

Guide to the Privacy and Electronic Communications Regulations

ico.

Information Commissioner's Office

Introduction	3
What are PECR?	4
What's new	8
Key concepts and definitions	9
Electronic and telephone marketing	13
Telephone marketing	17
Fax marketing	21
Electronic mail marketing	23
Using marketing lists	27
Cookies and similar technologies	31
Communications networks and services	38
Security of services	39
Security breaches	41
Traffic data	44
Location data	48
Itemised bills	51
Line identification (CLI)	52
Directories	55
Exemptions	58
Complaints	60

Introduction

About the Guide to Privacy and Electronic Communications Regulations

This guide is for organisations that wish to send electronic marketing messages (by phone, fax, email or text), use cookies, or provide electronic communication services to the public.

It explains how to apply the Regulations by giving practical examples and answering frequently asked questions.

What are PECR?

In brief...

The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the UK GDPR. They give people specific privacy rights in relation to electronic communications.

There are specific rules on:

- marketing calls, emails, texts and faxes;
- cookies (and similar technologies);
- keeping communications services secure; and
- customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

We aim to help organisations comply with PECR and promote good practice by offering advice and guidance. We will take enforcement action against organisations that persistently ignore their obligations, starting with those that generate the most complaints.

In more detail...

- [The basics](#)
- [What kind of areas do PECR cover?](#)
- [Do PECR apply to me?](#)
- [How does this fit with the UK GDPR?](#)
- [Are there any exemptions?](#)
- [How can the ICO help us comply?](#)
- [What action can the ICO take to enforce PECR?](#)

The basics

PECR are the [Privacy and Electronic Communications Regulations](#). Their full title is The Privacy and Electronic Communications (EC Directive) Regulations 2003.

They are derived from European law. PECR implement [European Directive 2002/58/EC](#), also known as 'the e-privacy Directive'.

The e-privacy Directive complements the general data protection regime and sets out more specific privacy rights on electronic communications. It recognises that widespread public access to digital mobile networks

and the internet opens up new possibilities for businesses and users, but also new risks to their privacy.

PECR have been amended a number of times. The more recent changes were made in 2018, to ban cold-calling of claims management services and to introduce director liability for serious breaches of the marketing rules; and in 2019 to ban cold-calling of pensions schemes in certain circumstances and to incorporate the UK GDPR definition of consent.

This guide covers the latest version of PECR, which came into effect on 29 March 2019.

The EU is in the process of replacing the current e-privacy law with a new e-privacy Regulation (ePR), to sit alongside the EU version of the GDPR. However, the ePR will not automatically form part of UK law - or sit alongside the UK GDPR - as the UK has left the EU.

PECR continues to apply alongside the UK GDPR but we will continue to keep our guidance under review and update it where necessary

What kind of areas do PECR cover?

PECR cover several areas:

- Marketing by electronic means, including marketing calls, texts, emails and faxes. See the [Electronic and telephone marketing](#) section of this guide for more information.
- The use of [cookies or similar technologies](#) that track information about people accessing a website or other electronic service. See the Cookies and similar technologies section of this guide for more information.
- Security of public electronic communications services. See the [Security of services](#) and [Security breaches](#) sections of this guide for more information.
- Privacy of customers using communications networks or services as regards traffic and location data, itemised billing, line identification services (eg caller ID and call return), and directory listings. See the [Communications networks and services](#) section of this guide for more information.

Do PECR apply to me?

Some of the rules only apply to organisations that provide a public electronic communications network or service. But even if you are not a network or service provider, PECR will apply to you if you:

- market by phone, email, text or fax;
- use cookies or a similar technology on your website; or
- compile a telephone directory (or a similar public directory)

How does this fit with the UK GDPR?

The UK GDPR sits alongside PECR. PECR rules apply and use the [UK GDPR standard of consent](#).

This means that if you send electronic marketing or use cookies or similar technologies you must comply with both PECR and the UK GDPR.

Naturally, there is some overlap, given that both aim to protect people's privacy. Complying with PECR will help you comply with the UK GDPR, and vice versa – but there are some differences and you must make sure you comply with both.

In particular, it's important to realise that PECR apply even if you are not processing personal data. For example, many of the rules protect companies as well as individuals, and the marketing rules apply even if you cannot identify the person you are contacting.

For more information on your other data protection obligations, see our separate [Guide to the UK GDPR](#).

If you are a network or service provider, Article 95 of the UK GDPR says the UK GDPR does not apply where there are already specific PECR rules. This is to avoid duplication, and means that if you are a network or service provider, you only need to comply with PECR rules (and not the UK GDPR) on:

- security and security breaches;
- traffic data;
- location data;
- itemised billing; and
- line identification services.

Are there any exemptions?

Yes. Some of the rules have built-in exemptions. These specific exemptions are explained in the relevant section of this guide.

There are also a few more-general exemptions that can apply to any of the rules – in brief, exemptions for national security, law enforcement, or compliance with other laws (see the [Exemptions](#) section of this guide).

How can the ICO help us comply?

If you are a [service provider](#) (eg a telecoms provider or an internet service provider), we can also conduct an audit of your [security measures](#). The audit will look at whether you have effective policies and procedures in place, and whether you are following them. It includes our recommendations on how you could improve. We believe that audits play a key role in helping organisations understand and meet their obligations.

We select service providers for audit based on the level of risk. If we select you for audit, we will write a letter of invitation, asking you to participate voluntarily. If you decide not to respond, then we have the power to undertake a compulsory audit. We agree a scope of work with you, and set this out in a letter of engagement. We will then carry out both an off-site check of your security policies and procedures, and an on-site review of your procedures in practice.

After completing the audit, we provide a comprehensive report and an executive summary. The report allows you to respond to our audit team's observations and recommendations. We publish the outcomes of PECR audits [on our website](#).

What action can the ICO take to enforce PECR?

ICO has several ways of taking action to change the behaviour of anyone who breaches PECR. They include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner can also serve a monetary penalty notice imposing a fine of up to £500,000 which can be issued against the organisation or its directors.

These powers are not mutually exclusive. We will use them in combination where justified by the circumstances.

We also publish a quarterly update on [action we have taken to enforce PECR](#).

What's new

We will update this page to highlight and link to what's new in our Guide to Privacy and Electronic Communications Regulations.

October 2022

We have added new detailed PECR guidance on [direct marketing using electronic mail](#).

We have added new detailed PECR guidance on [direct marketing using live calls](#).

December 2021

We have added checklists to the sections on [telephone marketing](#), [fax marketing](#) and [electronic mail marketing](#).

June 2019

We have revised the section on [cookies and similar technologies](#) in this Guide.

We have also updated our detailed guidance on [cookies and similar technologies](#).

January 2019

We have updated the section [what are PECR](#) and our guidance on [telephone marketing](#) to take into account the new Regulation 21B (marketing calls about pension schemes).

December 2018

We have updated the section [what are PECR](#) to include references to director liability for serious breaches.

September 2018

We have updated the section [what are PECR](#) and our guidance on [telephone marketing](#) to take into account the new Regulation 21A (marketing calls about claims management services).

Key concepts and definitions

In brief...

Different rules in PECR apply in different ways, using a variety of defined terms. Many of these terms are explained where relevant throughout this guide. The main concepts include:

- service provider: provides telephone or internet services;
- network provider: provides the underlying network equipment;
- subscriber: the person whose name is on the bill; and
- user: any individual using the phone or internet connection.

In more detail...

- [What are 'electronic communications'?](#)
- [What is a 'public electronic communications network'?](#)
- [What is a 'public electronic communications service'?](#)
- [What is a 'service provider'?](#)
- [What is a 'communications provider'?](#)
- [What is a 'public communications provider'?](#)
- [Who are 'subscribers' and 'users'?](#)
- [Who are 'corporate subscribers' and 'individual subscribers'?](#)

What are 'electronic communications'?

PECR do not define 'electronic communications'. Instead, the rules apply in different ways using specific concepts and definitions. For example, the marketing rules apply to specified types of marketing messages, and some other rules apply to [service providers](#) or [communications providers](#).

Nevertheless, the basic concept of an electronic communication underpins the regulations, so it may be helpful to get a general sense of what we mean by this term.

Put simply, electronic communications mean any information sent between particular parties over a phone line or internet connection. This includes phone calls, faxes, text messages, video messages, emails and internet messaging. It does not include generally available information such as the content of web pages or broadcast programming.

What is a ‘public electronic communications network’?

A ‘public electronic communications network’ is defined in section 151 of the [Communications Act 2003](#) as:



“an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public”.

An ‘electronic communications network’ is defined in section 32 of the Communications Act as:



“(a) a transmission system for the conveyance, by the use of electrical, magnetic or electro-magnetic energy, of signals of any description; and

(b) such of the following as are used, by the person providing the system and in association with it, for the conveyance of the signals—

(i) apparatus comprised in the system;

(ii) apparatus used for the switching or routing of the signals;

(iii) software and stored data; and

(iv) (except for the purposes of sections 125 to 127) other resources, including network elements which are not active.”

So a public electronic communications network is any transmitter or transmission system (plus associated equipment, software and stored data) used to convey electronic signals (including sounds, images or data of any description). This could be a wired or a wireless network – for example, a network of phone cables or a mobile phone network.

