Data Protection and PECR Training

Supporting notes and further reading

Module 14 : PECR

Introduction

These notes are designed to set out the key points covered during module 14 of our data protection online training programme. These notes are not designed to replace the online module, but are intended to be a point of reference for your follow-up study. You may find it helpful to have these notes and the relevant legislation open whilst watching the online module:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018 (DPA), and
- The Privacy and Electronic Communications Regulations (PECR)

This document contains:

Supporting notes

Module 14 looks at the Privacy and Electronic Communications Regulations, known as PECR. It covers:

Introduction to PECR

PECR sits alongside the DPA and the UK GDPR. It gives people specific privacy rights in relation to electronic communications.

It implemented the 2002 European ePrivacy Directive, and has been amended a number of times since then.

There are two distinct parts to PECR:

The first part is its non-marketing requirements. This covers:

- cookies (and similar technologies),
- keeping communications services secure,
- and customer privacy in terms of traffic and location data, itemised billing, line identification, and directory listings.

Traffic data is information about the routing or timing of any phone call, text or email.

The second part of PECR concerns requirements for unsolicited direct marketing. This could be by:

- phone,

- electronic mail (for example, text message and email), and
- fax.

Remember that if the direct marketing involves personal data, it also falls under the UK GDPR. Furthermore, direct marketing addressed to named individuals and sent **by post** only falls under the UK GDPR.

Key definitions

There are a number of definitions within PECR.

A service provider - someone who provides any service allowing members of the public to send electronic messages. This includes providers of telephone or internet services.

A subscriber - the person who has entered into a contract with the service provider and pays the bills. There are two types of subscriber:

> **An individual subscriber** – who can also be a sole trader or non-limited liability partnership in England, Wales or Northern Ireland. It means the person whose name is on the bill. So your name might be on your telephone bill and you are the subscriber.
>
> **A corporate subscriber** - a corporate body such as a limited company, or a public body such as the ICO. It can also be a limited liability partnership and covers all partnerships in Scotland. An example of this in practice means the ICO is a corporate subscriber for its telephones.

A user - any individual using a public electronic communications service (i.e. using the phone or internet connection). For example, the individual subscriber to a mobile phone could be the parent but the user is their teenage daughter.

PECR and personal data

Although it's a separate piece of legislation, PECR does have links with both the UK GDPR and the DPA.

When PECR requires consent, it must be to the UK GDPR standard.

When we discuss direct marketing, we will also refer to the DPA definition provided in section 122 and the UK GDPR Article 21 right to object. However, we'll see that PECR is broader than data protection legislation because it doesn't just protect individuals.

In other areas where PECR already covers an issue, similar UK GDPR obligations will not apply.

For example, PECR has its own regulations for:

- the security obligations of a telecoms provider, and
- personal data breach reporting.

So to avoid duplication, the UK GDPR doesn't apply where there are already specific PECR rules.

The UK GDPR and DPA cover the processing of personal data and only protect the data subject as a living individual.

PECR isn't about personal data – its provisions are wider and it can cover businesses as well. It applies to subscribers - so as well as individuals it also protects corporate subscribers. There are different rights for individual and corporate subscribers.

Just because PECR applies doesn't mean organisations can forget about the UK GDPR. An organisation is often processing personal data when it sends marketing. For example, an individual's email address will be personal data because it identifies a unique user and distinguishes them from other users, and a business email address may be personal data.

In some cases, the use of cookies will involve the processing of personal data. In these circumstances, an organisation will need to consider the UK GDPR provisions as well as the relevant PECR rules.

Traffic data

Traffic data includes information about routing, duration of calls and sessions and times of communication. For example, this applies to information about your telephone calls, and is about data that's collected and processed by a public communications provider like BT, EE or Vodafone.

If an organisation is processing traffic data, it must:

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

Telephone calls and privacy

A subscriber can ask for a bill **NOT** to be itemised to protect the privacy of individuals using the phone (for example, companies paying for an employees phone contract may not want to see every call made because this would be a privacy risk).

There are also rules surrounding the visibility of telephone numbers. Service providers must provide users with the ability to reject anomymous incoming calls, and to withhold their number when making a call (either automatically on all placed calls, or on an individual call basis by dialling 141 before placing the call).

