Privacy and Electronic Communications Regulations

Direct marketing

Information Commissioner's Office

Direct marketing

Data Protection Act
Privacy and Electronic Communications Regulations

Contents

Direct marketing
20160519
Version: 2.2

Introduction

This guidance has been updated to include 'GDPR update' boxes. These updates signpost key differences in the new data protection regime that will affect those wanting to conduct direct marketing from 25 May 2018 onwards, and link to new sources of relevant GDPR guidance.

We will be consulting on a Direct Marketing Code of Practice in due course to replace and update this guidance in more detail.

For more information on the GDPR, see our Guide to the GDPR.

1. The Data Protection Act 1998 (the DPA) is based around eight principles of good information handling. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

2. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) provide rules about sending marketing and advertising by electronic means, such as by telephone, fax, email, text and picture or video message, or by using an automated calling system. PECR also include other rules relating to cookies, telephone directories, traffic data, location data and security breaches.

3. An overview of the main provisions of the DPA and PECR can be found in The Guide to Data Protection and The Guide to the Privacy and Electronic Communications Regulations.

4. This is part of a series of guidance, which goes into more detail than the Guides, to help organisations to fully understand their obligations and to promote good practice.

5. This guidance explains the DPA and PECR rules on direct marketing – with a focus on calls and texts to individuals – and how this affects lead generation and the use of marketing lists. It will help responsible organisations to keep within the law and maintain a good reputation with customers, and sets out what enforcement action the ICO can take against those who ignore the rules.

6. This guidance can be read end-to-end for a full discussion of the issues, but it does not have to be used in that way. It has been designed so that organisations can dip in and out as necessary, using the links in the contents page to go directly to particular issues of concern. The text of each section will provide further links to other relevant parts of the guidance.

7. The guidance starts with a broad overview of the law, then contains separate sections on what counts as direct marketing, what counts as consent, the specific rules on calls and texts, and the use of marketing lists. We have also published a separate direct marketing checklist (pdf) to help organisations comply with the law and good practice.

Overview

GDPR Update

- A definition of direct marketing is contained within the DP Bill and is likely to be similar to the definition in the Data Protection Act 1998 (the 1998 Act).
- The GDPR definition of consent is similar to the 1998 Act, but is clearer that consent must be unambiguous and involve an affirmative action. There is also more detail on the level of detail and control individuals must have.
- An unambiguous affirmative action requires a positive opt-in. Don't use pre-ticked boxes or any other method of consent by default.
- Any third party controllers who will rely on the consent must be named – listing categories of organisation will not give valid third party consent.
- The GDPR contains substantial fines for failing to comply with its requirements including fines of up to €20 million, or 4% of your total worldwide annual turnover, whichever is higher.

- Direct marketing covers the promotion of aims and ideals as well as the sale of products and services. This means that the rules will cover not only commercial organisations but also not-for-profit organisations (eg charities, political parties etc).
- In many cases organisations will need consent to send people marketing, or to pass their details on. Organisations will need to be able to demonstrate that consent was knowingly and freely given, clear and specific, and should keep clear records of consent. The ICO recommends that opt-in boxes are used.
- The rules on calls, texts and emails are stricter than those on mail marketing, and consent must be more specific. Organisations should not take a one-size-fits-all approach.
- Organisations can make live marketing calls to numbers not registered with the TPS, if it is fair to do so. But they must not call any number on the TPS list without specific prior consent.

- Organisations must not make any automated pre-recorded marketing calls without specific prior consent.
- Organisations making marketing calls must allow their number (or an alternative contact number) to be displayed to the person receiving the call.
- Organisations must not send marketing texts or emails to individuals without their specific prior consent. There is a limited exception for previous customers, known as the soft opt-in.
- Organisations must stop sending marketing messages to any person who objects or opts out of receiving them.
- Organisations must carry out rigorous checks before relying on indirect consent (ie consent originally given to a third party). Indirect consent is highly unlikely to be valid for calls, texts or emails.
- Neither the DPA nor PECR ban the use of marketing lists, but organisations must take steps to ensure a list was compiled fairly and accurately reflects peoples' wishes. Bought-in call lists should be screened against the TPS. It will be very difficult to use bought-in lists for text, email, or automated call campaigns as these require very specific consent (either where the specific organisation is named or it is within a precisely defined category of organisation).
- The ICO will consider using its enforcement powers, including the power to issue a fine of up to £500,000, where an organisation persistently ignores individuals' objections to marketing or otherwise fails to comply with the law.
- Our direct marketing checklist can help organisations to comply.

Legal framework

8. The DPA and PECR both restrict the way organisations can carry out unsolicited direct marketing (that is, direct marketing that has not specifically been asked for).

9. This guidance focuses primarily on these DPA and PECR rules on direct marketing. However, direct marketing can engage a wide range of other regulatory and conduct issues.

Organisations should ensure they are also familiar with other relevant laws and industry codes of practice. See the section below on other regulation for more information.

Data Protection Act

GDPR Update

The 1998 Act will be superseded by the new Data Protection Act 2018 (as supplemented by the GDPR) on 25 May 2018. See our Guide to the GDPR for further information.

10. If direct marketing involves the processing of personal data (in simple terms, if the organisation knows the name of the person it is contacting), it must comply with the principles set out in the DPA. The most relevant principles here are:

    - The first principle: organisations must process personal data fairly and lawfully. In particular, they will usually need to tell the individuals concerned who they are and that they plan to use those details for marketing purposes - see the Privacy notices code of practice for more guidance on this area. Organisations will also need to tell people if they plan to pass those details on to anyone else, including selling or sharing the data for marketing purposes, and are likely to need their consent to do so. Organisations must not do anything that people would not reasonably expect or which would cause them unjustified harm.

    - The second principle: organisations must only collect personal data for specified purposes, and cannot later decide to use it for other 'incompatible' purposes. So they cannot use people's details for marketing purposes if they originally collected them for an entirely different purpose.

    - The fourth principle: organisations must ensure that personal data is accurate and, where necessary, kept up to date. So a marketing list which is out of date, or which does not accurately record people's marketing preferences, could breach the DPA.

11. Section 11 of the DPA also gives individuals the right to prevent their personal data being processed for direct marketing. An individual can, at any time, give written notice to stop (or not to begin) using their details for direct marketing. In other

words, organisations must stop any marketing directed at a particular individual if that person writes and asks them to stop. The organisation does not have to reply, but it is good practice to acknowledge the request and confirm that the marketing will stop.

12. The organisation must stop marketing within a reasonable period. The DPA does not say it has to stop immediately. For example, if a particular mass marketing campaign is already underway, it might be difficult to prevent one individual from receiving any further materials. However, in most circumstances we expect that calls, texts or other electronic communications should stop within 28 days of receiving the objection, and postal communications should stop within two months. And if the organisation can reasonably stop sooner, it must.

13. Organisations will not always need to process personal data to carry out a direct marketing exercise. For example, if they dial telephone numbers at random and don't know whose numbers they are, the DPA will not apply. However, they must always still comply with the rules set out in PECR.

Privacy and Electronic Communications Regulations

GDPR Update

The EU is in the process of replacing the ePrivacy Directive (and therefore PECR) with a new ePrivacy Regulation (ePR).

The new ePR will not be agreed by the EU before the GDPR comes into effect on 25 May 2018. The existing PECR rules will continue to apply until the ePR is finalised and comes into effect, but with some changes to account for the GDPR.

In particular, existing PECR rules will apply using the new GDPR definition of consent.

The relationship between PECR and the GDPR is slightly different to that between PECR and the 1998 Act, but this does not affect the marketing rules and organisations must continue to comply with both regimes.

14. PECR were designed to complement the DPA, and set out more detailed privacy rules in relation to the developing area of

electronic communications. However, organisations must also still comply with the DPA if they are processing personal data. Regulation 4 of PECR specifically states:

> *"Nothing in these Regulations shall relieve a person of his obligations under the Data Protection Act 1998 in relation to the processing of personal data."*

15. There is some overlap with the DPA, and they use some of the same concepts and definitions – including the definition of direct marketing.

16. If an organisation is sending unsolicited direct marketing by electronic means, or employing someone else to do so on its behalf, it must comply with PECR. This includes telephone calls (both live and automated), faxes, emails, text messages and other forms of electronic message.

17. PECR are broader than the DPA in the sense that they apply even if the organisation is not processing any personal data – which means they apply even if the organisation does not know the name of the person it is contacting. Some of the rules also apply to business-to-business marketing, as well as marketing to consumers.

18. Organisations must also comply with PECR if they are making calls or sending texts or emails to generate marketing leads, even if that initial message does not include any sales or promotional material. Any calls, texts or emails made for direct marketing purposes are covered.

19. Different rules apply to different types of communication, and also vary depending on whether the marketing is sent to an individual or a company.

20. In very broad terms, an organisation cannot make unsolicited marketing calls to numbers which are registered on the Telephone Preference Service (TPS), or to anyone who has told it that they don't want to receive its calls – see the section below on marketing calls for more detail. And an organisation cannot send texts or emails to individuals without their specific consent – see the section below on marketing texts and emails.