It does not include private or restricted networks, only networks used by service providers who have members of the public as customers.

The network ends at the customer’s point of connection (eg their master phone socket), so any equipment installed by a customer (eg wi-fi routers) does not form part of a relevant network.

In this guide ‘network’ means a public electronic communications network.

What is a ‘public electronic communications service’?

A ‘public electronic communications service’ is defined in section 151 of the [Communications Act 2003](#) as:



“any electronic communications service that is provided so as to be available for use by members of the public”.

An ‘electronic communications service’ is defined in section 32 of the Communications Act as:



“a service consisting in, or having as its principal feature, the conveyance by means of an electronic communications network of signals, except insofar as it is a content service.”

In other words, a public electronic communications service is any service that members of the public can sign up to in order to send or receive electronic signals (including sounds, images or data of any description) – for example, a phone contract or internet connection.

This does not include a ‘content service’ that provides or edits the actual content of signals – for example, a broadcast service or an online news service.

In this guide we generally use ‘service’ to mean a public electronic communications service.

What is a ‘service provider’?


Regulation 5(1) defines ‘service provider’ as a provider of a public electronic communications service.

Put simply, a service provider means someone who provides any service allowing members of the public to send electronic messages. This includes telecoms providers and internet service providers. Some service providers will operate their own network, but those using a network managed by a third party are also covered.

In our view, businesses offering wi-fi access to customers as a supplementary service are not service providers. A service provider would generally have a formal and ongoing contract with the customer subscribing to the service. By contrast, a coffee shop or hotel that provides wi-fi will itself be a subscriber to a service, and is simply permitting passing customers to use its connection.

For more information, see our [guidance for service providers on PECR security breaches](#) .

What is a ‘communications provider’?

A ‘communications provider’ is defined in section 405 of the [Communications Act 2003](#)  as someone who provides an electronic communications network or electronic communications service. So this term is broad and includes any organisation that operates a network or service, even if it is a private network or service not available to the public.

What is a ‘public communications provider’?

A ‘public communications provider’ is defined in PECR as a provider of a public electronic communications network or service. So this term covers [service providers](#) (that is, telecoms and internet service providers that have members of the public as customers), along with any third-party network operators that provide a network for those service providers.

Who are ‘subscribers’ and ‘users’?

PECR defines subscribers and users as follows:



“subscriber” means a person who is party to a contract with a provider of public electronic communications services for the supply of such services;

“user” means any individual using a public electronic communications service.

The subscriber is the customer who has a contract with the service provider – in other words, the person named on the bill for the telephone line or internet connection, or the person who owns the SIM card on a pay-as-you-go mobile contract. This may be an individual or an organisation.

The user is any individual actually using the phone or internet connection. This will not always be the same person as the subscriber – for example they might be the subscriber’s employee, a customer, a family member or a friend.

Who are ‘corporate subscribers’ and ‘individual subscribers’?

‘Corporate subscriber’ covers subscribers that are a corporate body with separate legal status. This includes companies, limited liability partnerships, Scottish partnerships, and some government bodies.

‘Individual subscriber’ covers individual customers (including sole traders) and other organisations (eg other types of partnership).

Electronic and telephone marketing

In brief...

PECR restrict unsolicited marketing by phone, fax, email, text, or other electronic message. There are different rules for different types of communication. The rules are generally stricter for marketing to individuals than for marketing to companies.

You will often need specific consent to send unsolicited direct marketing. The best way to obtain valid consent is to ask customers to tick opt-in boxes confirming they are happy to receive marketing calls, texts or emails from you.

In more detail...

- [What is 'direct marketing'?](#)
- [What kinds of electronic marketing are covered?](#)
- [When is marketing 'solicited' and when is it 'unsolicited'?](#)
- [What counts as consent?](#)
- [What is the difference between 'opt in' and 'opt out'?](#)
- [Do the rules apply to business-to-business marketing?](#)
- [What rules apply to international marketing campaigns?](#)
- [What if we pay someone else to do our marketing?](#)

What is 'direct marketing'?

Direct marketing is defined in section 122(5) of the Data Protection Act 2018 as:



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

This covers all advertising or promotional material, including that promoting the aims or ideals of not-for-profit organisations – for example, it covers a charity or political party campaigning for support or funds.

The marketing must be directed to particular individuals. In practice, all relevant electronic messages (eg calls, faxes, texts and emails) are directed to someone, so they fall within this definition.

Genuine market research does not count as direct marketing. However, if a survey includes any promotional material or collects details to use in future marketing campaigns, the survey is for direct marketing purposes and the rules apply.

Routine customer service messages do not count as direct marketing – in other words, correspondence with customers to provide information they need about a current contract or past purchase (eg information about service interruptions, delivery arrangements, product safety, changes to terms and conditions, or tariffs). General branding, logos or straplines in these messages do not count as marketing. However, if the message includes any significant promotional material aimed at getting customers to buy extra products or services or to renew contracts that are coming to an end, that message includes marketing material and the rules apply.

Further Reading

 [Direct marketing guidance](#) 

For organisations

What kinds of electronic marketing are covered?

PECR cover marketing by phone, fax, email, text or any other type of [‘electronic mail’](#).

There are different rules for live calls, automated calls, faxes, and electronic mail (this includes emails or texts).

PECR marketing provisions do not apply to other types of marketing, such as mailshots or online advertising. However, you must always still comply with the Data Protection Act and the UK GDPR; and if your online advertising uses cookies or similar technologies, the provisions about [cookies](#) may apply.

Further Reading

 [Sending direct marketing messages: At-a-glance guide](#)

For organisations

PDF (225.43K)

When is marketing ‘solicited’ and when is it ‘unsolicited’?

Most of the rules in PECR only apply to unsolicited marketing messages. They do not restrict solicited marketing.

Put simply, a solicited message is one that is actively requested. So if someone specifically asks you to send them some information, you can do so without worrying about PECR (although you must still say who you are, display your number when making calls, and provide a contact address).

An unsolicited message is any message that has not been specifically requested. So even if the customer has ‘opted in’ to receiving marketing from you, it still counts as unsolicited marketing. An opt-in means the customer agrees to future messages (and is likely to mean that the marketing complies with PECR). But this is not the same as someone specifically contacting you to ask for particular information.

This does not make all unsolicited marketing unlawful. You can still send unsolicited marketing messages – as long as you comply with PECR.

What counts as consent?

You will often need a person's consent before you can send them a marketing message. If you do need consent, then – to be valid – consent must be knowingly and freely given, clear and specific. It must cover both your particular organisation and the type of communication you want to use (eg call, automated call, fax, email, text). It must involve some form of very clear positive action – for example, ticking a box, clicking an icon, or sending an email – and the person must fully understand that they are giving you consent. You cannot show consent if you only provide information about marketing as part of a privacy policy that is hard to find, difficult to understand, or rarely read.

The clearest way to obtain consent is to ask the customer to tick an opt-in box confirming they are happy to receive your marketing calls, faxes, texts or emails.

You should keep clear records of what a person has consented to, and when and how you got this consent, so that you can demonstrate compliance in the event of a complaint.

You should be very careful when relying on consent obtained indirectly (consent originally given to a third party). You must make checks to ensure that the consent is valid and specifically identifies you. Generic consent covering any third party is not enough.

Remember that the customer is entitled to withdraw their consent at any time. You must make it easy for people to withdraw consent, and tell them how.

Further Reading



Consent

For organisations

What is the difference between 'opt in' and 'opt out'?

'Opt in' means a person has to take a specific positive step (eg tick a box, send an email, or click a button) to say they want marketing. 'Opt out' means a person must take a positive step to refuse or unsubscribe from marketing.

Some organisations provide opt-in boxes that are automatically pre-ticked. However, the UK GDPR is clear that pre-ticked boxes do not give valid consent.

You must use an 'affirmative' method of getting consent. We recommend you use unticked opt-in boxes wherever possible.

Do the rules apply to business-to-business marketing

Yes, but there are different rules for marketing to companies and marketing to individuals (which includes sole traders and some partnerships). In general, the rules on marketing to companies are not as strict.

For more information, see our separate guidance on [business-to-business marketing](#).

What rules apply to international marketing campaigns?

If you are sending messages to countries outside the UK, you must also comply with their laws. Currently, EU countries have very similar laws to ours, based on the e-privacy Directive. Some of them are stricter than the UK regulations, especially for marketing to companies.

We cannot offer guidance on the law of other countries. You will need to seek your own legal advice if you wish to carry out an international marketing campaign.

What if we pay someone else to do our marketing?

You are both responsible for complying with PECR. Even if someone else actually makes the calls or sends the messages, you are still responsible, as you are 'instigating' those calls or messages. If we needed to take enforcement action, we would usually take it against you as the instigator. In some cases we might consider taking action against a specialist subcontractor as well if they deliberately or persistently ignored the rules.

You should make sure you have a written contract that sets out your contractor's responsibilities. You may also want to ask your contractor to indemnify you (protect you against loss) for any breach of PECR. If they break the law and expose you to enforcement action (and reputational damage with customers), you may then be able to seek legal advice about taking action for breach of contract. However, an indemnity is not a substitute for proper checks of your contractor – remember it is still your name and reputation at stake.