A subscriber must also be able to prevent the display of a calling number (for example, a mental health charity might do this to preserve the privacy of the caller), and prevent the display of all connected lines (meaning the caller can't see the number of the lines they have connected to). An example of this in practice would be if you called a business on its main helpline number and your call is forwarded on to a mobile number - this wouldn't be displayed to you.

Location data

Location data concerns the geographical position of equipment such as a phone, computer or tablet. These devices can record information such as latitude, longitude, direction of travel and time location.

An organisation can only process location data if it is a public communication provider, a provider of a value-added service, or a person acting on the authority of such a provider. In these circumstances, organisations can still only do this if:

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

Examples of a value added service may include:

- a call service locating 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.

This doesn't cover GPS apps (such as maps and navigation) on mobile devices. This is because the app receives GPS signals independently from the cellphone network, and indidivuals have control over how this GPS data is used.

There are certain circumstances where the PECR provisions around privacy and location data don't apply. Eg, a telecoms company is allowed to trace malicious or nuisance calls at the request of the subscriber and this overrides the provisions that allow callers to withhold their number.

In the case of emergency calls such as 999 a caller can't withhold their number and restrictions on processing location data are overridden. This enables return calls to be made and means emergency services can be informed of location quickly and easily. Caller display may also prevent hoax calls.

A public communications provider can issue an emergency alert if asked to do so by a public authority, to warn or inform users or subscribers about an emergency in their area like a terrorist attack or flood. Again, this overrides the restrictions on processing traffic data.

Directories

PECR applies to public directories such as telephone directories.

The person collecting the personal data of the individual subscribers to be included in the directory must:

- inform them of the purposes of the directory (this echoes the UK GDPR transparency requirements);
- give them the opportunity to refuse; and
- allow them to verify, correct or withdraw their details at any time.

These must all be made available free of charge.

A corporate subscriber must be able to tell the producer of a directory that it does not want its data to be included.

Reverse searching involves taking a telephone number and using this to identify the name, address or other details of a subscriber. If this is undertaken, then the organisation must obtain the express consent of the data subject - and remember its obligation to provide transparency information under the UK GDPR.

Cookies and similar technologies

A cookie is a small text file that is downloaded onto 'terminal equipment' (for example, 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. Software on your computer (normally your web browser) can store these cookies and send them back as part of the request next time you visit the site.

Cookies are widely used in order to make websites work, or to work more efficiently, as well as to provide information to the owners of the site.

Without cookies, or something similar, websites would have no way to 'remember' visitors.

Examples of cookies include where they are used to:

- remember what's in your basket when shopping for goods online;
- track your browsing behaviour and target advertising to you.

Organisations 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.

There are two exemptions to the consent requirement. Consent is not needed if:

- the cookie is for the sole purpose of carrying out the transmission of a communication, or
- the processing is strictly necessary to provide the service requested by the subscriber or user; eg cookies for shopping baskets.

Direct marketing

Direct marketing is defined in section 122 of the DPA and applies to PECR. It means the communication (by whatever means) of advertising or marketing material which is directed to particular individuals. The DPA definition is wider than PECR in that it covers any communication whereas PECR only covers unsolicited electronic marketing - for example by telephone calls, electronic mail, texts or other types of messages.

The interpretation of the term 'advertising' is intended to be broad. It's not just about the promotion of products or services but will include fundraising and campaigning (where aims and ideals are promoted). This includes political parties which have to comply with PECR for campaigning activities that involve making calls and sending text or email messages.

If a message contains elements that are direct marketing then the marketing rules apply, even if that is not the main purpose of the message. There are no restrictions on solicited marketing where someone has asked for the marketing (for example, if someone emails a kitchen company to ask for details of any current offers on new cabinets).

PECR rules only apply to unsolicited marketing. Even if the customer ticked a box agreeing to the kitchen company's direct marketing, any emails detailing new offers will still be technically unsolicited - because the customer didn't specifically ask for that particular marketing material.

Examples of unsolicited direct marketing which fall under PECR:

- charities making phone calls to ask for donations
- a mobile phone company advertising a new phone by text message
- a political party sending emails to promote their aims and policy ideas
- a company emailing out a market research questionnaire but also advertising its products (if it was pure market research with no promotional material then it would not be direct marketing)
- an automated call from a private company about a flu outbreak. If this is from a company trying to sell its 'flu jab' then it is marketing
- an email from a lender to an individual asking them to register for a company credit card

PECR and consent

In many circumstances, an organisation needs consent in order to send **unsolicited direct marketing by electronic means** – with PECR using the UK GDPR definition of consent.