21. An organisation must always say who it is. It also has to provide contact details, so that an individual can make contact

if they want to opt out of the marketing. Organisations making marketing calls must allow their number (or an alternative contact number) to be displayed to the person receiving the call.

Other regulation

22. The ICO regulates the DPA and PECR, but there are also a number of other rules and industry codes of practice affecting marketing, which are regulated by other bodies. Some of the key areas of other regulation are set out here – but this is not intended to be an exhaustive list, and organisations should always ensure that they are familiar with all laws and standards of conduct which apply to them.

23. Ofcom regulates the Communications Act 2003, which covers the improper use of a public electronic communications network, including making silent or abandoned calls. Ofcom has powers to issue fines up to £2 million for persistent misuse. More information is available in Ofcom's October 2010 statement on Tackling abandoned and silent calls.

24. The Direct Marketing Association (DMA) publishes the Direct Marketing Code of Practice, setting standards of ethical conduct and best practice in direct marketing. Compliance is mandatory for all DMA members, but we encourage all those involved in direct marketing, whether DMA members or not, to comply with the code in order to ensure the highest possible standards of ethical conduct and to promote consumer confidence. The code is enforced by the independent Direct Marketing Commission (DMC). More information is available on the DMC website.

25. The UK Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing (the CAP code) contains rules which all advertisers, agencies and media must follow. It covers the content of advertising material, and specific rules on certain types of advertising (eg advertising to children, advertising certain types of products, or distance selling). The CAP code is enforced by the Advertising Standards Authority (ASA), who can take steps to remove or amend any ads that breach the rules, and have a number of sanctions at their disposal. More information is available on the ASA website.

26. The Consumer Protection from Unfair Trading Regulations 2008 prohibit a number of unfair, misleading or aggressive

marketing practices, including "*making persistent and unwanted solicitations by telephone, fax, email or other remote media*". Some breaches of the regulations are a criminal offence. The regulations are currently enforced by local trading standards offices and the Office of Fair Trade (OFT). More information is available on the OFT website and the gov.uk website. Note that the OFT will be replaced by the Competition and Markets Authority (CMA) from April 2014.

27. Claims management companies – that is, any business which handles compensation claims for customers, including claims for personal injury or mis-sold financial products (such as payment protection insurance or PPI) – are authorised and regulated by the Ministry of Justice Claims Management Regulator (CMR) under the Compensation Act 2006, and must comply with the Conduct of Authorised Persons Rules 2013. Claims management companies involved in non-compliant marketing or lead generation may be subject to CMR enforcement action, including having their licence revoked. More information and a copy of the CMR enforcement policy is available on the CMR website.

ICO enforcement

GDPR Update

The GDPR contains substantial fines for failing to comply with its requirements, including fines of up to €20 million, or 4% of your total worldwide annual turnover, whichever is higher.

PECR penalties are likely to remain the same.

28. The ICO has received a large number of complaints about unwanted marketing calls and texts. Our focus is on reducing the number of complaints by taking systematic enforcement action, starting with the organisations that generate the most complaints.

29. The ICO can take enforcement action wherever the law relating to direct marketing is not being complied with. Any breach of the DPA or PECR could result in an Enforcement Notice, requiring you to take action to remedy the breach. Failure to comply is a criminal offence.

30. The ICO can also impose civil monetary penalties (fines) of up to £500,000 for a serious breach. We are most likely to take such action where an organisation persistently ignores people's objections to marketing calls or texts, sends mass texts without consent, or fails to screen its call list against the TPS.

Example
The ICO has issued monetary penalty notices under PECR against a range of organisations. For example;

Making repeated live marketing calls to numbers listed on the TPS without prior consent, and ignoring people's objections to those calls:

- Telecom Protection Service Ltd - £80,000
- Nuisance Call Blocker Ltd - £90,000

Making automated marketing calls without consent:

- Home Energy and Lifestyle Management Ltd - £200,000
- Direct Security Marketing Ltd - £70,000

Sending marketing emails without consent:

- Telegraph Media Group Ltd - £30,000

Sending marketing text messages without consent;

- Parklife Manchester Ltd - £70,000

31. We will also consider enforcement action under the DPA against organisations who sell marketing lists without people's knowledge or consent. Obtaining and selling people's details without clear consent is likely to breach the first data protection principle, which requires personal data to be obtained and disclosed fairly and lawfully, and is also likely to lead to further direct marketing in breach of the DPA and PECR.

Example
An online pharmacy, Pharmacy 2U, offered its customers' names and addresses for sale through an online marketing list company. However Pharmacy 2U had not informed its customers that it intended to sell their details, and the customers had not given their consent for their personal data to be sold on.

The ICO found the company to have breached the first

principle of the DPA regarding fair and lawful processing of personal data and issued it with a monetary penalty notice of £130,000.

32. More information about our enforcement powers and policies and current enforcement activity is available on our website. We will take targeted, risk-driven action in line with our:

- Data Protection Regulatory Action Policy
- Statement on enforcing the revised Privacy and Electronic Communications Regulations
- Guidance about the issue of monetary penalties.

Direct marketing

The definition of direct marketing

GDPR Update

The GDPR doesn't define 'direct marketing'. However the DP Bill which is currently being debated contains a definition of direct marketing which is very similar to the 1998 Act definition – this is however subject to change until the Bill is made into law.

33. Section 11(3) of the DPA defines "direct marketing" as:

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

34. This definition also applies for PECR, as regulation 2(2) of PECR provides that any undefined expressions have the same meaning as in the DPA.

35. This definition covers **any** advertising or marketing material, not just commercial marketing. All promotional material falls within this definition, including material promoting the aims of not-for-profit organisations. See the section below on Charities, political parties and other not-for-profit organisations for more

on this point. It will also cover any messages which include some marketing elements, even if that is not their main purpose.

> **Example**
> A bank makes a telephone call to a customer about the administration of their bank account. However during the call the bank also outlines its mortgage products. Although the main purpose of the call is for administration because the call is also being used to promote other products and services it still falls within the definition of direct marketing.

36. The definition also covers any means of communication (although PECR rules only apply to electronic communication). It is not limited to traditional forms of marketing such as telesales or mailshots, and can extend to online marketing, social networking or other emerging channels of communication. Although the focus of this guidance is on marketing calls, emails and texts, remember that the DPA can apply to any type of direct marketing.

37. The key element of the definition is that the material must be directed to particular individuals. Indiscriminate blanket marketing – for example, leaflets delivered to every house in an area, magazine inserts, or adverts shown to every person who views a website – will not therefore fall within this definition of direct marketing.

Market research and 'sugging'

38. The direct marketing rules will not apply if an organisation contacts customers to conduct genuine market research (for example the purpose is to use market research to make decisions for commercial or public policy) or contracts a research firm to do so, as this will not involve the communication of advertising or marketing material. However, organisations conducting market research will still need to comply with other provisions of the DPA, and in particular ensure they process any individually identifiable research data fairly, securely and only for research purposes.

39. However, an organisation cannot avoid the direct marketing rules by labelling its message as a survey or market research if it is actually trying to sell goods or services, or to collect data

to help it (or others) to contact people for marketing purposes at a later date. This is sometimes referred to as 'sugging' (selling under the guise of research). If the call or message includes any promotional material, or collects data to use in future marketing exercises, the call or message will be for direct marketing purposes. The organisation must say so, and comply with the DPA and PECR direct marketing rules.

40. If an organisation claims it is simply conducting a survey when its real purpose (or one of its purposes) is to sell goods or services, generate leads, or collect data for marketing purposes, it will be breaching the DPA when it processes the data. It might also be in breach of PECR if it has called a number registered with the TPS, sent a text or email without consent, or instigated someone else to do so.

41. Organisations must not ask market research firms they employ to:

    - promote their products (this will include asking the research firm to use the organisation's goods/services as a way to incentivise participation); or
    - give them the research data for future sales or marketing purposes

    unless the individuals contacted agree to this and all communications comply with PECR (eg calls are screened against the TPS register).

42. If during a genuine market research project an organisation discovers errors in its customer database, we consider it can use the research data to correct these errors without breaching the DPA or PECR. This is consistent with the obligation under the fourth principle to ensure personal data is accurate and up to date. However, organisations should not deliberately use market research as a method of keeping their customer database updated.

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

Charities, political parties and other not-for-profit organisations

GDPR Update

The GDPR rules also apply to charities, political parties and not-for-profit organisations. You will need to ensure that your processing for marketing or fundraising purposes is compliant with the GDPR by 25 May 2018.

See our Guide to the GDPR for further information.

44. Direct marketing is not limited to advertising goods or services for sale. It also includes promoting an organisation's aims and ideals. This means that the direct marketing rules in the DPA and PECR will apply to the promotional, campaigning and fundraising activities of not-for-profit organisations. For example, a charity or political party contacting particular individuals to appeal for funds or votes, or contacting supporters to encourage them to write to their MP or attend a public meeting or rally, would be covered by the direct marketing rules.

45. Not-for-profit organisations are not exempt from either the DPA or PECR and therefore will need to ensure that their activities comply with the law.