Having a written contract with your contractor ties in with your contract obligations under the UK GDPR. See our separate [Guide to the UK GDPR](#) for more information on contracts.

Further Reading

 [Direct marketing guidance](#)

For organisations

Telephone marketing

In brief...

In general, you must not make marketing calls to any number listed on the Telephone Preference Service (TPS) or Corporate TPS (CTPS), unless that person has specifically consented to your calls. You can call a number if it is not listed on the TPS or CTPS and you are not marketing claims management services. So you need to screen call lists against the TPS and CTPS. You can only make marketing calls in relation to pension schemes if you meet a strict criteria. You must allow your number to be displayed.

In more detail...

- [What are the rules on making live calls?](#)
- [What are the rules on automated calls?](#)
- [What are the TPS and the CTPS?](#)
- [When can we make marketing calls to individuals?](#)
- [When can we make marketing calls to businesses?](#)
- [Where can we get more information?](#)
- [Checklists](#)

What are the rules on making live calls?

The rules on live marketing calls are in regulation 21, 21A and 21B. In short, you must not make unsolicited live calls:

- to anyone who has told you they don't want your calls;
- to any number registered with the TPS or CTPS, unless the person has specifically consented to your calls – even if they are an existing customer (unless the call is in relation to pension schemes and you meet a strict criteria, see below);
- for the purpose of claims management services, unless the person has specifically consented to your calls; or
- in relation to pension schemes unless you are a trustee or manager of a pension scheme or a firm authorised by the Financial Conduct Authority, and the person you are calling has specifically consented to your calls or your relationship with the individual meets a strict criteria.

You must always say who is calling, allow your number (or an alternative contact number) to be displayed to the person receiving the call, and provide a contact address or freephone number if asked.

What are the rules on automated calls?

The rules on automated calls are in regulation 19, and are stricter. You must not make an automated marketing call – that is, a call made by an automated dialling system that plays a recorded message – unless the person has specifically consented to receive this type of call from you. General consent for marketing, or even consent for live calls, is not enough – it must specifically cover automated calls. See [What counts as consent?](#)

All automated calls must include your name and a contact address or freephone number. You must also allow your number (or an alternative contact number) to be displayed to the person receiving the call.

What are the TPS and the CTPS?

The TPS is the Telephone Preference Service. It is a central register of individuals who have opted out of receiving live marketing calls.

The CTPS is the Corporate TPS. It works in the same way as the TPS, but for companies and other corporate bodies (limited liability partnerships, Scottish partnerships and government bodies).

For more information and details of how to subscribe to the TPS/CTPS, see www.tpsonline.org.uk.

When can we make marketing calls to individuals?

You can call any individual who has specifically consented to receive marketing calls from you – for example, by ticking an opt-in box. See [What counts as consent?](#)

You can also make live calls without consent to a number if it is not listed on the TPS – but only if that person hasn't objected to your calls in the past and you are not marketing claims management services.

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

In general you cannot make live marketing calls in relation to pension schemes. However there is an exception to this but you must be a trustee or manager of the scheme, or authorised by the Financial Conduct Authority. You must also have either the individual's consent for the calls or your relationship with the individual must meet a strict criteria. The criteria that you must meet if you want to make such a call without consent is as follows:

- you have an existing customer relationship with the person you are calling;
- they might reasonably expect such a call from you; and
- you gave them a chance to opt-out of such calls when you collected their details and in every message you send them.

When can we make marketing calls to businesses?

The rules are the same as for calls to individuals. So, you can call any business that has specifically

consented to your calls – for example, by ticking an opt-in box.

You can also make live calls to any business number that is not registered on the TPS or the CTPS, but only if they haven't objected to your calls in the past and you are not marketing claims management services.

You should remember that some businesses (sole traders and some partnerships) register with the TPS, and others (companies, some partnerships and government bodies) register with the CTPS. For business-to-business (B2B) calls, you will therefore need to screen against both the TPS and the CTPS registers, as well as your own 'do not call' list.

For more information, see our separate guidance on [business-to-business marketing](#).

Where can we get more information?

For more detailed information and practical advice on making live direct marketing calls, see our [direct marketing using live calls guidance](#).

Checklists

Live marketing calls

- We screen numbers against the Telephone Preference Service (TPS) or for corporate subscribers the Corporate Telephone Preference Service (CTPS).
- We keep our own 'do not call' list of anyone who says they don't want our marketing calls.
- We screen numbers against our 'do-not-call' lists and we don't call anyone that asks us not to.
- We have consent if we make marketing calls about claims management services.
- We ensure that we are authorised if we make marketing calls about pension schemes and that we have the person's consent to call them (unless contacting our existing customers if they would expect the calls, and we offered them an opt-out when they gave their details and each time we contact them).
- We display our number to the person we're calling.
- We say who we are and if asked we give an address or Freephone number that people can contact us on.

Automated marketing calls

- We only make automated marketing calls if we have consent.
- We display our number to the person we're calling.
- We say who we are in the message and give an address or Freephone number that people can contact us on.

We stop making automated marketing calls if consent is withdrawn.

Fax marketing

In brief...

You must not send marketing faxes to individuals or to any number listed on the Fax Preference Service (FPS), unless they have specifically consented to your faxes. You can send marketing faxes to companies that are not listed on the FPS. So you need to screen business fax lists against the FPS.

In more detail...

- [What are the rules on sending faxes?](#)
- [What is the FPS?](#)
- [When can we send marketing faxes to individuals?](#)
- [When can we send marketing faxes to businesses?](#)
- [Checklist](#)

What are the rules on sending faxes?

The rules on marketing faxes are in regulation 20. In short, you must not send marketing faxes to:

- individuals, including sole traders and some partnerships, unless they have specifically consented to your faxes; or
- a company or other corporate body that has told you they don't want your faxes; or
- any number registered with the FPS, unless the person has specifically consented to your faxes.

All marketing faxes must include your name and a contact address or freephone number.

What is the FPS?

The FPS is the Fax Preference Service. It is a central register of people who have opted out of receiving marketing faxes. For more information, see www.fpsonline.org.uk/fps.

It is primarily aimed at businesses but individuals can also register their fax numbers if they wish.

When can we send marketing faxes to individuals?

You can only send a marketing fax to an individual if they have specifically consented to receive marketing faxes from you – for example, by ticking an opt-in box. See [What counts as consent?](#)

When can we send marketing faxes to businesses?

You can fax any business that has specifically consented to your faxes – for example, by ticking an opt-in box.

Sole traders and some partnerships are treated as individuals – so you can **only** send them marketing faxes if they have specifically consented to your faxes.

You can fax a corporate body (eg a company, Scottish partnership, limited liability partnership or government body) without consent, but only if the number is not registered on the FPS and they haven't objected to your faxes in the past. So you will need to screen B2B fax lists against the FPS. You will also need to keep your own 'do not fax' list of any businesses that object or opt out, and screen against that as well.

For more information, see our separate guidance on [business-to-business marketing](#).

Checklist

- We only send marketing faxes to individuals (including sole traders and some types of partnership) if we have consent.
- We screen numbers against the fax preference service before sending marketing faxes to businesses.
- We keep our own 'do not fax' list of any business who says they don't want our faxes.
- We screen against our 'do not fax' list before sending marketing faxes to businesses and we don't fax anyone that asks us not to.
- We say who we are in the message and give an address or Freephone number that people can contact us on.

Electronic mail marketing

In brief...

You must not send marketing emails or texts to individuals without specific consent. There is a limited exception for your own previous customers, often called the 'soft opt-in'.

You can send marketing emails or texts to companies. However, it is good practice to keep a 'do not email or text' list of any companies that object.

In more detail...

- [What are the rules on electronic mail marketing?](#)
- [What about texts and other types of electronic message?](#)
- [What is a 'soft opt-in'?](#)
- [Is there a text or email version of the TPS?](#)
- [When can we email or text individuals?](#)
- [When can we email or text businesses?](#)
- [Do these rules apply to viral marketing?](#)
- [What about online marketing and behavioural advertising?](#)
- [Where can we get more information?](#)
- [Checklist](#)

What are the rules on electronic mail marketing?

The rules on electronic mail marketing are in regulation 22. In short, you must not send electronic mail marketing to individuals, unless:

- they have specifically consented to electronic mail from you; or
- they are an existing customer who bought (or negotiated to buy) a similar product or service from you in the past, and you gave them a simple way to opt out both when you first collected their details and in every message you have sent.

You must not disguise or conceal your identity, and you must provide a valid contact address so they can opt out or unsubscribe.

What about texts and other types of electronic message?

This same rule applies to emails, texts, picture messages, video messages, voicemails, direct messages via social media or any similar message that is stored electronically.

The term 'electronic mail' has an intentionally broad meaning that includes new forms of messaging. It is defined as:



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

What is a 'soft opt-in'?

The term 'soft opt-in' is sometimes used to describe the rule about existing customers. The idea is that if an individual bought something from you recently, gave you their details, and did not opt out of marketing messages, they are probably happy to receive marketing from you about similar products or services even if they haven't specifically consented. However, you must have given them a clear chance to opt out – both when you first collected their details, and in every message you send.