It reinforces the need to be specific and informed by requiring that the consent is specific to the method of direct marketing (for example, by agreeing to direct marketing by text message or email – and also specific to the value-added service for traffic data).

This means general consent for marketing or even consent for live calls won't be specific enough for automated calls. The organisation wanting to do the marketing must be named, and the consent involve some form of very clear positive action indicating agreement.

Pre-ticked opt-in boxes are banned under the UK GDPR. Just because someone fails to opt-out of direct marketing - for example, unchecking a pre-ticked box - means it wouldn't be considered valid consent.

Automated marketing calls

An automated direct marketing call plays a recorded message and there is no human involvement. They enable organisations to send lots of messages at a minimal cost, and strict rules apply to these because there's no chance for interaction with the caller and they are instructive and impersonal. **Organisations** need consent to make an automated marketing call – this applies to corporate or individual subscribers, and they must:

- say who is calling (for example, the organisation's name);
- allow its number (or an alternative contact number) to be displayed to the party receiving the call; and
- provide their contact details or a Freephone number.

For example:

- an organisation was prosecuted for instigating almost 100 million unsolicited automated marketing calls
- these were mostly related to road traffic accidents and PPI compensation
- the ICO issued a large civil monetary penalty
- the Director was struck off and banned from being a director for six years

The preference services

Registration with the Telephone Preference Service (TPS) or Corporate Telephone Preference Service (CTPS) acts as a general opt-out of receiving any live marketing calls. It's free to register. Registration for the TPS never expires, but CTPS registration expires after a year if not renewed. These statutory services are intended to allow subscribers to say they don't want calls or marketing over the telephone. They are run by the DMA (the Data and Marketing Association) under contract to the ICO.

PECR itself makes no distinction between these services.

The TPS:

- registers subscribers;
- handles the majority of complaints about marketing calls and faxes;
- maintains the register of numbers and sells access to organisations who need to screen; and

- works closely with the ICO.

An organisation must check numbers against these lists before making live calls. The services don't apply to automated calls because organisations must have consent for those. We receive complaints from both the TPS and the ICO Online Reporting Tool (OLRT). We have a dedicated team which considers these complaints.

PECR also covers the Fax Preference Service which is statutory and intended for corporate subscribers – although faxes aren't really used much any more.

There is also the Mailing Preference Service which applies to postal marketing and is not statutory and not covered by PECR.

Electronic mail

PECR defines what's meant by electronic mail, and it includes:

- email;
- SMS;
- picture & video messages;
- voicemail & answerphone;
- messaging apps, for example, WhatsApp and Snapchat;
- direct messages on social networks, for example, Twitter and Facebook;
- (in some cases) smartphone notifications - where the notification is 'pushed' over the network as opposed to generated by the app itself on the phone.

If the technology relies on broadcasting messages without a specific individual as the target, it doesn't fall under PECR. This also applies to Bluetooth when it's used in this way.

An organisation must have the individual subscriber's consent to send direct marketing by electronic mail, unless the so-called 'soft opt-in' exception applies.

All organisations sending marketing via email must identify themselves and provide a valid address for opt-out. An organisation can email or text any corporate body but an individual can object to direct marketing under Article 21 of the UK GDPR (which gives individuals the right to prevent processing of personal data for the purposes of direct marketing).

This also applies if a marketing email is sent to an individual within a corporate subscribers organisation, for example *joebloggs@abc.co.uk*.

That individual might exercise their Article 21 right to object, even if the subscriber (the person paying the telecoms bill) is a company rather than an individual.

The soft opt-in

The only circumstances in which an organisation can send electronic mail marketing to an individual without prior consent is where the 'soft opt in' applies. This term isn't in the legislation and only applies to electronic mail.

The 'soft opt-in' isn't a way of getting consent – instead, it's a limited situation in which consent isn't necessary. In these circumstances, the UK GDPR lawful basis is legitimate interests.

