind).

- **Let people can change their mind.**

A person's most recent indication of their wishes about your direct marketing is the most important and it is possible for them to change their mind. For example, their original objection is overridden if they specifically withdraw their objection or in the future agree to direct marketing from you. However, failing to opt-out of your direct marketing at a later date doesn't override their previous objection.

## Further Reading

 [Relevant provisions in the UK GDPR – see Articles 21\(2\), 21\(3\), 21\(4\) and Recital 70, and Articles 12, 13\(2\)\(b\) and 14\(2\)\(c\)](#) 

External link

### Further reading

- [Right to object](#)

## What do we do if someone opts out of our direct marketing?

If someone opts out of your direct marketing, you **must** stop using their information for the direct marketing purposes that the opt-out covers.

For example, you may be relying on the PECR soft opt-in to send direct marketing emails. If your customer uses the 'unsubscribe' link within your email to opt-out, you **must not** send them any further marketing emails.

Someone opting-out of receiving direct marketing works in the same way as if they had issued an objection to direct marketing on that channel. This is because they are making it clear that they don't wish to get your direct marketing. However, unlike an 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.

### Example

A customer receives direct marketing by text message and by email from a company. The company is relying on the PECR soft opt-in to send the messages. As part of this, each text message includes an opt-out ('to opt-out text STOP to 12345') and each email has an unsubscribe button.

The customer decides they no longer want to receive marketing by text message and follows the instructions to opt-out by texting the word STOP.

The company stops sending marketing to them by text message. However, as they have not unsubscribed from its emails the company continues to send marketing by this other method, as it is still compliant to do so.

If you give people opt-out options when you collect their details, you **should** make it clear what method of direct marketing this covers.

You can send a message immediately after someone has opted out to confirm they have unsubscribed and provide information about how to resubscribe if they change their mind. But this message **must not** require them to take action to confirm their opt-out. It may also be possible to remind people about their direct marketing preferences (see [What do we do if someone objects to our direct marketing?](#)).

## What do we do if someone withdraws their consent?

Although people may have initially been happy to consent to your direct marketing, they may change their mind. Data protection law and PECR allow people to withdraw their consent to your direct marketing.

The key things to remember are:

- you **must** make it as easy for people to withdraw consent as it was to give it;
- if someone withdraws their consent you **must** stop the direct marketing that the consent covers immediately or as soon as possible; and
- if consent is withdrawn and this was your data protection reason ("lawful basis") for the direct marketing, you **must not** swap to a different basis to continue your direct marketing (this would be unfair).

## Further Reading

 [Relevant provisions in the UK GDPR – see Article 7\(3\)](#) 

External link

### Further reading

- [Consent](#)

## What are direct marketing suppression lists?

Direct marketing suppression lists or 'do not contact lists' are lists of people who have told you that they



don't want to:

- get direct marketing from you; or
- have their information used for direct marketing purposes.

Data protection law and PECR don't say you have to use a suppression list, but you **should** use one to help you to comply instead of just deleting their details. By using a suppression list, you can check any new marketing lists against it. This ensures you don't send direct marketing to anyone who has asked you not to, or use their information for direct marketing purposes if they have objected.

Sometimes organisations are concerned that the law stops them from putting someone on a suppression list when they object. This is not correct. While you **must not** keep using someone's information for direct marketing purposes when they object, keeping a suppression list isn't for direct marketing purposes. You are keeping this list so that you can comply with your statutory obligations (ie to comply with their objection) and not for direct marketing purposes.

### Example

A person whose phone number is not on the TPS receives a live direct marketing call from a company. The person asks the company not to call them again. In response the company simply deletes their phone number.

A few months later the company buys in a list of telephone numbers that have been checked against the TPS. This list includes that person's number because it isn't registered on the TPS. The company makes a further direct marketing call to that person.

The company has breached PECR by calling their number as the person had previously told it not to call.