The soft opt-in rule means you may be able to email or text your own customers, but it does not apply to prospective customers or new contacts (eg from bought-in lists). It also does not apply to non-commercial promotions (eg charity fundraising or political campaigning).

Is there a text or email version of the TPS?

No. There is no equivalent email or text preference service. This is because you may only send emails or texts to individuals if you have their specific consent or have already offered them an opt-out, so this type of central opt-out register shouldn't be needed.

When can we email or text individuals?

You can email or text an individual if they have specifically consented to receiving emails or texts from you – for example, by ticking an opt-in box. See [What counts as consent?](#)

You can also email or text an existing customer who has bought (or discussed buying) a similar product or service from you in the past – but only if you gave them a clear chance to opt out of getting marketing emails or texts when you collected their details, and in every message.

When can we email or text businesses?

Sole traders and some partnerships are treated as individuals – so you can only email or text them if they have specifically consented, or if they bought a similar product from you in the past and didn't opt out from

marketing messages when you gave them that chance.

You can email or text any corporate body (a company, Scottish partnership, limited liability partnership or government body). However, it is good practice – and good business sense – to keep a ‘do not email or text’ list of any businesses that object or opt out, and screen any new marketing lists against that.

You may also need to consider data protection implications if you are emailing employees at a corporate body who have personal corporate email addresses (eg [\[email protected\]](#)).

For more information, see our separate guidance on [business-to-business marketing](#).

Do these rules apply to viral marketing?

Yes – you must comply if you send a marketing message, or if you ‘instigate’ someone else to send it.

Some organisations try to get round the rules by asking people to forward a marketing message to their friends. However, you are ‘instigating’ them to send that message, so you must still comply with PECR. (This does not mean you are responsible every time a customer forwards a message without your knowledge – you must have encouraged them to send it.)

Another form of viral marketing is to ask people to provide their friends’ contact details. However, you must still ensure that any marketing messages you send to those friends comply with PECR. This may be difficult, as you cannot be sure whether the friends actually agreed to give you their details. We would therefore advise against this type of viral marketing.

What about online marketing and behavioural advertising?

If you are marketing using direct messaging via social media, the electronic mail marketing rules apply.

PECR do not set out specific rules on other types of online marketing such as display or banner ads. However, there are [rules on cookies](#), which are often used to profile users and target behavioural advertising.

If you are using personal data, you also need to comply with the Data Protection Act and the UK GDPR. For more information on this area, see our separate guidance:

Further Reading

 [Guide to the UK General Data Protection Regulation \(GDPR\)](#)

For organisations

Where can we get more information?

For more detailed information and practical advice on this topic, see our [direct marketing using electronic mail guidance](#).

Checklist

- We only send electronic mail with consent (unless contacting previous customers about our own similar products, and we offered them an opt-out when they gave us their details).
- We offer an opt-out (by reply or unsubscribe link) and act on this promptly.
- We keep a 'do not contact' list of anyone who opts out or unsubscribes from our electronic mail.
- We screen against our 'do not contact' list and we don't send electronic mail to anyone who has asked us not to.
- We don't disguise or conceal who we are when we send electronic mail.
- We don't ask or encourage people to forward our electronic mail marketing to their friends or family.
- We don't ask people to give us the contact details of their friends and family to use for electronic mail marketing.

Using marketing lists

In brief...

You should check the origin and accuracy of bought-in lists. You should screen call lists against the TPS, and only use bought-in lists for email, text or recorded calls with very specific consent.

For in-house marketing lists, use opt-in boxes wherever possible. Specify consent to marketing by email, by text, by fax, by phone or by recorded call. Ask for specific consent also if you want to pass details to other companies, and make sure you name or describe those companies.

Keep clear records of consent, and keep a 'do not contact' list of anyone who objects or opts out.

In more detail...

- [Can we use bought-in marketing lists?](#)
- [What's the best way to compile our own marketing list?](#)
- [Can we sell our marketing list?](#)
- [Can we share our list with other companies in our group?](#)
- [Can one company use one list for multiple trading names?](#)
- [How should we respond to objections or opt-outs?](#)
- [How do the rules apply to our loyalty scheme members?](#)
- [Can we send marketing by post?](#)

Can we use bought-in marketing lists?

You can use bought-in lists to make live marketing calls, but you should screen against both the TPS and your own 'do-not-call' list of people who have previously objected to or opted out of your calls.

You must be very careful before using bought-in lists for recorded calls, texts or emails. You can only use them if all the people on the list specifically consented to receive that type of message from you. Generic consent covering any third party will not be enough.

If you are using bought-in B2B fax lists, you must screen against both the FPS and your own 'do-not-fax' list of people who have previously objected to or opted out of your faxes. You may only fax individuals (including sole traders and some partnerships) if they have specifically consented to receiving faxes from you.

You must make checks to satisfy yourself that any list is accurate and the details were collected fairly, and that the consent is specific and recent enough to cover your marketing.

Further reading

For more information on collecting people's information from other sources, see our [direct marketing guidance](#).


What's the best way to compile our own marketing list?

You may want to compile your own in-house marketing list using details of people who have bought goods or services in the past, or who have registered on your website or made an enquiry. However, you should not assume that everyone is happy to receive marketing just because they have provided their contact details.

You should make it clear upfront that you intend to use their details for marketing purposes. The best way to get clear consent for your marketing is to provide opt-in boxes that specify the type of messages you plan to send (eg by email, by text, by phone, by fax, by recorded call).

You should record when and how you got consent, and what type of messages it covers. If possible, you should also record whether the customer is an individual or a company, as different rules apply. If this is not clear, assume they are an individual.

Further reading

For further information, see our [guidance on direct marketing](#) .

Can we sell our marketing list?

As a general rule, you can only sell your marketing list if you have the consent of the listed individuals to do so.

Other businesses will only be able to use the list for recorded calls, texts or emails if the people on the list have specifically consented to receive that type of message from that company.

Further reading

For more information on sharing information for direct marketing purposes, see our [direct marketing guidance](#).

Can we share our list with other companies in our group?

The same rules apply as for other third parties. If you intend to share the list within your group, you must have each individual's specific consent to marketing from your group companies.

As always, the best way to get consent is to provide an opt-in box. You should list the group companies (you could do this online by providing a link). You may even want to consider offering separate opt-ins for each company, to give the individual greater choice and to target your group's marketing more effectively. You cannot show consent if you only provide information about marketing from your group companies as part of a privacy policy that is hard to find, difficult to understand, or rarely read.

Can one company use one list for multiple trading names?

If you are a single entity trading under several different names, you should not assume that a customer opting in to marketing from one brand is consenting to marketing from all your brands. Consent must be informed, and customers may not even be aware of any connection between the brands. You may also find it difficult to rely on the [soft opt-in](#), as this only applies to similar products and services.

If you want to use one list for all your trading names, you should list them all clearly when you obtain the opt-in.

If an individual opts out of marketing from one trading name, you should assume this opt-out applies to all your trading names unless they make it clear otherwise.

How should we respond to objections or opt-outs?

As soon as someone objects to or opts out of your marketing, you should add them to a 'do not contact' list. You should screen all your marketing against this list to make sure you don't contact anyone who has opted out. You can send an immediate reply confirming they have unsubscribed, but you must not contact them at a later date even if this is just to ask if they want to opt back in.

You must not simply delete their details altogether, as you need to ensure they are not later put back on your marketing list by mistake (for example if you buy more leads that include the same details). If someone asks you to delete their details, you should explain that you will need to keep them on a 'do not contact' list to make sure you comply with their right to opt out.

Further reading

For more information on objections and opt-outs, see our [direct marketing guidance](#).

How do the rules apply to our loyalty scheme members

If you operate a loyalty scheme, you should make sure your customers understand what messages they will receive if they sign up. They are likely to expect a periodic update on how many points or vouchers they have earned. In our view, under the [soft opt-in rule](#), as long as you provide a clear opt-out when they sign up and in every subsequent message, you may also send them further [electronic mail](#) about other promotions unless they opt out.

If you operate a joint loyalty scheme with other companies, you must make sure customers are fully aware of the nature of the scheme and range of the promotions you propose to send. In our view, under the soft

opt-in rule, as long as you do so and provide a clear opt-out when they sign up and in every message, the scheme may send electronic mail about incentives offered by any of the partners.

However, if a participating company wants to send additional marketing messages outside the loyalty scheme, it must have the individual's clear consent to do so. If there are several partners in a loyalty scheme, you may therefore find it easier to provide specific opt-in boxes when people sign up.

Can we send marketing by post?

PECR do not cover marketing by post, but if you are sending post to named individuals you must comply with the Data Protection Act and the UK GDPR.

Further Reading

 [Direct marketing guidance](#) 

For organisations

Cookies and similar technologies

In brief...

You must tell people if you set cookies, and clearly explain what the cookies do and why. You must also get the user's consent. Consent must be actively and clearly given.

There is an exception for cookies that are essential to provide an online service at someone's request (eg to remember what's in their online basket, or to ensure security in online banking).