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

The case went to the Information Tribunal. In *Scottish National Party v Information Commissioner (EA/2005/0021, 15 May 2006)*, the tribunal confirmed that the direct marketing rules in PECR and the DPA covered the promotional activities of both commercial and not-for-profit organisations, and so political parties had to comply with PECR when carrying out campaigning calls.

46. Not-for-profit organisations need to be aware that the definition of direct marketing will cover any messages that contain marketing elements even if this is not the main purpose of the message.

Example
A charity makes an administrative telephone call to an individual who has set up direct debit donations with a high street fundraiser as they wish to confirm the individual's bank details. If the call simply confirms the details then it will not be covered by the direct marketing rules.

However if the charity uses this administrative call to suggest that the individual increases their donation or provides any other information promoting the charity's work then this will mean that the call ceases to be purely administrative and the direct marketing rules will apply.

47. Not-for-profit organisations must ensure that they screen against the Telephone Preference Service (TPS) when undertaking telephone campaigns – this is the same as any organisation wishing to conduct live marketing telephone calls.

48. Live marketing calls can only be made to numbers registered on the TPS where the subscriber (ie the person who gets the telephone bill) has specifically consented to receiving the marketing calls from that organisation. PECR does not contain an exemption for existing supporters who are registered on TPS. Therefore in order to avoid breaching PECR, not-for-profit organisations will need to ensure that any existing supporters who are registered with the TPS have specifically consented to receiving marketing calls from that organisation. Please see the section on Marketing calls for further information.

49. Not-for-profit organisations need to ensure that they clearly and prominently explain to supporters what their details will be used for and obtain clear, specific consent for electronic marketing. See the section on Consent for more information.

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

50. Not-for-profit organisations should take particular care when communicating by text or email. This is because the 'soft opt-in' exception only applies to commercial marketing of products or services. Not-for-profit organisations might be able to use the soft opt-in for any commercial products or services they offer. But they will not be able to send campaigning texts or emails without specific consent, even to existing supporters.

51. See the section below for more information on marketing texts and emails and the soft opt-in.

52. Not-for-profit organisations that wish to share/sell their marketing lists with other organisations must ensure that their supporters were made aware of this when the personal details were collected and that specific consent to pass on the details was obtained. Consent cannot be inferred from supporters just because a marketing list is to be shared with or sold to an organisation which has similar aims/objectives to the originating organisation – such an assumption does not override these requirements. Please refer to the section on selling a marketing list for more information.

53. Although this guidance is relevant to any organisation sending direct marketing material, further advice specifically aimed at political parties is also available in our Guidance for political parties for campaigning or promotional purposes.

Solicited and unsolicited marketing

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

Example
A customer submits an online form requesting a double glazing quote. Sending this quote to the customer is solicited marketing, but any further contact from the company would be unsolicited.

55. If the marketing has not been specifically requested, it will be unsolicited and the PECR rules apply. This is true even if the customer has 'opted in' to receiving marketing from that organisation.

Example
When he requested the quote, the customer also ticked a box opting in to receiving information about future home improvement offers. A few months later, the company sends an email with details of a new offer. This is unsolicited marketing, because the customer did not contact the company to specifically request information about that particular offer.

56. An opt-in means that the customer is happy to receive further marketing in future, and is likely to mean the unsolicited marketing is lawful (see the next section on consent). But it is still unsolicited marketing, which means the PECR rules apply.

Consent

57. Consent is central to the rules on direct marketing. Organisations will generally need an individual's consent before they can send marketing texts, emails or faxes, make calls to a number registered with the TPS, or make any automated marketing calls under PECR. They will also usually need consent to pass customer details on to another organisation under the first data protection principle. If they cannot demonstrate that they had valid consent, they may be subject to enforcement action.

58. To be valid, consent must be knowingly and freely given, clear and specific. Organisations should keep clear records of what an individual has consented to, and when and how this consent was obtained, so that they can demonstrate compliance in the event of a complaint.

The definition of consent

GDPR Update

The definition of consent has been updated. Whilst the key elements of the consent definition remain (freely given, specific, informed, and there must be an indication signifying agreement), the GDPR is clearer that the indication must be unambiguous and involve a clear affirmative action.

There are also several other new provisions on consent - for example specific provisions on keeping records of consent, clarity and prominence of consent requests, the right to withdraw consent, and avoiding making consent a condition of a contract.

See our GDPR consent guidance for full details.

59. Consent is defined in European Directive 95/46/EC (the data protection directive on which the DPA is based) as:

> *"any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".*

60. The key points are that for consent to be valid, it must be:

- *freely given* – the individual must have a genuine choice over whether or not to consent to marketing. Organisations should not coerce or unduly incentivise people to consent, or penalise anyone who refuses. Where consent to marketing is a condition of subscribing to a service, the organisation will have to demonstrate how this indicates that consent was freely given (see paragraph 66 below).

- *specific* – in the context of direct marketing, consent must be specific to the type of marketing communication in question (eg automated call or text message) and the organisation sending it. This is discussed further below.

Example
The Universities and Colleges Admissions Service (UCAS) used an application form that only allowed applicants to opt-out of

receiving marketing from commercial companies if they un-ticked three boxes covering marketing emails, post and text messages. The wording of the opt-out also meant that unticking the boxes would result in the applicant not receiving information about career opportunities and education providers or health information.

The Commissioner ruled that this approach meant applicants felt obliged to let UCAS use their information for commercial purposes otherwise they'd potentially miss out on important information about their career or education. Therefore it breached the requirement under the DPA that personal data be processed fairly and PECR which require consent to be freely given and for a specific purpose. The ICO therefore required UCAS to change its practices.

- *informed* – the person must understand what they are consenting to. Organisations must make sure they clearly and prominently explain exactly what the person is agreeing to, if this is not obvious. Including information in a dense privacy policy or hidden in 'small print' which is hard to find, difficult to understand, or rarely read will not be enough to establish informed consent. This links to the fairness requirements found in the first data protection principle of the DPA. Further information on privacy notices is available in the Privacy Notices Code of Practice.

Example
A company makes a marketing call to an individual. During the call the individual is asked if they would be happy to be contacted by third parties for marketing purposes. The individual agrees and is then played an automated message in which a computerised voice rapidly lists company names which are incredibly difficult to understand.

This will not constitute informed consent. Firstly the individual has been asked to agree to third party marketing prior to being informed who the third party organisations actually are. Secondly the compressed audio file played to the individual is virtually unintelligible. Therefore even if it was played before agreement was sought this would not constitute informed consent as the list was given far too fast for anyone to pick out the company names.

- *an indication signifying agreement* – consent must be a positive expression of choice. It does not necessarily have to be a proactive declaration of consent – for example, consent might sometimes be given by submitting an online form, if there was a clear and prominent statement that this would be taken as agreement and there was the option to opt out. But organisations cannot assume consent from a failure to opt out unless this is part of a positive step such as signing up to a service or completing a transaction. For example, they cannot assume consent from non-response to an email, as this would not be a positive indication of agreement.

Example
A company decides that it wants to use its customer database to market individuals. The customers have not previously consented to receiving marketing messages so the company sends a letter to customers stating that it intends to send them details of special offers by post and email. The letter provides a number for customers to call if they don't want to receive marketing.

Non response does not constitute valid consent for marketing. Failure to call the number to opt-out will not satisfy the requirement that individuals provide an indication signifying agreement. The company will not therefore be able to market its customers on this basis.

61. This basic definition of consent also applies for PECR. Regulation 2(3) incorporates definitions from European Directive 2002/58/EC (the e-privacy directive on which PECR are based), and the directive states that *"consent by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC"*.

62. However, the wording of each of the regulations in PECR requiring consent for electronic marketing calls or messages go further, and also require that:

> *"the [recipient] has previously notified the [caller or sender] that he consents for the time being to such communications being sent by, or at the instigation of, the [caller or sender]".*

63. In our view, this means that consent for electronic marketing messages is more tightly defined than in other contexts, and must be extremely clear and specific. In particular:

- *the recipient has notified the sender* – the person must notify consent to the organisation actually sending the marketing. An organisation must therefore be very careful when relying on indirect (third party) consent which was originally given to another organisation. The person must have intended for their consent to be passed on to the organisation doing the marketing. See the section below on Indirect (third party) consent for more information.

- *consents for the time being* – the context must indicate that consent is ongoing. Consent for a one-off message, or consent that is clearly only intended to cover a short period of time or a particular context, will not count as ongoing consent for all future marketing messages. We also consider that consent 'for the time being' implies that consent lasts as long as circumstances remain the same, and will expire if there is a significant change in circumstances. See the section below on Time limits for more information.

- *to such communications* – the person must specifically consent to the type of communication in question. In other words, organisations cannot make an automated call unless the person has consented to receiving automated calls, cannot send a text unless they have consented to receive texts, and so on. Consent to receive phone calls cannot be

extended to cover texts or emails, and vice versa. And a general statement of consent to receive marketing might be valid for mail marketing, but will not cover calls or texts.

- *being sent by the sender* – the person must specifically consent to messages from the particular sender of the message. Again, this means organisations need to be very careful if relying on consent originally given to a third party. See the section below on Indirect (third party) consent for more information.