If the company had placed the number on a suppression list rather than deleting it, the breach would have been prevented. This is because checking the bought-in list against its own suppression list would have identified that there was an objection to receiving direct marketing calls on that number.

It is also important that you do the following:

- **Only keep the minimum amount of information needed.**

Suppression involves keeping just enough information about someone to ensure you respect their preferences in the future, so you **must not** keep more than you need. You **should** clearly mark the information so you don't use it for the direct marketing purposes they objected to.

- **Understand what is and isn't a suppression list.**

The TPS and CTPS registers are types of suppression lists where people or organisations actively register an objection to receiving live direct marketing phone calls. You **must** check phone numbers against these statutory registers. The MPS is also a type of suppression list for postal marketing that you **should** check, although it is not a statutory one.

Don't confuse direct marketing suppression lists with screening lists. You may use a screening list when you have decided to screen out certain people because they don't fit the particular direct marketing campaign that you or a third party are running. Unlike a suppression list, you don't use a screening list to comply with someone's objection to direct marketing. Use of a screening list is processing for direct marketing purposes.

## What do we do if someone asks us to delete their information?

People may ask you to delete or erase the information you hold about them. They have a specific data protection right to ask you to erase their information (also known as the right to be forgotten). This can include their information that you use for direct marketing purposes.

However, this right only applies in certain circumstances such as:

- you are using consent for the direct marketing and it is withdrawn;
- you no longer need their information for your direct marketing purpose; or
- someone objects to you using their information for direct marketing purposes.

You don't need to automatically treat withdrawals of consent or objections to direct marketing as an erasure request. However, in practice if someone withdraws their consent, you can no longer keep using their information for that purpose. Similarly, if someone objects to you using their information for direct marketing purposes, you **must** stop. Therefore, you are likely to need to delete that information (unless you need to keep a small amount for another reason, such as on a suppression list).

### Example

A customer contacts a company to object to direct marketing and at the same time asks it to delete their information. The company stops using their information for direct marketing and deletes all of it, apart from a small amount that it keeps on its suppression list. This prevents it from using the customer's personal information for direct marketing purposes in the future. The company is complying with the customer's right.

Because we don't consider that a suppression list is used for direct marketing purposes, there is no automatic right for people to have their information on such a list deleted. (See [What are direct marketing suppression lists?](#))

## Further Reading

 [Relevant provisions in the UK GDPR – see Article 17 and Recitals 65 and 66, and Article 19](#)   
External link

## Further reading

- [Right to erasure](#)

# Enforcement

## At a glance

The ICO empowers people and organisations through information. The law recognises that responsible direct marketing brings benefits and our focus is on helping you carry out direct marketing in a compliant way.

We have powers to protect people if there has been a breach of data protection or PECR laws. We always use these in a targeted and proportionate way.

## In more detail

- [What is the role of the ICO?](#)
- [How does the ICO deal with complaints?](#)
- [What are the ICO's enforcement powers?](#)

### What is the role of the ICO?

The ICO exists to empower you through information:

- We empower you as a member of the public to confidently contribute to a thriving society and sustainable economy.
- We empower your organisation to plan, invest, responsibly innovate and grow.
- We empower you by promoting openness and transparency by public bodies.
- We empower you to hold us to account for the difference we make when enforcing the laws we oversee.

Our focus is on compliance with data protection and e-privacy legislation in the UK. The Information Commissioner is the independent supervisory authority for data protection law and PECR in the UK. In particular, in the context of this guidance, we help organisations to carry out direct marketing in a compliant way.

Where the provisions of this guidance overlap with other regulators, we will work with them to ensure a consistent and co-ordinated response.

### How does the ICO deal with complaints?

If someone raises a concern with us about the way you have handled their information in the context of direct marketing, we will record and consider their complaint. We will take this guidance into account when considering your compliance. We will assess your initial response to the complaint, and we may ask you some questions and give you a further opportunity to explain your position. We expect you to be accountable for how you meet your data protection obligations. Therefore, you **should** make sure that you give a full and detailed explanation about how you use their information and how you comply, when you initially respond to complaints from people.