The same rules also apply if you use any other type of technology to store or gain access to information on someone's device.

In more detail...

- [What is a cookie?](#)
- [What do we need to do to comply?](#)
- [What else is covered, apart from cookies?](#)
- [What information must we give users?](#)
- [What counts as consent?](#)
- [Do we need consent from the subscriber or from the user?](#)
- [Are there any exemptions?](#)
- [Do the rules still apply if the data is anonymous?](#)
- [Where can we get more information?](#)
- [How do these rules affect apps?](#)
- [Checklists](#)

What is a cookie?

A cookie is a small text file that is downloaded onto 'terminal equipment' (eg a computer or smartphone) when the user accesses a website. It allows the website to recognise that user's device and store some information about the user's preferences or past actions.

What do we need to do to comply?

The rules on cookies are in regulation 6. The basic rule is that you must:

- tell people the cookies are there;
- explain what the cookies are doing and why; and
- get the person’s consent to store a cookie on their device.

As long as you do this the first time you set cookies, you do not have to repeat it every time the same person visits your website. However, bear in mind that devices may be used by different people. If there is likely to be more than one user, you may want to consider repeating this process at suitable intervals.

You may also need to obtain fresh consent if your use of cookies changes over time.

What else is covered, apart from cookies?

Although this guide focuses on cookies, regulation 6 actually applies to anyone who stores information on a user’s device or gains access to information on a user’s device, in either case by any method.

This means the same rules apply to any similar technologies – such as Local Shared Objects (sometimes called Flash cookies) – and can also cover other types of technology, including [apps](#) on smartphones, tablets, smart TVs or other devices.

These rules also outlaw spyware or any similar covert surveillance software that downloads to a user’s device and tracks their activities without their knowledge.

What information must we give users?

PECR do not set out exactly what information you must provide or how to provide it – this is up to you. The only requirement is that it must be “clear and comprehensive” information about your purposes. You must explain the way the cookies (or other similar technologies) work and what you use them for, and the explanation must be clear and easily available. Users must be able to understand the potential consequences of allowing the cookies. You may need to make sure the language and level of detail are appropriate for your intended audience.

This is similar to the [transparency requirements](#) of the UK GDPR (privacy notices).

Further Reading

For further information, see our detailed [guidance on cookies](#) and the section of the Guide to the UK GDPR on the [right to be informed](#).

What counts as consent?

To be valid, consent must be freely given, specific and informed. It must involve some form of unambiguous positive action – for example, ticking a box or clicking a link – and the person must fully understand that they are giving you consent. You cannot show consent if you only provide information about cookies as part of a privacy policy that is hard to find, difficult to understand, or rarely read.

Similarly, you cannot set non-essential cookies on your website's homepage before the user has consented to them.

Consent does not necessarily have to be explicit consent. However, consent must be given by a clear positive action. You need to be confident that your users fully understand that their actions will result in specific cookies being set, and have taken a clear and deliberate action to give consent. This must be more than simply continuing to use the website. To ensure that consent is freely given, users should have the means to enable or disable non-essential cookies, and you should make this easy to do.

You should take particular care to ensure clear and specific consent for more privacy-intrusive cookies, such as those collecting sensitive personal data such as health details, or used for behavioural tracking. The ICO will take a risk-based approach to enforcement in this area, in line with our regulatory action policy.

For more advice on obtaining consent, including the rules on browser settings, see our [cookies guidance](#) and our [consent guidance](#).

Further Reading

For further information, see our detailed [guidance on cookies](#), as well as our [guidance on consent](#) in the Guide to the UK GDPR.

Do we need consent from the subscriber or from the user?

Regulation 6 states that consent should be obtained from the [subscriber or user](#).

In practice you may not be able to tell who is the subscriber and who is a user – which means you may not be able to distinguish between consent provided by the subscriber and by the user. The key will be that valid consent has been provided by one of them.

PECR does not say whose wishes should take precedence if they are different. If there appears to be a conflict – for example, if a subscriber or user previously consented but now the current user of the same device objects – it would seem sensible to rely on the most recent indication. This would mean you always respect the current user's preferences, even if you cannot be sure of the subscriber's preferences.

Further Reading

For further information, see our detailed [guidance on cookies](#).

Are there any exemptions?

There are two exemptions which apply where:

- the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or

- the cookie is strictly necessary to provide an 'information society service' (eg a service over the internet) requested by the subscriber or user. Note that it must be essential to fulfil their request – cookies that are helpful or convenient but not essential, or that are only essential for your own purposes, will still require consent.

This means you are unlikely to need consent for:

- cookies used to remember the goods a user wishes to buy when they add goods to their online basket or proceed to the checkout on an internet shopping website;
- session cookies providing security that is essential to comply with data protection security requirements for an online service the user has requested – eg online banking services; or
- load-balancing cookies that ensure the content of your page loads quickly and effectively by distributing the workload across several computers.

However, it is still good practice to provide users with information about these cookies, even if you do not need consent.

Further reading

For further information, [see our cookies guidance](#).

You may also want to refer to the opinion adopted by European data protection authorities in June 2012 ([Article 29 Working Party opinion 04/2012](#)), which clarifies that some usage of session-ID cookies, multimedia cookies, and user interface customisation cookies (eg language-preference cookies) is likely to fall within the information society services exemption.

Although this publication refers to the requirements of the e-privacy Directive and the old EU Data Protection Directive (which preceded the EU and UK versions of the GDPR), it is also useful for understanding the requirements of PECR.

Do the rules still apply if the data is anonymous?

Yes. Although cookies that process personal data give rise to greater privacy and security risks than those that process anonymous data, PECR apply to all cookies.

If your cookie data is not anonymous, note that you will also need to comply with the Data Protection Act and the UK GDPR. You may need to carry out a data protection impact assessment (DPIA). You may actually need to consider whether you could use anonymised data instead, in order to comply with the data protection principles (which require personal data to be adequate, relevant and not excessive). This is likely to be particularly relevant where you are not using the data to provide a service to the user – for example, if you are simply counting visitors to a website.

At the same time, you should be aware that the creation of anonymous information may involve processing of personal data – for example, to generate aggregate statistics based on user interaction. This processing would therefore be covered by the GDPR.

See our separate [Guide to UK GDPR](#) for more information.

Where can we get more information?

For more detailed information and practical advice on this topic, see our [guidance on cookies](#).

The ICO will continue to take a risk-based approach to enforcement in this area, taking into account the level of intrusion, the efforts made to provide clear information and get consent, and consumer concern. You can find more about the action we are taking on cookies on [the Enforcement section of the ICO website](#).

How do these rules affect apps?

Apps store information on smart devices, and some apps may also access information on the device (eg contacts or photos). App developers should therefore provide clear information to users about what the app does, and exactly how it uses their information, **before** users click to install the app. It is also important to consider user privacy controls and avoid switching optional features on by default. This ties in closely with the requirements of the Data Protection Act and the UK GDPR.

Further reading – ICO guidance

For more information on how to comply, see our separate guidance [Privacy in mobile apps](#). Although written under the 1998 Act, it may still assist you.

Checklists

Understanding cookies

- We understand what cookies are and what they can be used for.
- We know the difference between session cookies and persistent cookies.
- We know the difference between first party and third party cookies.
- We understand what 'similar technologies' are and how PECR applies to them.

Auditing our use of cookies

- We know what cookies our online service either already uses or intends to use.
- We have removed any cookies that we don't need.
- We have confirmed the purposes of each cookie.

- We identify what information each cookie processes, including whether they are linked to other information we hold about our users or otherwise involve processing personal data.
- Where personal data is involved, we have ensured that we process this data in line with the requirements of the UK GDPR.
- We have confirmed whether our cookies are session or persistent cookies.
- We have confirmed whether our cookies are first party or third party cookies.
- We have appropriate arrangements in place for the use of any third-party cookies, including what information they share with any third party, how it is shared, and what our users are told.
- We have established how long our cookies last and that this duration is appropriate.
- We have identified those cookies that are strictly necessary, and those that are not.

Information about cookies

- We have ensured that we provide clear and easy to understand information about the cookies we use.
- We have ensured that our information is comprehensive and covers all the cookies we use.

Consent for cookies

- We have implemented a consent mechanism that allows users of our online service to control the setting of all cookies that are not strictly necessary.
- We ensure that our consent mechanism ensures the consent we obtain is in line with the UK GDPR's requirements.
- We keep any records of cookie consent for an appropriate period of time.

Documenting and reviewing our cookie use

- We have documented all of the above.
- We have built in an appropriate review period.

Communications networks and services

PECR are not just concerned with marketing by electronic means. They also contain provisions that concern the security of public electronic communications services and the privacy of customers using communications networks or services.

Some of these provisions only apply to service providers (eg the security provisions) but others apply more widely. For example, the directories provision applies to any organisation wanting to compile a telephone, fax or email directory.

This part of the guide explains the rules on communications networks and services.

Security of services

In brief...

Service providers must take appropriate measures to safeguard the security of their service. What 'appropriate' means depends on the nature of the risk, the technology available, and the cost.

Service providers must also inform their customers of any significant security risks.

In more detail...