Implied consent

GDPR Update

The GDPR requires that consent is given 'by a statement or by a clear affirmative action'. The idea of an affirmative act does still leave room for 'implied' consent in some circumstances, particularly in more informal offline situations. The key issue is that there must be a positive action that makes it clear someone is agreeing to the use of their information for a specific and obvious purpose. However, this type of 'implied' consent would not extend beyond what was obvious and necessary.

The GDPR is also clear that consent should not be bundled up as a condition of service unless it is necessary for that service.

See our GDPR consent guidance for further details.

Currently, the 1998 Act allows you to make transparency information 'readily available', but under the GDPR you must actively provide people with the information in a way that is easy for them to access. Putting a notice on your website without letting people know it's there will not be good enough. See our guidance on the right to be informed for further details.

64. Neither the DPA nor PECR say that consent for marketing must be explicit, however it is good practice to have explicit consent. Implied consent can also be valid consent in some situations – in other words, if it is reasonable from the context to conclude that the person consents to marketing, even if they have not said so in as many words.

65. However, organisations cannot rely on 'implied consent' as a euphemism for ignoring the need for consent, or assuming everyone consents unless they complain. Even implied consent must still be freely given, specific and informed, and must still involve a positive action indicating agreement (eg clicking on a button, or subscribing to a service). The person must have understood that they were consenting, and exactly what they were consenting to, and must have had a genuine choice –if a condition of subscribing to a service is giving consent to marketing, the organisation will have to demonstrate how this indicates that consent was freely given.

66. The ICO recommends that organisations do not make consent to marketing a condition of subscribing to a service unless they can clearly demonstrate how consent to marketing is necessary for the service and why consent cannot be sought separately. It is also relevant to consider whether there is a choice of other services and how fair it is to couple consent to marketing with subscribing to the service. It will also be important to assess whether this approach creates an imbalance between the individual and organisation (see the UCAS example above).

67. In some other contexts, the intended use of personal data is so obvious that the act of providing the data in the first place is enough to indicate consent – eg providing a postal address when completing an online transaction clearly indicates consent to use that address to deliver the goods. It might be clear that the use of data is a necessary part of a service or activity – eg if a website displays a clear banner saying that using the site will result in cookies being set, then clicking through the pages is likely to indicate implied consent to the use of those cookies, as long as sufficient information is made available to fully inform users.

68. However, direct marketing is highly unlikely to form an obvious or integral part of another service or activity in the same way. It will be difficult to show that a customer understood they were agreeing to receive marketing messages unless there was a very clear statement explaining that their action would be taken that way, and a free choice whether or not to consent.

69. It is not enough for implied consent if such a statement is only provided as part of a privacy policy or notice which is hard to find, difficult to understand, lengthy, or rarely read. The customer will be unaware of what they are agreeing to, which means they are not informed and there is no valid consent.

Organisations must ensure that clear and relevant information is readily available to their customers, explaining exactly what they are agreeing to and what choices they have. For more advice and guidance on how to write a good privacy notice, see the Privacy notices code of practice.

70. In short, implied consent in the context of direct marketing messages is not necessarily an easier option and is likely to require organisations to take similar steps to explicit consent. For example, if explicit consent can be obtained using an opt-in box, implied consent is still likely to require a prominent statement paired with an opt-out box. We therefore recommend that organisations use opt-in boxes in order to obtain explicit consent. (See below for more information on using opt-in and opt-out boxes.)

Methods of obtaining consent

71. The clearest way of obtaining consent is to invite the customer to tick an opt-in box confirming that they wish to receive marketing messages via specific channels (eg post, email, live phone call etc). This represents best practice and we would advise all organisations to adopt this approach, although it is not necessarily the only way of obtaining consent. Recital 17 of the e-privacy directive says:

> *"Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website".*

72. In our view, there must be some form of communication or positive action by which the individual clearly and knowingly indicates their agreement. This might involve clicking an icon, sending an email, subscribing to a service, or providing oral confirmation.

73. The crucial consideration is that the individual must fully understand that their action will be taken as consent, and must fully understand exactly what they are consenting to. There must be a clear and prominent statement explaining that the action indicates consent to receive marketing messages from that organisation (including what method of communication it will use). Text hidden in a dense privacy policy or in 'small

print' which is easy to miss would not be enough. Organisations should also provide a simple method of refusing consent (eg an opt-out box), to ensure that the consent is freely given.

74. Note that organisations cannot email or text an individual to ask for consent to future marketing messages. That email or text is in itself sent for the purposes of direct marketing, and so is subject to the same rules as other marketing texts and emails. And calls asking for consent are subject to the same rules as other marketing calls.

Opt-in and opt-out boxes

GDPR Update

Pre-ticked opt-in boxes are banned under the GDPR. You also cannot rely on silence, inactivity, default settings, or your general terms and conditions, or seek to take advantage of inertia, inattention or default bias in any other way. The GDPR does not specifically ban opt-out boxes but they are essentially the same as pre-ticked boxes and in our view are unlikely to comply. Both methods bundle up consent requests with other matters by default, and then rely on inactivity. Consent under the GDPR must be a positive indication and must be separate from other matters, so you are unlikely to be able to demonstrate consent using an opt-out box.

See our GDPR consent guidance for further information.

75. It is important to understand what opt-in and opt-out boxes mean (and don't mean), and how to use them effectively.

76. Opt-in boxes are boxes where a tick indicates that the person agrees to receiving the specified marketing. Best practice is to provide an unticked opt-in box, and invite the person to confirm their agreement by ticking. This is the safest way of demonstrating consent, as it requires a positive choice by the individual to give clear and explicit consent.

77. When using opt-in boxes, organisations should remember that to comply with PECR they should provide opt-in boxes to obtain specific consent for each type of electronic marketing they want to undertake (eg automated calls, faxes, texts or emails). Best practice would be to also provide similar opt-in boxes for marketing calls and mail.

Opt-in example (good practice)
"Tick if you would like to receive information about our products and any special offers by post ☐ / by email ☐ / by telephone ☐ / by text message ☐ / by recorded call ☐"

78. Some organisations provide pre-ticked opt-in boxes, and rely on the user to untick it if they don't want to consent. In effect, this is more like an opt-out box, as it assumes consent unless the user clicks the box. A pre-ticked box will not automatically be enough to demonstrate consent, as it will be harder to show that the presence of the tick represents a positive, informed choice by the user.

79. An opt-out box is a box that the user must tick to object or opt out of receiving marketing messages. However, the fact that someone has failed to object or opt out only means that they have not objected. It does not automatically mean that they have consented. For example, they may not even have seen the box if they were using a smartphone or other small screen device. For this reason, we would always advise the use of opt-in boxes instead.

80. Even so, in some circumstances, failure to tick an opt-out box (or untick an opt-in box) might be part of a wider mechanism of indicating consent. For example, if the user must take a positive action to submit a form (eg click a button), and the organisation provides a clear and prominent message along the following lines, the fact that a suitably prominent opt-out box has not been ticked might help to establish that clicking the button was a positive indication of consent:

Opt-out example
"By submitting this registration form, you indicate your consent to receiving email marketing messages from us. If you do not want to receive such messages, tick here: ☐"

81. Organisations should always ensure that the language used is clear, easy to understand, and not hidden away in a privacy policy or 'small print' – see our Privacy Notices code of practice for more advice on how to provide clear information to customers. Avoid legal phrases and confusing double negatives. Make sure it is easy to tell whether a box is an opt-

in or opt-out box, and use one consistent method - using a mixture of opt-in and opt-out boxes can be very confusing for customers and may mean informed consent is harder to demonstrate.

82. Use opt-in boxes wherever possible, but if using opt-out boxes (or pre-ticked opt-in boxes), make sure they are prominently placed and hard to miss.

Indirect (third party) consent

GDPR Update

Any third party controllers who will be relying on the consent must be named – precisely defined categories of third parties will not be acceptable under the GPDR definition.

You must keep records to demonstrate what the individual has consented to, including what they were told, and when and how they consented.

See our GDPR consent guidance for further details.

83. We use the term 'indirect consent' here to cover situations where a person tells one organisation that they consent to receiving marketing from other organisations. This is also sometimes known as 'third party consent' or 'third party opt-in'.

84. This will be relevant to any organisation using a bought-in marketing list. It will not have had any contact with those customers before, so they cannot have told the organisation directly that they consent to its marketing. But the list broker or other third party source might claim that the customers have consented to receiving marketing from other organisations.

85. Although there is a well-established trade in third party opt-in lists for traditional forms of marketing, organisations need to be aware that indirect consent will not be enough for texts, emails or automated calls. This is because the rules on electronic marketing are stricter, to reflect the more intrusive nature of electronic messages. PECR specifically requires that the customer has notified **the sender** that they consent to messages **from them**: see the definition of consent above. In

most circumstances, indirect consent would not meet this test – as the customer did not directly notify the sender, they notified someone else. Therefore it is best practice for an organisation to only send marketing texts and emails, or make automated calls to individuals, if it obtained consent directly from that person.