The ICO prefers to work with organisations to find a resolution. You may avoid formal enforcement action if you recognise and take ownership of the correction of any data protection shortcomings by developing a performance improvement plan.

In terms of PECR, we encourage people to report their concerns to us as we use this information to monitor compliance and decide where to take enforcement action. We will also take this guidance into account when we consider if your direct marketing complies with PECR.

If we consider that you have failed (or are failing) to comply with data protection law 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 data protection law or PECR.

Tools at our disposal for 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 £17.5 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 and non-criminal enforcement. Currently, we can also serve a monetary penalty notice imposing a fine of up to £500,000 that we can issue against the organisation or its directors. These powers are not mutually exclusive. We will use them in combination where justified by the circumstances.

Any action taken against you, and the level of fine imposed, will be determined by which regime you have infringed. These powers are set out in detail on the ICO website (see the further reading box).

We take a risk-based, effective, proportionate approach to enforcement. Our aim is to create an environment within which people are protected, while supporting organisations to ensure they can operate and innovate efficiently in the digital age. We will be as robust as we need to be in upholding the law, while ensuring that enterprise is not constrained by red tape, or by concern that sanctions will be used disproportionately.

The ICO seeks to maximise our impact. For example, by focusing our enforcement powers on high-risk areas or circumstances where non-compliance could do the most harm and taking action on cases involving reckless or deliberate harms. The ICO is therefore unlikely to take enforcement action against an organisation that was genuinely seeking to comply and had taken reasonable steps to comply with the provisions of the legislation.

## Further Reading


 [Relevant provisions in the DPA 2018 – see Part 6 Enforcement](#) 

External link

 [Relevant provisions in PECR – see Regulations 31, 31A, 31B, 32 and Schedule 1](#) 

External link


### Further reading


- [What we do](#)
- [Regulatory Action Policy](#) 

# Annex A: Glossary


This glossary is a quick reference for key data protection and PECR terms and abbreviations used in this guidance. It includes links to further reading and other resources that may give you useful context and more detail.

Please note, this glossary is not a substitute for reading this direct marketing guidance, the ICO's other guidance, and associated legislation.

<b>Automated call</b>	A telephone call made by an automated dialling system that plays a recorded message.
<b>Consent</b>	Defined in UK GDPR 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". PECR also uses this definition. Consent is also one of the UK GDPR lawful bases for processing. For more information, see our <a href="#">guidance on consent</a> .
<b>Controller</b>	Defined in UK GDPR Article 6(7) as "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". For more information, see our <a href="#">guidance on controllers and processors</a> .
<b>Corporate subscriber</b>	Defined in Regulation 2(1) of PECR as "a subscriber who is (a) a company within the meaning of section 735(1) of the Companies Act 1985; (b) a company incorporated in pursuance of a royal charter or letters patent; (c) a partnership in Scotland; (d) a corporation sole; or (e) any other body corporate or entity which is a legal person distinct from its members".
<b>CTPS</b>	Corporate Telephone Preference Service. This is the statutory list of corporate subscribers who have registered a general objection to receiving live direct marketing calls. See the <a href="#">CTPS website</a>  for more details.
<b>Data subject</b>	The identified or identifiable living person the personal information relates to.
<b>Direct marketing</b>	Defined in section 122(5) of the DPA 2018 as "the communication (by whatever means) of advertising or marketing material which is directed to particular individuals".
<b>DPA 2018</b>	Data Protection Act 2018. This sits alongside the UK GDPR and sets out the framework for data protection in the UK. See our guidance <a href="#">about the DPA 2018</a> for more information.
<b>Electronic mail</b>	Defined in Regulation 2(1) of PECR 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".