The 'soft opt-in' applies when the organisation itself obtained the contact details in the course of a sale or negotiations for a sale. It must have obtained them directly from the individual. Just 'browsing' online does **not** qualify as negotiations for a sale, but completing an online enquiry form asking for more details about a specific product would qualify.

Charities and political parties are unlikely to be able to rely on the 'soft opt-in' because it doesn't apply to non-commercial promotions and its unlikely that the details will have been obtained in the course of a sale or negotiations for a sale.

For the 'soft opt-in' to apply, the marketing must be for the organisations own similar products or services.

Individual expectation is key and it will depend on the way an organisation or brand is viewed. For example, individuals doing a weekly food shop online from a large supermarket might reasonably expect further emails about other groceries and other products such as books or DVDs. However, they are unlikely to expect emails about banking or insurance products sold under the supermarket brand. These products are not bought and sold in a similar context.

For the 'soft opt-in' to apply the organisation must also have provided a clear, simple and easy way to opt out at the time the details are collected, and must also provide an opt–out in each subsequent communication – again this must be simple like an unsubscribe link or replying to a text message with STOP.

An example of the soft opt-in:

- an individual provides their details for a car insurance quote using an insurance company's website. The details have been obtained in the course of a sale or negotiations for a sale
- the company explains with the quote that it wants to send marketing emails, and provides an 'opt out' box that people can tick
- ten months later, the insurance company sends an email with a price for the next year's insurance, but only to those individuals who did not opt out of marketing
- the email contains a link to unsubscribe from future marketing
- the company is marketing its own similar products and has provided another opt-out

PECR powers

The ICO has the power under PECR to issue enforcement notices and information notices, and is also able to require a Communication Service Provider (CSP) to provide us with the identity of the subscriber suspected of making unsolicited calls.

Breaking an enforcement notice is an offence and can lead to large fine in a court. We can also impose Civil Monetary Penalties (CMP) under PECR of up to £500,000.

The criteria for a CMP is serious contravention by a person that is either:

- deliberate; or
- where the person knew or ought to have known there was a real risk of the contravention occurring but failed to take reasonable steps to prevent it.

We can also:

- issue undertakings which commit an organisation to a particular course of action in order to improve compliance;
- conduct an audit to check a service provider is complying with its security obligations and make recommendations;
- impose fixed penalty fines of £1,000 - for example, on a service provider who fails to notify us of a personal data breach within 24 hours; and
- apply to Court for an order under section 213 of Enterprise Act 2002 requiring a person to cease conduct harmful to consumers.

Not covered under PECR

PECR doesn't cover the following:

- **Silent calls** - when a marketing company is using automatic diallers to call more telephone numbers than they have call handlers. There's no content so there's no marketing, and this is dealt with by Ofcom.

- **Debt collection messages** - the purpose of these messages is to collect money, not to market anything.

- **Scams** - complaints about scams usually relate to the validity of an underlying offer and should be referred to the Competition and Markets Authority. PECR only covers the nature of the message (ie whether it falls under marketing) and not the content.

- **Spam messages** – spam messages were originally used to mean emails sent to automatically generated email addresses that may or may not exist. These don't qualify as direct marketing because they are not "directed at individuals". The term is sometimes used more widely to cover nuisance emails or texts of any kind which may include direct marketing emails.

- **Service messages** - such as a message about a change to terms and conditions, or a problem with an individual's account, do not fall under PECR, as long as there is no element of marketing.

- **Marketing messages from overseas**.

Further reading

Start by looking at the Guide to PECR that's been published on our website, especially the section on key concepts and definitions.

You should then have a look at the action we've taken to enforce PECR over the last quarter, and look at the guide to ICO PECR audits. Both of these will give you a good sense of how we as an office approach PECR.

After this, you should familiarise yourself with the direct marketing checklist.

You should look through the guidance for the use of personal data in political campaigns, paying particular attention to the section on political campaigning and direct marketing.

You should also read the 'Your data matters' page on the same topic.

Then take a look at our published guidance on cookies and similar technologies and familiarise yourself with the relevant sections and topics that have been covered in these notes.

You should then return to the guidance that we've published for indidivuals, and read through or watch the videos on:

- individual's rights to object to the use of their data,
- spam texts,
- spam emails, and
- nuisance calls.

Back to top

KNOWLEDGE SERVICES
UPDATED: 29 APRIL 2022