86. However, we do accept that indirect consent might be valid in some circumstances, if it is clear and specific enough. In essence, the customer must have anticipated that their details would be passed to the organisation in question, and that they were consenting to messages from that organisation. This will depend on what exactly they were told when consent was obtained.

87. Clearly, organisations cannot infer consent just because consent was given to a similar organisation, or an organisation in the same group. It must have extended to the organisation actually sending the message as well.

88. Indirect consent may therefore be valid if that organisation was specifically named. But if the consent was more general (eg marketing 'from selected third parties') this will not demonstrate valid consent to marketing calls, texts or emails.

89. However indirect consent could also be valid if the consent very clearly described precise and defined categories of organisations and the organisation wanting to use the consent clearly falls within that description. Consent is not likely to be valid where an individual is presented with a long, seemingly exhaustive list, of general categories of organisations. The names of the categories used must be tightly defined and understandable to individuals. In practice, this means that the categories of companies need to be sufficiently specific that individuals could reasonably foresee the types of companies that they would receive marketing from, how they would receive that marketing and what the marketing would be.

Example
A company's privacy policy contains the following information;

"We may use the personal information that you supply to us and work with other third party businesses to bring selected retail opportunities to you via direct mail, email and telemarketing. These businesses may include providers of direct marketing services and applications, including lookup

and reference, data enhancement, suppression and validation and email marketing."

This statement will not demonstrate valid consent for a third party to market an individual. It is not clear what these businesses actually are or what they do – these business types are likely to be meaningless to the majority of individuals. The categories are also very wide and potentially cover vast numbers of organisations.

90. It is extremely unlikely that a customer would intend to consent to unlimited future marketing calls or texts from anyone, anywhere. The question is what the customer would reasonably expect, given the context. Would they have anticipated that they were consenting to messages from that particular organisation? If the nature of the promotion is quite different from the context in which consent was originally obtained, consent is unlikely to be valid under PECR – even if it was superficially expressed to cover third parties.

91. Note also that consent does not last forever, and this time factor is even more important with indirect consent. Even if the customer did originally intend to notify their consent to some third parties at the time they gave it, they are unlikely to intend to keep notifying new third parties at a much later date. How long the intention to notify will last is likely to depend on the context. See the section below on time limits for more on this.

92. Organisations need to remember that consent for third party marketing is a one-step process. For example the customer gives consent to organisation A to pass their details onto organisation B. This original/same consent cannot be used by organisation B to pass the customer's details onto further organisations.

93. Organisations must therefore make rigorous checks as to how and when consent was obtained, by whom, and what the customer was told. It is not acceptable to rely on assurances of indirect consent without undertaking proper due diligence, in order to demonstrate consent if challenged. Organisations must ensure that consent was validly obtained, that it was reasonably recent, and that it clearly extended to them or organisations very closely fitting their description. If it was generic consent to marketing from any third party, it will be

very difficult to show specific enough consent for calls, texts or emails. And at the very least, any promotion (eg by mail) must be consistent with the context in which consent was given – for example, aimed at a similar market.

Example
A travel company asks customers to fill out a satisfaction survey during their trip. The survey includes a box to opt in to marketing messages from third parties. The customers' details are then passed down a chain of list brokers. Five years later, a company buys a list with these customers' details and wants to send messages promoting its home improvement products. Given how long ago the consent was obtained, and the fact that there is no link between the original travel product and the home improvement product, this will not constitute valid consent for marketing calls or texts from that home improvement company.

94. It is very important that organisations trust the source of any indirect consent. If a list broker or other third party source cannot provide details of how and when consent was obtained, organisations should not rely on it. If an organisation receives complaints from individuals it was told had indirectly consented to its messages, this should act as an alert that the source may be unreliable, and the organisation should not rely on indirect consent from that source in future. See also the section below on buying a marketing list.

95. Some organisations may wish to contact their customers with marketing material relating to third parties. This can take different forms such as the third party providing all of the content of the material which the organisation then sends out or it could be a dual branding exercise between the organisation and the third party.

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

96. In such circumstances although the organisation is not passing the contact details of its customers to a third party it still needs to ensure that it has appropriate consent from its customers to receive marketing promoting third parties. Where possible it would be good practice for the organisation to screen against the third party's suppression list.

Time limits

GDPR Update

The GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time.

See our GDPR consent guidance for further details.

97. There is no fixed time limit after which consent automatically expires. However, consent will not remain valid forever. How long consent remains valid will depend on the context – the question is whether it is still reasonable to treat it as an ongoing indication of the person's current wishes.

98. Of course, consent can be explicitly withdrawn at any time. An organisation may have clear evidence that an individual consented to marketing – for example, a form with a marketing opt-in box ticked. Despite this, if the individual later complains about the fact that it is sending marketing to them, or chooses to unsubscribe or opt out, this means the organisation no longer has their consent and must stop consent-based marketing. A person's most recent indication of their wishes regarding the receipt of marketing is paramount. For indirect consent obtained via a third party, it is also good practice to ask whether the individual wants to withdraw consent from other organisations as well, and if so to inform the third party source to suppress those details and to inform any other users.

99. Even if consent is not explicitly withdrawn, it will become harder to rely on as a genuine indication of the person's wishes as time passes. Further, consent under PECR is expressly considered to be 'for the time being'. We consider this implies a period of continuity and stability, and that any significant change in circumstances is likely to mean that consent comes to an end.

100. Exactly how long an organisation can continue to rely on consent will depend on the circumstances and the person's expectations, which can be affected by the context in which consent was originally given and the nature of the relationship.

101. If consent was originally given in the context of a particular promotional campaign which was only anticipated to last a short period, this might not be enough to indicate ongoing consent for other unrelated marketing messages once that campaign is over. For example, consent to messages about the upcoming launch of a particular new product is not a clear indication of ongoing consent to messages about a different product a year later.

102. If a customer gives consent when signing up to a service, consent is likely to expire if they subsequently cancel their subscription. The organisation should not rely on that consent to send further unsolicited messages to win the customer back.

103. Organisations need to be particularly careful with indirect consent (ie consent given to a third party) for calls, texts or emails. The person must have intended to notify the organisation sending the message that they consent to their messages. It is unlikely that this intention will last very long. Even if they would have originally been happy to receive marketing from that organisation at the time they gave their consent, and for that marketing to continue indefinitely, they will not expect to suddenly start receiving calls, texts or emails from new organisations at a much later date.

104. As a general rule of thumb, if an organisation is making contact by phone, text or email for the first time, we recommend that it does not to rely on any indirect consent given more than six months ago – even if the consent did clearly cover that organisation. However, we accept there may be some very specific cases where the circumstances clearly indicate that the person would expect to start receiving marketing at a certain later date (eg consent to receive offers on seasonal products or annually renewable insurance services).

Proof of consent

GDPR Update

If you are relying on consent you must be able to demonstrate that the individual has consented to you processing their data

for that particular purpose. This means that you must keep evidence of consent – who, when, how, and what you told people.

See our GDPR consent guidance for further details.

105. If someone claims that they did not consent to receive an organisation's marketing messages, that organisation may be at risk of enforcement action unless it can demonstrate that the person did give valid consent.

106. Organisations should therefore make sure that they keep clear records of exactly what someone has consented to. In particular, they should record the date of consent, the method of consent, who obtained consent, and exactly what information was provided to the person consenting. They should not rely on a bought-in list unless the seller or list broker can provide these details. Organisations may be asked to produce their records as evidence to demonstrate compliance in the event of a complaint.

Marketing calls

General rule: screen live calls against the TPS

107. Organisations can make live unsolicited marketing calls, but must not call any number registered with the TPS unless the subscriber (ie the person who gets the telephone bill) has specifically told them that they do not object to their calls. In effect, TPS registration acts as a general opt-out of receiving any marketing calls.

108. In practice, this means that to comply with PECR organisations should screen the list of numbers they intend to call against the TPS register. More information about how to subscribe to the TPS list is available at www.tpsonline.org.uk, or by contacting:

Telephone Preference Service
DMA House
70 Margaret Street
London W1W 8SS

Tel: 020 7291 3310

Email: licensee@dma.org.uk

109. Organisations can only call a customer listed on the TPS if that customer has notified the organisation that they do not object to its calls. This needs to be a positive step to express their wishes – in other words, consent. For example, they might have ticked an opt-in box agreeing to that organisation's marketing calls, confirmed during a previous conversation that they do not object to its calls, or signed up for a service where there is a clear and prominent statement that doing so indicates that they do not object.

110. Opt-in consent is always best. If an organisation wants to rely on another type of action (eg signing up for a service) as notification that the customer does not object, the wording must be very clear and prominent so that the customer will reasonably expect that organisation's marketing calls. There should also be a simple means for them to opt out.

Example
By signing up to this service, you agree to us contacting you by phone to tell you about our other products and services.
If you do not want to receive calls, please tick here □

111. It is not enough that someone simply failed to object to past calls, or failed to take positive steps to opt out of calls. For example, an organisation cannot assume that failing to click on an unsubscribe link, or not replying to an email inviting them to opt out, is notification that they do not object. They must have taken a proactive step to 'notify' the organisation of their wishes.