<b>Individual subscriber</b>	Regulation 2(1) of PECR defines an individual as “a living individual and includes an unincorporated body of such individuals”. This means that it includes sole traders and other organisations (eg certain types of partnership).
<b>Joint controller</b>	Where two or more controllers jointly determine the purposes and means of processing. See our <a href="#">guidance on controllers and processors</a> for more information.
<b>Legitimate interests</b>	Legitimate interests is one of the UK GDPR lawful bases for processing personal information. It provides a lawful basis for processing where the processing is necessary for your legitimate interests or those of a third party, but only where these legitimate interests outweigh individuals’ interests, rights and freedoms. For more information see our guidance on <a href="#">legitimate interests</a> .
<b>Live call</b>	A telephone call where there is a live person who is speaking to the person they have called.
<b>MPS</b>	Mailing Preference Service. This is a non-statutory list of those who have registered a general objection to receiving direct marketing by post. See the <a href="#">MPS website</a>  for more details.
<b>PECR</b>	Privacy and Electronic Communications Regulations 2003 (as amended). These <a href="#">Regulations</a> sit alongside the DPA 2018 and the UK GDPR. PECR gives specific privacy rights in relation to electronic communications.
<b>Personal data (or personal information)</b>	Defined in UK GDPR Article 4(1) as “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”. For more information, see our guidance on <a href="#">what is personal data?</a> .
<b>Privacy information</b>	The information that controllers must provide to data subjects about the collection and use of their personal information. This information is specified in UK GDPR Articles 13 and 14. For more details, see our guidance on the <a href="#">right to be informed</a> .
<b>Processing</b>	Defined in UK GDPR Article 4(2) as “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”.
<b>Processor</b>	Defined in UK GDPR Article 4(8) as “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”. For more information, see our guidance on <a href="#">controllers and processors</a> .



<b>Profiling</b>	Defined in UK GDPR 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”.
<b>Soft opt-in</b>	The commonly used term to describe the exception in Regulation 22(3) of PECR, which, if met, means consent is not required to send direct marketing by electronic mail.
<b>Special category data</b>	Defined in UK GDPR Article 9(1) as “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”. For more information, see our guidance on <a href="#">special category data</a> .
<b>Subscriber</b>	Defined in Regulation 2(1) of PECR as “a person who is party to a contract with a provider of public electronic communications services for the supply of such services”.
<b>Suppression list</b>	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).
<b>Third party</b>	Defined in UK GDPR Article 4(10) as “a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data”.
<b>TPS</b>	Telephone Preference Service. This is the statutory list of individual subscribers who have registered a general objection to receiving live direct marketing calls. See the <a href="#">TPS website</a>  for further information.
<b>UK GDPR</b>	The United Kingdom General Data Protection Regulation. This sets out the framework for data protection in the UK along with the DPA 2018.
<b>User</b>	Defined in Regulation 2(1) of PECR as “any individual using a public electronic communications service”. See the <a href="#">Guide to PECR</a> for more information on a ‘public electronic communications service’.

# Annex B: Wider regulatory framework

The Commissioner regulates data protection and PECR laws. However, there are other rules and industry standards affecting direct marketing that are regulated by other bodies.

Compliance with other regulation and industry standards can assist you in demonstrating that your direct marketing activities comply with data protection law and PECR. For example, that your use of people's information for direct marketing purposes is lawful and fair.

You should be familiar with all laws and industry standards that apply to you.

## Other resources outside this guidance

[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 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 (CAP code). The CAP code contains rules which all advertisers, agencies and media must follow. It covers advertising content, and specific rules on certain types of advertising (eg advertising to children, advertising certain types of products).

The [Data & Marketing Association \(DMA\)](#) 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. The body that regulates charities based in Scotland is the [Scottish Charity Regulator \(OSCR\)](#).

The [Phone-paid Services Authority](#) is the UK regulator for content, goods and services charged to a phone bill (ie premium rate services).