- [Who has security obligations?](#)
- [What must we do to comply?](#)
- [What are 'appropriate measures'?](#)
- [What must we tell our customers about security risks?](#)

Who has security obligations?

[Service providers](#) (eg telecoms providers or internet service providers) must safeguard the security of that service.

Network providers (organisations that operate and maintain the underlying [network](#)) must comply with any reasonable security requests made by the service provider.

What must we do to comply?

Security obligations are set out in regulation 5. If you are a service provider, you must take appropriate technical and organisational measures to safeguard the security of your service.

You must also inform your customers of any significant security risks.

What are 'appropriate measures'?

An appropriate measure is one that is proportionate to the risks it safeguards against. You can take into account the state of technological development and the cost of implementing the measure.

Regulation 5(1A) says these measures must at least:



“(a) ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;

(b) protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure; and

(c) ensure the implementation of a security policy with respect to the processing of personal data.”

These provisions are similar to security obligations in the UK GDPR, although PECR security obligations for service providers override the equivalent UK GDPR provisions. However, our [Guide to GDPR is still a useful source of guidance on security measures](#).

Regulation 5(2) says that, if necessary, you should take measures in conjunction with the network provider. This regulation aims to ensure reasonable cooperation between service and network providers.

The ICO has the power to audit a service provider's security measures.

What must we tell our customers about security risks?

If you take appropriate measures but there is still a significant risk to the security of the service, you must inform subscribers of:

- the nature of the risk;
- any measures they can take to safeguard against it; and
- the likely cost to them of taking those measures.

You must provide this information free of charge, except for any nominal costs the subscriber may have in receiving or collecting the information (eg the cost of downloading an email).

Security breaches

In brief...

Service providers are required to notify the ICO if a 'personal data breach' occurs. They must also notify customers if the breach is likely to adversely affect customers' privacy, and keep a breach log.

In more detail...

- [What is a 'personal data breach'?](#)
- [What must we do if there is a breach?](#)
- [When and how do we notify the ICO?](#)
- [When and how do we notify our customers?](#)
- [What do we need to record in our breach log?](#)

What is a 'personal data breach'?

A personal data breach is:



"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service".

A personal data breach may mean that someone other than the data controller gets unauthorised access to personal data. But a personal data breach can also occur if there is unauthorised access within an organisation, or if a data controller's own employee accidentally alters or deletes personal data.

What must we do if there is a breach?

[Service providers](#) (eg telecoms providers or internet service providers) have certain obligations if a personal data breach occurs. These are set out in regulation 5A.

If you are a service provider, you must:

- notify the ICO;

- consider whether to notify your customers; and
- record details in your own breach log.

This takes the place of UK GDPR breach reporting obligations. You don't need to take any separate action to comply with the UK GDPR.

When and how do we notify the ICO?

You must notify the ICO within 24 hours of becoming aware of the essential facts of the breach. This notification must include at least:

- your name and contact details;
- the date and time of the breach (or an estimate);
- the date and time you detected it;
- basic information about the type of breach; and
- basic information about the personal data concerned.

Please use our [breach notification form](#). You can attach documents to the form if necessary.

If possible, you should also include full details of the incident, the number of individuals affected and its possible effect on them, the measures taken to mitigate those effects, and information about your notification to customers. If these details are not yet available, you must provide them as soon as possible. You must submit a second notification form to us within three days, either including these details, or telling us how long it will take you to get them.

Failure to submit breach notifications can incur a £1,000 fine.

When and how do we notify our customers?

If the breach is likely to adversely affect the personal data or privacy of your [subscribers or users](#), you need to notify them of the breach without unnecessary delay. You need to tell them:

- your name and contact details;
- the estimated date of the breach;
- a summary of the incident;
- the nature and content of the personal data;
- the likely effect on the individual;
- any measures you have taken to address the breach; and
- how they can mitigate any possible adverse impact.

You do not need to tell your subscribers about a breach if you can demonstrate that the data was encrypted (or made unintelligible by a similar security measure).

If you do not tell your customers, the ICO can require you to do so if we consider the breach is likely to adversely affect them.

What do we need to record in our breach log?

You must also keep your own record of all personal data breaches in an inventory or log. It must contain:

- the facts surrounding the breach;
- the effects of the breach; and
- remedial action taken.

We have produced a [template log](#) to help you record the information you need. We also ask you to [submit your log](#) to us on a monthly basis.

For more information, see our detailed guidance for service providers on [notification of PECR security breaches](#).

Traffic data

In brief...

You can only process traffic data (eg information about the routing, duration or timing of a message) for limited purposes with the authority of the network or service provider.

You must tell customers if you keep their traffic data, and get their consent before using it for marketing or value-added services. You must erase or anonymise it as soon as you have finished with it (unless another law requires you to keep it).

In more detail...

- [What is traffic data?](#)
- [What are the rules on traffic data?](#)
- [Who needs to comply?](#)
- [What can we use traffic data for?](#)
- [What information must we give customers?](#)
- [When do we need consent?](#)
- [What counts as consent?](#)
- [How long can we keep traffic data?](#)

What is traffic data?

Traffic data is defined as:



“any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing in respect of that communication and includes data relating to the routing, duration or time of a communication”.

This includes information about the routing or timing of any phone call, text or email, whether it relates to an individual or a company.

The focus here is on data collected and processed by a [public communications provider](#). It is not likely to include data collected by another party via another route (eg data collected directly from nearby mobile

devices by an organisation's wi-fi equipment).

What are the rules on traffic data?

The rules on traffic data are in regulations 7 and 8. Only [public communications providers](#), or those acting under their authority, can process traffic data. In summary, if you are processing traffic data, you must:

- only use it for permitted purposes;
- give your customers information about the processing;
- get their consent for certain uses of the data; and
- erase or anonymise it as soon as you have finished with it (unless another law requires you to keep it).

There is an exemption for emergency alerts where a relevant public authority needs to warn, advise or inform users or subscribers of an emergency in their location (regulation 16A).

Who needs to comply?

The relevant [public communications provider](#) has ultimate responsibility for complying with these rules. If you are a network or service provider and are using a third-party data processor to process traffic data on your behalf, you need to take steps to ensure they comply with PECR. In particular, you should have a written contract setting out what the data processor is allowed to do.

This is similar to UK GDPR contract obligations – but remember that to comply with PECR the contract needs to cover the traffic data of corporate subscribers as well as the personal data of individuals. See our separate [Guide to UK GDPR for more information on general contract obligations](#).

However, anyone else processing traffic data without proper authority would also be in breach of PECR.

What can we use traffic data for?

Network providers can only process traffic data:

- to manage billing or traffic;
- to handle customer enquiries;
- to prevent or detect fraud.

Service providers can also process traffic data:

- to market electronic communication services (with consent);
- to provide a 'value-added service' (with consent).

The processing must be restricted to what is necessary for these activities. However, PECR do not prevent you providing traffic data to Ofcom or any other authority that has statutory authority to resolve disputes.

What information must we give customers?

You must give the relevant [subscriber or user](#) information about the type of traffic data you will be processing for billing, marketing or value-added services, and how long you will keep it.

PECR do not specify how to provide this information. However, the information should be clear and easily available – and remember that if you need to get consent for your processing, the consent won't be valid if the information is buried in a privacy policy. (See below for more on [what counts as consent](#).)

This ties in with the transparency requirements of the UK GDPR. Although the UK GDPR won't apply to traffic data where the PECR rules apply, following the approach in our [UK GDPR guidance on transparency](#) can also help you comply with the PECR transparency requirements.

When do we need consent?

You need consent if you want to use or store someone's traffic data for marketing purposes, or to provide any value-added service.

'Marketing' in this context is not limited to direct marketing by phone, text or email. For example, it may also include using traffic data to analyse a customer's usage patterns to offer alternative tariffs.

A 'value-added service' is defined as:



"any service which requires the processing of traffic data or location data beyond that which is necessary for the transmission of a communication or the billing in respect of that communication".

This may, for example, include an email content-filtering service offered by an internet service provider, which monitors traffic data to scan incoming emails. It may also include a mobile network operator using their customers' traffic data to target advertising.

What counts as consent?

To be valid, consent must be freely given, specific and informed. It must involve some form of clear positive action – for example, ticking a box, clicking a link, sending an email, or subscribing to a service – and the person must fully understand that they are giving you consent to use traffic data. You cannot show consent if you only provide information about the use of traffic data as part of a privacy policy that is hard to find, difficult to understand, or rarely read.

You will not be able to rely on a blanket 'catch-all' statement on a bill or website, and should get separate consent for marketing and for each value-added service requested. The clearest way to obtain consent is to use specific opt-in boxes.

PECR also specify that you must get consent from the person who the data is actually about – who might be a [subscriber or a user](#). For this reason it may not always be enough to rely on consent given by the subscriber in advance when they signed up to a contract, if someone else will actually be using the connection.

In the case of companies and other corporate subscribers (limited liability partnerships, Scottish partnerships and government bodies), you can accept assurances from a representative giving consent on behalf of the organisation, unless you have reasonable grounds to question their authority.

PECR specify that consent must be given to the provider. If the relevant value-added service is offered by a third party (with your authority), you should make it very clear that the traffic data will be passed to that third party. If the customer gives consent to a provider for a particular service, they should not then be surprised when they are contacted by a third party about that service.