112. If someone who an organisation has called in the past subsequently registers their number with TPS, the organisation should not make any more marketing calls to them from that point. Even if they have not specifically objected to calls in the past, registering with TPS acts as a general objection which all organisations must respect. An organisation can only call the person again if they have already specifically consented to receive its marketing calls. If so, the fact that they later register with TPS will not override that specific consent, and that organisation may continue to call them.

113. An organisation might want to continue calling an existing customer who has registered with the TPS even though they have not specifically consented, because it is confident in light of the past relationship that they would not object. However, calls in these circumstances are in breach of PECR and could result in enforcement action.

114. When making calls an organisation must always say who is calling, allow their 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.

Fairness

115. PECR does not stop organisations making marketing calls to numbers not registered with the TPS. However, if an organisation knows the name of the individual it is calling, it must still comply with the DPA. In particular, to comply with the first principle, it cannot make marketing calls to them unless it is fair to do so.

116. Organisations must have obtained the person's contact details fairly and lawfully to start with (see the section below on generating leads for more on this). In short, the person should be aware that the organisation has their number and plans to use it for marketing purposes. The organisation must not make any calls that the person would not reasonably expect, or which would cause them unjustified harm.

117. If an organisation obtained someone's contact details from a third party list and doesn't take proper steps to check whether they agreed to this, any marketing calls are likely to be unfair. It is therefore very important to undertake proper due diligence on any bought-in marketing lists – see the section below on buying a marketing list for more on this.

118. Organisations cannot make a marketing call to a number that they originally collected for an entirely different purpose without first getting consent for the change in use.

Example
A bank records information about some of the individuals who are shareholders of its corporate account holders. It collects and holds this information to comply with its duties under anti-money laundering regulations. Unless the bank had

obtained their prior consent, it would be unfair to use this information to make marketing calls inviting those individuals to open personal accounts with the bank.

119. Organisations must not go beyond what someone would reasonably expect in the circumstances, and must not make calls which would unduly distress that person or cause them other unjustified harm. For example, organisations might need to be particularly careful if they are aware that someone is elderly or vulnerable, or if the nature of the marketing might cause offence or stress. Organisations should avoid frequent redialling of unanswered numbers, or calls at antisocial hours.

The right to opt out

GDPR Update

The GDPR gives individuals the right to object at any time to processing of their personal data for the purposes of direct marketing. The right to object to marketing is absolute and you must stop processing for these purposes when someone objects.

See our right to object guidance for further details.

If you are relying on consent to make the live marketing calls then the individual has the right to withdraw their consent at any time. It must be as easy to withdrawn consent as it was to give it.

See our GDPR consent guidance for further details.

120. Organisations must not make unsolicited marketing calls to a person who has said that they don't want those calls. In other words, there is a right to opt out, and organisations cannot call someone who has objected to or opted out of marketing calls.

121. Organisations should not make it difficult to opt out, for example by asking customers to complete a form or confirm in writing. As soon as a customer has clearly said that they don't want the calls, they must stop.

122. If a customer objects or opts out at any time, their details should be suppressed as soon as possible. It is important not to

simply delete their details entirely, otherwise there is no way of ensuring that the organisation does not call them again. See the section on suppression below.

Automated calls

123. The rules on automated calls – that is, calls made by an automated dialling system which play a recorded message – are stricter. Organisations can only make automated marketing calls to people who have specifically consented to receiving automated calls from them. Consent to receive live calls is not sufficient. Indirect consent (ie consent originally given to a third party) is also unlikely to be sufficient. See the section above on what counts as consent.

124. All automated calls must give the identity of the caller, and a contact address or freephone number. Organisations must allow their number (or an alternative contact number) to be displayed to the person receiving the call.

125. Note that there is no need to screen against the TPS when making automated calls. It makes no difference whether or not a number is registered with the TPS. Even if the number is not on the TPS list, that call cannot be made without the person's consent.

Business-to-business calls

126. The same rules apply to marketing calls made to businesses. Sole traders and partnerships may register their numbers with the TPS in the same way as individual consumers, while companies and other corporate bodies register with the Corporate Telephone Preference Service (CTPS). So organisations making business-to-business marketing calls will need to screen against both the TPS and CTPS registers.

Marketing texts and emails

General rule: only with consent

127. Organisations can generally only send marketing texts or emails to individuals (including sole traders and some partnerships) if that person has specifically consented to receiving them. Indirect consent (ie consent originally given to

a third party) is unlikely to be sufficient. See the section above on what counts as consent.

128. The same rule applies to any marketing sent by 'electronic mail', which is defined in PECR as:

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

129. In other words, the same rules will apply to any electronically stored messages, including email, text, picture, video, voicemail, answerphone and some social networking messages. The rules also still apply to viral marketing – organisations will still need consent even if they do not send the messages themselves, but instead instigate others to send or forward them.

130. Organisations must not disguise or conceal their identity in any marketing texts or emails, and must provide a valid contact address for individuals to opt out or unsubscribe (which would mean consent was withdrawn). It is good practice to allow individuals to reply directly to the message and opt out that way, to provide a clear and operational unsubscribe link in emails or at least to provide a freephone number.

Existing customers: the 'soft opt-in'

131. Although organisations can generally only send marketing texts or emails with specific consent, there is an exception to this rule for existing customers, known as the 'soft opt-in'. This means organisations can send marketing texts or emails if:

- they have obtained the contact details in the course of a sale (or negotiations for a sale) of a product or service to that person;
- they are only marketing their own similar products or services; **and**
- they gave the person a simple opportunity to refuse or opt out of the marketing, both when first collecting the details and in every message after that.

132. The texts or emails must be marketing products or services, which means that the soft opt-in exception can only apply to commercial marketing. Charities, political parties or other not-for-profit bodies will not be able to rely on the soft opt-in when sending campaigning texts or emails, even to existing supporters. In other words, texts or emails promoting the aims or ideals of an organisation can only be sent with specific consent.

133. The contact details must be obtained directly from the individual by the organisation who wishes to engage in the marketing and the marketing must be in relation to that organisation's similar products and services. Therefore the soft opt-in can only be relied upon by the organisation that collected the contact details. This means organisations cannot rely on a soft opt-in if they obtained a marketing list from a third party – they will need specific consent. See the section on indirect (third party) consent for more on this.

134. The customer does not actually have to have bought anything to trigger the soft opt-in. It is enough if 'negotiations for a sale' took place. This means that the customer should have actively expressed an interest in buying an organisation's products or services – for example, by requesting a quote, or asking for more details of what it offers. There must be some sort of express communication:

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

135. The communication must be about buying products or services. It is not enough simply to send any query:

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

136. Organisations can only send texts or emails about similar products or services. We consider that the key question here is whether the customer would reasonably expect messages about the product or service in question. This is likely to depend on the context – including the type of business and the category of product. For example, someone who has shopped at a supermarket might reasonably expect messages about a much wider range of goods than someone who has shopped at a specialist store for a specialist product.

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

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

137. Organisations must give the customer the chance to opt out – both when they first collect the details, and in every email or text. Organisations should not assume that all customers will be happy to get marketing texts or emails in future, and cannot rely on the soft opt-in rule unless they provided a clear opportunity to opt out first.

138. It must be simple to opt out. When first collecting a customer's details, this should be part of the same process (eg online forms should include a prominent opt-out box, and staff taking down details in person should specifically offer an opt-out). In subsequent messages, we consider that the individual should be able to reply directly to the message, or click a clear 'unsubscribe' link. In the case of text messages, organisations

could offer an opt-out by sending a stop message to a short code number: eg 'text STOP to 12345'. The only cost should be the cost of sending the message.

The right to opt out

GDPR Update

The GDPR gives individuals the right to object at any time to processing of their personal data for the purposes of direct marketing. The right to object to marketing is absolute and you must stop processing for these purposes when someone objects.

See our right to object guidance for further details.

If you are relying on consent to send the marketing texts or emails then the individual has the right to withdraw their consent at any time. It must be as easy to withdrawn consent as it was to give it.

See our GDPR consent guidance for further details.

139. Organisations must not send marketing texts or emails to an individual who has said they do not want to receive them. Individuals have a right to opt out of receiving marketing at any time. Organisations must comply with any written objections promptly to comply with the DPA – but even if there is no written objection, as soon as an individual says they don't want the texts or emails, this will override any existing consent or soft opt-in under PECR and they must stop.

140. Organisations must not make it difficult to opt out, for example by asking customers to complete a form or confirm in writing. It is good practice to allow the individual to respond directly to the message – in other words, to use the same simple method as required for the soft opt-in. In any event, as soon as a customer has clearly said that they don't want the texts or emails, the organisation must stop, even if the customer hasn't used its preferred method of communication.

141. If a customer objects or opts out at any time, their details should be suppressed from marketing lists as soon as possible. It is important not to simply delete their details entirely, otherwise there is no way of ensuring that the organisation

does not contact them again. See the section on suppression below.

Business-to-business texts and emails

GDPR Update

If you are processing an individual's personal data to send business to business texts and emails the right to object at any time to processing of their personal data for the purposes of direct marketing will apply. The right to object to marketing is absolute and you must stop processing for these purposes when someone objects.

See our right to object guidance for further details.

142. These rules on consent, the soft opt-in and the right to opt out do not apply to electronic marketing messages sent to 'corporate subscribers' which means companies and other corporate bodies eg limited liability partnerships, Scottish partnerships, and government bodies. The only requirement is that the sender must identify itself and provide contact details.

143. However, it serves little purpose to send unsolicited marketing messages to those who have gone to the trouble of saying they do not want to receive them.

144. Corporate subscribers do not include sole traders and some partnerships who instead have the same protection as individual customers. If an organisation does not know whether a business customer is a corporate body or not, it cannot be sure which rules apply. Therefore we strongly recommend that organisations respect requests from any business not to email them.

145. In addition, many employees have personal corporate email addresses (eg firstname.lastname@org.co.uk), and individual employees will have a right under section 11 of the DPA to stop any marketing being sent to that type of email address.

Other types of direct marketing

146. The focus of this guidance is on marketing calls and texts (and by extension, emails and other forms of electronic mail).

However, PECR also specifically regulate marketing by fax, and the DPA can apply to any other type of direct marketing.

Marketing faxes

147. Organisations must not send marketing faxes to individuals (including sole traders and some partnerships) without their specific consent. See the section above on what counts as consent.

148. Organisations can send marketing faxes to companies (or other corporate bodies) without consent, but must not fax any number listed on the Fax Preference Service (FPS) unless that company has specifically said that they do not object to those faxes. This means that to comply with PECR, organisations will need to screen the list of numbers they intend to fax against the FPS register. For more information about FPS, see http://corporate.fpsonline.org.uk/.

149. In addition, organisations must not send marketing faxes to anyone who has said they do not want to receive them. In other words, there is a right to opt out, and organisations cannot fax someone who has objected to or opted out of marketing faxes.

150. All marketing faxes must include the name of the sender and a contact address or freephone number.

Marketing online

151. Organisations must comply with the DPA if they are targeting online adverts at individual users using their personal data – which might apply if, for example, they display personalised adverts based on browsing history, purchase history, or log-in information. However, non-targeted marketing (ie the same marketing displayed to every user) or contextual marketing (ie targeted to the content of the page itself rather than the identity or characteristics of users) is unlikely to be subject to the DPA.

152. For more information on how to comply with the DPA when marketing goods and services online, see the Personal information online code of practice.

153. PECR does not set out any specific rules on direct marketing online, although it does contain rules on cookies, which are

often used to profile users and target behavioural advertising. For more information on using cookies, see our Guidance on the rules on use of cookies and similar technologies.

Marketing mail

GDPR Update

If you are relying on consent to send marketing mail then the individual has the right to withdraw their consent at any time. It must be as easy to withdrawn consent as it was to give it.

See our GDPR consent guidance for further details.

The GDPR also gives individuals the right to object at any time to processing of their personal data for the purposes of direct marketing. The right to object to marketing is absolute and you must stop processing for these purposes when someone objects.

See our right to object guidance for further details.

154. PECR does not cover marketing by mail, but organisations sending marketing mail to named individuals must comply with the DPA. If an organisation knows the name of the person it is mailing, it cannot avoid DPA obligations by simply addressing the mail to 'the occupier', as it is still processing that individual's personal data behind the scenes.

155. In essence, the DPA requires that an individual is aware that an organisation has their contact details, and intends to use them for marketing purposes. The organisation must have obtained the address fairly and lawfully. It cannot send marketing mail if the address was originally collected for an entirely different purpose. And organisations must not send marketing mail to anyone who objects or opts out. They must comply with any written objections promptly under section 11 of the DPA. See the section on the DPA above for more information.

156. Individuals can register their address with the Mail Preference Service (MPS), which works in a similar way to the TPS. The DPA does not specifically require organisations to screen against the MPS, but it is good practice to do so and will save time and money. It is, however, a requirement under the DMA code and the CAP code, and we are aware that the DMA

considers it is also a legal requirement under the Consumer Protection from Unfair Trading Regulations 2008. We therefore advise organisations to screen against the MPS to ensure compliance with the first principle requirement to act fairly and lawfully.

157. If an organisation is sending mailshots to every address in an area and does not know the identity of the people at those addresses, it is not processing personal data for direct marketing, and the DPA rules will not apply. However, it may still need to comply with other guidelines and codes on marketing and advertising.

Lead generation and marketing lists

158. Marketing lists can be compiled in different ways, and vary widely in quality. A good marketing list will be up to date, accurate, and reliably record specific consent for marketing. A list like this can be used in compliance with the law and should generate few – if any – complaints. However, other lists may be out of date, inaccurate, and contain details of people who have not consented to their information being used or disclosed for marketing purposes. Using such a list is likely to result in a breach of both the DPA and PECR.

159. A list might contain data compiled in-house from customer contacts. Or it might be a bought-in list of people an organisation has never dealt with directly. Or it could be a mixture of the two. This is an important distinction, because a list compiled in-house should be more accurate and up to date – and easier to check. Quality issues are harder to identify if lists are bought in. And, for certain types of marketing, the law works differently if people's details were not obtained directly.

Generating leads

GDPR Update

You must be able to demonstrate that you have obtained valid consent, which means that you must keep records of who consented, when, how, and what you told people.

See our GDPR consent guidance for further details.

160. There are a wide range of sources for marketing leads. These might include public directories, previous customers and people who have sent an email, registered on a website, subscribed to offers or alerts, downloaded a mobile app, entered a competition, used a price-comparison site to get a quote, or provided their details in any other way. An organisation may be able to legitimately use these sources, but must ensure that it complies with the DPA – and in particular that it acts fairly and lawfully – whenever and however it collects personal data.

161. This also applies to list brokers and lead generation firms. Whether an organisation is collecting personal data for its own use, or to sell marketing leads on to others, it must always act fairly and lawfully.

162. If collecting contact details directly from individuals, an organisation should provide a privacy notice explaining clearly that it intends to use those details for marketing purposes. This should not be hidden away in a dense or lengthy privacy policy or in small print. Organisations must not conceal or misrepresent their purpose (eg as a survey or competition entry) if they also intend to use the details for marketing purposes. And if they intend to sell or disclose the details to other organisations, the privacy notice should make this very clear, and get the person's specific consent for this. See the Privacy notices code of practice for more information on how to provide an appropriate privacy notice.

163. Organisations should also get specific consent at this stage for any marketing texts, emails or automated calls (eg by providing an opt-in box). See the section above on what counts as consent.

164. Organisations cannot escape their obligations by asking existing contacts to provide contact details for their friends and family. Organisations must still act fairly and lawfully, and cannot assume that the contact will act in the other person's best interests – especially if there are incentives for providing the information. In fact, we would advise against this type of viral marketing, as it will be difficult to be sure there is the necessary consent to comply with obligations under the DPA and PECR. Organisations who do this must at the very least clearly explain that the contact should only provide someone else's details with that person's consent, and that the person may be told who provided their details. They should also

provide a privacy notice to the new contact as soon as possible, unless it would be disproportionate to do so.

165. Remember that PECR applies to any calls, texts or emails made for any direct marketing purpose, including lead generation – even if there is no sales or promotional material in that first message. So organisations cannot send mass texts, emails or automated calls in order to generate leads, as they won't have the necessary consent. And organisations cannot generate new leads by cold-calling numbers registered with the TPS.

166. We are aware that some organisations trace and record the number of any customer who calls them, even if the caller has taken steps to block their number. Overriding a caller's preference for anonymity in this way undermines the calling line identification (CLI) provisions in PECR, and collecting blocked numbers would clearly be unfair under the DPA. Even if a caller has not actively blocked their number, organisations must inform callers if their number will be kept for marketing purposes, and should offer them an opt-out.

167. Some disreputable organisations obtain leads under false pretences – for example, by misrepresenting their purpose as market research, or in extreme cases by using phishing scams – or try to induce employees of other organisations to leak their customer lists. Generating leads in this way – or in any other way which is not open and honest – is a clear breach of the DPA. Further, it will be a criminal offence under section 55 to knowingly or recklessly obtain personal data from another organisation without its knowledge and consent.

168. Organisations obtaining leads from a third party should refer to the section below on buying a marketing list.

Selling a marketing list

GDPR Update

You must name any third party controllers who will be relying on the consent – precisely defined categories of third parties will not be acceptable under the GPDR.

You must be able to demonstrate that the individual has consented to you processing their data for that particular purpose. This means that you must keep evidence of consent – who, when, how, and what you told people.

See our GDPR consent guidance for further details.

169. Organisations must act fairly and lawfully when selling a marketing list. If an organisation obtained details from individuals with the intention of selling them on, it must have made it clear that their details would be passed on to third parties for marketing purposes and obtained their consent for this. It is good practice to specifically name (or at least give a clear description of) the third parties to whom details may be sold. See the section above on what counts as consent.

170. Anyone selling a list should understand that the rules on electronic marketing are stricter than for more traditional marketing methods, and that they cannot take a one-size-fits-all approach to consent or the sale of marketing lists. A list with general consent to third party marketing may be enough for mail marketing, but is unlikely to cover calls, texts or emails. Call lists must be screened against the TPS, and third party lists can only be used for text or email marketing in limited circumstances.