Remember that the customer is entitled to withdraw their consent at any time, in which case you should immediately stop using the traffic data for marketing or value-added services. You should make it easy to withdraw consent, and tell people how.

How long can we keep traffic data?

The general rule is that you must erase or anonymise the data when it is no longer needed to transmit a communication – in other words, as soon as the message has been sent or the phone call has ended.

Of course, if the traffic data is still required for billing purposes, you will need to keep it longer in order to calculate charges. PECR say you can keep this billing data until the end of the period in which proceedings can be brought to challenge the bill or chase payment (including the period for appealing any decisions). In terms of contract law, this would usually mean a limitation period of six years (plus appeals time).

However, in our view it will not usually be necessary to keep the data for this long. You should only keep it when the circumstances require this – for example, if the bill remains unpaid or has been challenged before being paid. You also need to have told the customer how long you plan to keep this data.

If you have consent to keep the traffic data for marketing or value-added services, you can only keep it for as long as is necessary for those purposes. Again, you also need to have told the customer how long you plan to keep it.

There is an exemption if another law requires you to keep the data for longer than this – for example, for national security or crime prevention reasons. You need to set up procedures for allowing access to the data in such cases. See the [exemptions section of this guide](#) for more information.

Location data

In brief...

You can only process location data (information from the network or service about the location of a phone or other device) with the authority of the network, service or value-added service provider, and only if:

- it is anonymous; or
- you have consent to use it for a value-added service.

In more detail...

- [What is location data?](#)
- [What are the rules on location data?](#)
- [Who needs to comply?](#)
- [What is a 'value-added service'?](#)
- [How should we get consent?](#)

What is location data?

Location data is defined as:



“any data processed in an electronic communications network or by an electronic communications service indicating the geographical position of the terminal equipment of a user of a public electronic communications service, including data relating to—

- (f) the latitude, longitude or altitude of the terminal equipment;
- (g) the direction of travel of the user; or
- (h) the time the location information was recorded”.

In other words, it is information collected by a network or service about where the user’s phone or other device is or was located – for example, tracing the location of a mobile phone from data collected by base stations on a mobile phone network.

In our view, this does not generally include GPS-based location information from smartphones, tablets, sat-navs or other devices, as this data is created and collected independently of the network or service

provider. Neither does it include location information collected at a purely local level (eg by wi-fi equipment installed by businesses offering wi-fi on their premises). However, organisations using such data still need to comply with the Data Protection Act.

What are the rules on location data?

The rules on location data are in regulation 14 and are very strict. You can only process location data if you are a [public communications provider](#), a provider of [a value-added service](#), or a person acting on the authority of such a provider, and only if:

- the data is anonymous; or
- you have the user's consent to use it for a value-added service, and the processing is necessary for that purpose.

This regulation does not apply if the data is traffic data. See above for more information on [when you can use traffic data](#).

There is an exemption for emergency 999 or 112 calls (regulation 16). There is also an exemption for emergency alerts where a relevant public authority needs to warn, advise or inform users or subscribers of an emergency in their location (regulation 16A).

Who needs to comply?

The relevant [public communications provider](#) has ultimate responsibility for complying with these rules. If you are a network or service provider and you are passing location data to a third-party value-added service provider, or using a third-party data processor to process location data on your behalf, you need to take steps to ensure they comply with PECR. In particular, you should have a written contract with any data processor setting out what the data processor is allowed to do.

This is similar to UK GDPR contract obligations – but remember that to comply with PECR the contract needs to cover the location data of corporate users as well as the personal data of individuals. See our separate [Guide to UK GDPR for more information on general contract obligations](#).

However, anyone else processing location data without proper authority would also be in breach of PECR.

What is a 'value-added service'?

A 'value-added service' is defined as:



“any service which requires the processing of traffic data or location data beyond that which is necessary for the transmission of a communication or the billing in respect of that communication”.

This may include, for example, a call service that locates the driver of a broken-down vehicle, a 'find my

phone' service offered by a mobile provider, or a mobile network operator using their customers' location to target location-specific content.

How should we get consent?

To be valid, consent must be freely given, specific and informed. It must involve some form of clear positive action – for example, ticking a box, clicking a link, sending an email, or subscribing to a service – and the person must fully understand they are giving you consent to use their location data. You cannot show consent if you only provide information about the use of location data as part of a privacy policy that is hard to find, difficult to understand, or rarely read.

PECR specify that you must give the user or subscriber information about:

- the types of location data you will be processing;
- what you are using it for;
- how long you will keep it; and
- whether it will be passed to a third party to provide the value-added service.

You will not be able to rely on a blanket 'catch-all' statement on a bill or website, and should get separate consent for each value-added service requested. The clearest way to obtain consent is to ask for an explicit opt-in to the use of location data.

PECR also specify that you must get consent from the person who the data is actually about – who may be a [subscriber or a user](#). For this reason it may not always be enough to rely on consent given by the subscriber in advance when they signed up to their contract, if someone else will actually be using the connection.

In the case of companies and other corporate subscribers (limited liability partnerships, Scottish partnerships and government bodies), you can accept assurances from a representative giving consent on behalf of the organisation, unless you have reasonable grounds to question their authority.

PECR specify that the network or service provider must provide the relevant information. However, if the relevant value-added service is offered by a third party, we accept that it is likely to be more appropriate for the third-party provider to contact the customer directly to provide information and obtain the relevant consent. The important point is that the customer must understand who is using the data and who is providing the service.

Remember that the customer is entitled to withdraw their consent at any time, in which case you should immediately stop using the location data. You must give users a free and easy way to withdraw their consent each time they connect to the network or send a communication. You may also want to offer the option of changing their settings to temporarily withdraw consent. However, you must make the effect of this very clear so that the customer understands exactly how this works and in what circumstances their consent would be reactivated.

Itemised bills

In brief...

Customers have the right to receive bills that are not itemised.

In more detail...

[Who needs to comply?](#)

[What are the rules on itemised bills?](#)

Who needs to comply?

These rules apply to [service providers](#) (eg telecoms providers or internet service providers).

What are the rules on itemised bills?

Regulation 9 says that if a [subscriber](#) asks to receive bills that are not itemised, you must comply with that request. So you can send itemised bills as long as the customer hasn't asked you not to.

This recognises the fact that itemised bills may put the privacy of users at risk, even though many subscribers may find them useful to verify the amount of the bill.

The rights of subscribers who want to receive itemised bills need to be balanced with the privacy of other users. Ofcom also recognises privacy in its sector rules ('General Conditions'). For example, General Condition C3 says subscribers can request itemised bills; but it also says that itemised bills should not include calls to Freephone numbers (which may include helplines). For further information please see [Ofcom's website](#) [↗](#).

Line identification (CLI)

In brief...

If you are a service provider, you must provide information about CLI and related privacy services. You must enable customers to withhold their number, and to reject anonymous calls.

There are exemptions for tracing malicious or nuisance calls, and for emergency 999 or 112 calls.

In more detail...

- [What is CLI?](#)
- [What are the rules on CLI?](#)
- [Who needs to comply?](#)
- [What privacy options must we give callers?](#)
- [What privacy options must we give customers receiving calls?](#)
- [Can we charge for any of these services?](#)
- [Are there any exemptions?](#)

What is CLI?

CLI can mean either 'calling line identification' or 'connected line identification'.

Calling line identification allows the person receiving the call to see the caller's number. This covers caller ID displays as well as the 1471 service and other call-return services.

Connected line identification works the other way round: it allows the caller to see the number of the person answering the phone. This may not always be the same as the number they dialled – for example, where someone has forwarded out-of-hours business calls to their private line or mobile phone.

What are the rules on CLI?

The rules about CLI are in regulations 10 to 13. In brief, where CLI is available, service providers must:

- allow callers to withhold their number;
- allow called subscribers to prevent the caller's number being displayed;
- provide an anonymous-call rejection service;
- allow called subscribers to withhold their number; and

- provide information to the public about CLI services.

Further Reading

 [Ofcom's Guidelines for the provision of Calling Line Identification Facilities and other related services over Electronic Communications Networks](#) 

External link

Who needs to comply?

These rules apply to all [service providers](#) (eg telecoms providers). All network or service providers must also comply with any reasonable requests from another service provider in this area.

What privacy options must we give callers?

You must give your [subscribers](#) the option of automatically preventing caller ID (in other words, to withhold their number) on every call made on their line. This option should be free and simple.

You must also provide a free and simple way for any [user](#) to withhold the number on a particular call (even if the subscriber has not chosen to automatically withhold the number on every call) – for example, by entering a prefix code before dialling the phone number they wish to call.

What privacy options must we give customers receiving calls?

You must give your customers the option of preventing caller ID on incoming calls. This is likely to be important for helplines that guarantee the caller's anonymity, such as The Samaritans, Alcoholics Anonymous or police information lines. This option must be free (for reasonable use) and simple.

You must give your customers a simple way of rejecting calls if the caller has withheld their number (sometimes called anonymous call rejection, or ACR). Because this must be available to the [subscriber](#) and not just the user, our view is that you must offer automatic call rejection. We are aware that automatic network-level call rejection is not currently feasible on all categories of service, for example on mobile services. We therefore advise that automatic network-level call rejection should be offered where it is technically feasible for the category of service. You must offer other options – eg a call-reject button on the device – if automatic network-level call rejection is not possible.

You must also give customers receiving calls the option of withholding their number from the caller. This is to preserve their privacy if they have forwarded calls to a different number from the one the caller dialled – for example, if business calls have been forwarded to a mobile phone. This option should be free and simple.

Regulation 17 also requires service providers to terminate unwanted call forwarding. If someone else is automatically forwarding calls to your customer's number, that customer can ask you to stop the call forwarding and you must do so as soon as possible.

Can we charge for any of these services?

PECR specify that you must provide most of these services free of charge. However, you may make a reasonable charge for anonymous call rejection services.

There is nothing in PECR to stop you charging for CLI itself.

Are there any exemptions?

You can only override a customer's CLI preferences in limited circumstances, namely to trace malicious or nuisance calls or to facilitate emergency 999 and 112 calls.

Malicious or nuisance calls

The rules about malicious or nuisance calls are in regulation 15. If a customer asks you to trace malicious or nuisance calls, you can override the caller's request to withhold their number – but you must be satisfied that your actions are 'necessary and expedient' to trace a malicious or nuisance call.

You can also provide information about the caller's identity to anyone with a 'legitimate interest' (this is not defined, but is likely to include the police or a regulatory body, as well as the customer receiving the calls).

However, you should still be cautious with requests for information about a caller's identity. For example, if you are not satisfied that the caller has actually been making malicious or nuisance calls, it may not be fair or appropriate to reveal their identity to the customer receiving the calls. But it may still be appropriate to pass their identity to the police for further investigation.

Emergency 999 and 112 calls

Regulation 16 sets out an exemption for emergency 999 or 112 calls. Callers cannot withhold their number on these calls. This is to enable the emergency services to make return calls if needed. Also the rules on location data do not apply, so that the emergency services can be informed of the caller's location quickly and easily.

Directories

In brief...

If you want to compile a telephone, fax or email directory or offer a directory enquiry service, you must tell individuals and give them the chance to opt out. You must also get express opt-in consent for reverse searches (eg using a phone number to look up a name).

In more detail...

- [What kind of directories are covered?](#)
- [What do we need to do to comply?](#)
- [What information must we provide?](#)
- [Do we need consent to put people in our directory?](#)
- [Who should we leave out?](#)

What kind of directories are covered?

There is no definition of directory, but the regulations refer to:



“a directory of subscribers, whether in printed or electronic form, which is made available to members of the public or a section of the public, including by means of a directory enquiry service”.

This means any directory or service whose main function is to allow someone with a minimum amount of information (such as name and approximate address) to look up phone, fax or email contact details (including mobile phone numbers).

In our view, this does not cover types of directory that are not solely or mainly to provide a comprehensive list of subscribers' contact details, even if they include some contact details of a particular group of people. For example, trade directories whose main purpose is to provide detailed information about certain types of businesses would not be covered, nor would church or club membership contact lists. Similarly, we do not consider that WHOIS look-up services are covered. The main purpose of WHOIS is to search for information about the identity of the person who has registered a website, rather than to search for contact details of subscribers.

What do we need to do to comply?

The rules on directories are in regulation 18. In brief, if you want to compile a directory, you must:

- tell individual subscribers;
- give them the chance to choose whether to be included;
- get their express consent for reverse searches; and
- correct or withdraw entries on request.

You cannot charge for opt-outs or corrections.

What information must we provide?

Before you can include an individual in a directory, you must explain its purposes to them. In particular, your explanation should include:

- what the directory is and what information is included;
- that people who know their name and approximate address will be able to look up their phone number;
- whether people with their phone number will be able to look up their name and address (reverse searches); and
- how to opt out.

If you offer a range of ex-directory options, you must explain how each of them works. The individual must understand the consequences of choosing particular options.

There is an established competitive market in telephone directory information services and products. A core set of minimum information is needed for a directory to work, but you can decide what additional personal data is relevant to your particular directory. The more the information differs from what directories traditionally publish (name, address and phone number), the more information you will need to give people to ensure they understand what you are doing with their personal data.

This also ties in with the transparency requirements of the UK GDPR. See our separate [Guide to UK GDPR](#) for more information.

You do not have to provide this information to companies or other corporate subscribers (limited liability partnerships, Scottish partnerships and government bodies).

Do we need consent to put people in our directory?

You must give individuals the chance to decide whether they want to be included.

PECR do not say this needs to be opt-in consent. However, you must at least give individuals a clear chance to opt out. The person must fully understand they have made a choice and will be included in the directory unless they opt out, and it must be simple to opt out. You must have given clear and prominent information about how to opt out and specifically drawn the person's attention to this – it is not enough to rely on 'small print' on your website or on a bill.

However, you will need express opt-in consent if your directory includes reverse searches that allow people to look up a name and address from a phone number. Consent must always be freely given, specific, and fully informed, and will not be valid if it is buried among terms and conditions. The clearest way to obtain consent for reverse searching will be to provide a specific opt-in box and a clear and concise explanation of how searches work.

This does not apply to companies or other corporate subscribers (limited liability partnerships, Scottish partnerships and government bodies) – although they still have the right to opt out.

Who should we leave out?

You cannot include any individual if you have not yet given them the relevant information or the chance to opt out.

You cannot include any individual or business who has told you they want to opt out.

You must also remove or correct someone's details on request. This only applies to future editions of your directory. In other words, you do not need to recall existing editions of printed directories – but you must amend future printed editions, and you must update online versions as soon as possible.

Exemptions

In brief...

There are only two general exemptions from PECR: a national security exemption, and a law and crime exemption (for compliance with other laws, law enforcement, or legal advice or proceedings). You should consider these exemptions on a case-by-case basis.

There is no exemption for contractual obligations.

In more detail...

- [Are there any exemptions from PECR?](#)
- [How does the national security exemption work?](#)
- [How does the law and crime exemption work?](#)
- [Can we contract out of PECR?](#)
- [Is there anything else we need to think about?](#)

Are there any exemptions from PECR?

Some of the rules have built-in exemptions – for example, [exemptions from the cookie rules](#). These are covered in the section of this guide that explains those rules.

There are also two more-general exemptions that can apply to any of the rules: a national security exemption, and a law and crime exemption (in brief, for compliance with other laws, law enforcement, or legal advice or proceedings). Only [communications providers](#) can use these exemptions.

These exemptions do not automatically exempt you from all the rules. They will only apply to the extent that compliance with PECR actually conflicts with the relevant interests. If you can still comply with some of the rules in PECR, you must.

How does the national security exemption work?

The national security exemption is in regulation 28. It exempts communications providers from any of the rules in PECR if that exemption is required (ie you reasonably need to breach that regulation) for the purpose of safeguarding national security.

A Minister of the Crown can issue a certificate stating that an exemption was, is or will be required in certain circumstances for national security reasons. A ministerial certificate is conclusive proof that the

exemption applies in those circumstances. Any person directly affected by a ministerial certificate may appeal against it to the Information Rights Tribunal.

How does the law and crime exemption work?

The law and crime exemption is in regulation 29. It exempts communications providers from any of the rules in PECR if complying with that rule would:

- breach a provision of another enactment;
- breach a court order;
- be likely to prejudice the prevention or detection of crime; or
- be likely to prejudice the apprehension or prosecution of offenders.

It also applies if the exemption is required (ie, you need to breach that regulation):

- for or in connection with any legal proceedings;
- to obtain legal advice; or
- to establish, exercise or defend legal rights.

Can we contract out of PECR?

No. You cannot agree to disapply PECR, and there is no exemption for contractual obligations.

Regulation 27 says any term in a contract between a service provider and a subscriber or network provider that is inconsistent with PECR will be automatically void.

Is there anything else we need to think about?

If you are a [communications provider](#), you need to set up procedures for responding to other bodies who ask for access to your customers' personal data for national security or law enforcement reasons.

If such a request is justified, it is likely to be exempt from PECR. However, regulation 29A requires you to establish and maintain internal procedures in these circumstances. The ICO can require you to provide information about your procedures, the number of requests you have received, the legal justification for the request, and your response.

Complaints

If someone complains about your electronic marketing (eg spam calls or texts), cookies or other privacy issues regarding electronic communications, we will record and review their concerns, and we may investigate your compliance with PECR. If we decide it is likely you have failed to comply with PECR or other data protection legislation, we may ask you to take steps to remedy this and avoid similar complaints in future. If appropriate, we may decide to take [enforcement action](#).

We do not always investigate individual complaints. However, we do encourage individuals to report their concerns to us. Although we do not investigate every individual complaint, we use this information to monitor compliance and decide where to take enforcement action. Our enforcement action is likely to focus on organisations that generate the most complaints.

The [concerns section of our website](#) contains more information on when and how individuals can report their concerns to us.

If someone suffers damage because you breached PECR, they can also make a claim against you in court for compensation under regulation 30, without involving the ICO. A possible defence to such a claim is to prove that you took all reasonable care to comply.