171. A buyer will only be able to send marketing texts or emails, or make automated calls, to people on the list if they gave specific consent. In most cases indirect consent – that is, consent given to someone other than the organisation doing the marketing – will not be enough for this. This means that some marketing lists will be of limited value to buyers wanting to carry out text, email or automated call campaigns. See the section above for more information about the limitations of indirect (third party) consent.

172. An organisation wanting to sell a marketing list for use in text, email or automated call campaigns will therefore need to keep clear records showing when and how consent was obtained, by whom, and exactly what the individual was told (including copies of privacy notices), so that it can give proper assurances to buyers. Organisations must not claim to sell a marketing list with consent for texts, emails or automated calls if it does not have clear records. We consider it would be unfair and in breach of the DPA to sell a list without keeping clear records of consent, as it is likely to result in individuals receiving non-compliant marketing.

173. An organisation wanting to sell a marketing list for use in telephone campaigns should also make clear whether it has

pre-screened the list against the TPS register, and if so on what date it was last screened.

174. Note that it is a criminal offence under section 55 of the DPA to sell or offer to sell a marketing list if any of the customer details were knowingly or recklessly obtained from another data controller without its consent.

175. Although an organisation will usually need an individual's consent to sell their details on for marketing purposes, if a business is insolvent, or being closed down or sold, its customer database can be sold on without prior consent. However, the seller must make sure the buyer understands that they can only use the information for the same purpose for which it was collected by the original business. Any use of the information should be within the reasonable expectations of the individuals concerned. So, when a database is sold, its use should stay the same or similar. For example, if the database contains information obtained for insurance, the database should only be sold to another insurance-based business providing similar insurance products. Selling it to a business for a different use is likely to be incompatible with the original purpose, and likely to go beyond the expectations of the individuals. If the buyer does want to use the information for a new purpose, they will have to get consent from the individuals concerned.

Buying a marketing list

GDPR Update

If you are buying a 'consented' marketing list, the consent request must have identified you specifically. Even precisely defined categories will not be enough to give you valid informed consent under the GDPR definition.

You must keep records to demonstrate what the individual has consented to, including what they were told, and when and how they consented.

See our GDPR consent guidance for further details.

If you buy personal data from another organisation, you must provide people with your own transparency information detailing anything that they haven't already been told.

See our guidance on the right to be informed for further details.

176. Organisations buying or renting a marketing list from a list broker or other third party must make rigorous checks to satisfy themselves that the third party obtained the personal data fairly and lawfully, that the individuals understood their details would be passed on for marketing purposes, and that they have the necessary consent.

177. Organisations should take extra care if using a bought-in list to send marketing texts, emails or automated calls. They must have very specific consent for this type of marketing, and in most cases indirect consent (ie consent originally given to another organisation) will not be enough – see the section above on indirect (third party) consent. Remember also that the 'soft opt-in' exception for email or text marketing cannot apply to contacts on a bought-in list.

178. Organisations must check how and when consent was obtained, by whom, and what the customer was told. It is not acceptable to rely on assurances of indirect consent without undertaking proper due diligence, to demonstrate consent if challenged. Organisations seeking to rely on consent must ensure that consent was validly obtained, that it was reasonably recent, and that it clearly extended to them specifically or to organisations fitting their description.

179. Reasonable due diligence might include checking the following:

- Who compiled the list? When? Has it been amended or updated since then?
- When was consent obtained?
- Who obtained it and in what context?
- What method was used – eg was it opt-in or opt-out?
- Was the information provided clear and intelligible? How was it provided – eg behind a link, in a footnote, in a pop-up box, in a clear statement next to the opt-in box?
- Did it specifically mention texts, emails or automated calls?
- Did it list organisations by name, by description, or was the consent for disclosure to any third party?
- Has the list been screened against the TPS or other relevant preference services? If so, when?
- Has the individual expressed any other preferences – eg regarding marketing calls or mail?
- Has the seller received any complaints?

- Is the seller a member of a professional body or accredited in some way?

180. A reputable list broker should be able to demonstrate that the marketing list for sale or rental is reliable, by explaining how it was compiled and providing full details of what individuals consented to, when and how. If the seller cannot provide this information, a buyer should not use the list. It would be prudent for a buyer to have a written contract in place confirming the reliability of the list, as well as making its own checks. The contract should give a buyer reasonable control and audit powers.

181. Once an organisation has bought the list it should make sure it is prepared to deal with any inaccuracies or complaints arising from its use. If it receives complaints from individuals whose details came from a particular source, this would suggest that the source is unreliable and should not be used. A sampling exercise might help to assess how reliable the list actually is. It is also good practice to inform the individual where their details came from and ask whether they want to withdraw consent from other organisations as well, and if so to inform the source that consent has been withdrawn from all users.

182. The DPA requires that any personal information held should be adequate, relevant and not excessive, and that it should not be kept for longer than necessary. Organisations buying a list should decide how much of the information they actually need to keep. Any unnecessary personal information should be deleted. Personal information should not be held simply on the basis that it might become useful one day.

183. Organisations buying a list should also consider providing their own privacy notice to the individuals concerned as soon as possible, unless it would be disproportionate to do so. See the Privacy notices code of practice for more information on when and how to provide a privacy notice. We accept that in practice this is likely to be more difficult for organisations making contact by phone.

184. It is also good practice for organisations using bought-in lists to include the name and contact details of the organisation that provided the person's details in any marketing message.

185. Even if an organisation does not need specific consent for its marketing (eg for calls screened against the TPS list, or for mail marketing), it should still not go beyond what the

individuals would reasonably expect. It should only market products or services which are reasonably similar to those which have been promoted to those customers in the past, or which they have a clear reason to expect. Bought-in call lists must always be screened against the TPS. And they should also be screened against the organisation's own in-house suppression (do not call) list, to ensure it doesn't contact anyone who has already said they want to opt out of its marketing.

In-house marketing lists

GDPR Update

You must keep records to demonstrate what the individual has consented to, including what they were told, and when and how they consented.

See our GDPR consent guidance for further details.

186. Organisations might want to compile their own in-house marketing list of people who have bought goods or services in the past, or who have registered on a website or made an enquiry. They can do so, but should ensure they use these details fairly, and must make it clear that they intend to use the details for marketing. Organisations should not assume that an individual consents to marketing just because they have provided their details. See the section above for more information on generating leads.

187. Organisations should record whether the customer is an individual (including sole traders and some partnerships) or a company, as different rules apply. If this is not clear, assume they are an individual.

188. Organisations should also keep a copy of the information provided to the customer, and record when and how they obtained any consent. They should specifically record whether they have consent for texts, emails and automated calls.

189. Organisations should generally screen an in-house marketing list against the TPS register before making any marketing calls. It might be possible in some circumstances to make calls from an in-house list without screening against the TPS register – but only if they have obtained a clear positive indication from

every person on the list that they do not object to those calls. It is not enough to simply rely on the fact that they had failed to object in the past unless the list is also screened against the TPS. See the section above on marketing calls for more information.

Suppression

GDPR Update

The right to object to direct marketing under Article 21(3) does not prevent a controller from holding a suppression list, as the list supports the individual's right to object and is held for compliance rather than for direct marketing purposes. See our right to object guidance for further details.

190. Organisations should maintain a 'suppression list' of people who have opted out or otherwise told that organisation directly that they do not want to receive marketing.

191. Note that individuals may ask an organisation to remove or delete their details from a database or marketing list. However, in most cases organisations should instead follow the marketing industry practice of suppressing their details.

192. Rather than deleting an individual's details entirely, suppression involves retaining just enough information to ensure that their preferences are respected in the future. Suppression allows organisations to ensure that they do not send marketing to people who have previously asked them not to, as there is a record against which to screen any new marketing lists. If people's details are deleted entirely, there is no way of ensuring that they are not put back on the database. Deleting details might also breach industry-specific legal requirements about how long to hold personal data.

193. Organisations must not contact people on a suppression list at a later date to ask them if they want to opt back in to receiving marketing. This contact would involve using their personal data for direct marketing purposes and is likely to breach the DPA, and will also breach PECR if the contact is by phone, text or email.

194. However, we recognise that people can change their minds and that marketing strategies also change. There is some merit in making sure that the information about people's preferences is

accurate and up to date. We consider that it can be acceptable to send a message immediately after someone has opted out confirming they have unsubscribed and providing information about how to resubscribe, or to remind individuals that they can opt back in to marketing if the reminder forms a minor and incidental addition to a message being sent anyway for another purpose. However, organisations must do this sensitively, must not include marketing material in the message, and must never require an individual to take action to confirm their opt-out.

Example
A bank sends out annual statements to its customers detailing transactions on their deposit accounts during the previous year. A message is printed at the bottom of each statement to remind customers that they may wish to review their marketing preferences and telling them how to update them.

Example
A fitness centre regularly mails a newsletter to its members. Some members have objected to this use of their personal data and the fitness centre has, quite properly, flagged this objection on their system.

The fitness centre wants to ensure that these previously expressed wishes have not changed, particularly since the content of the newsletter has changed considerably over the last few months and it can also now be sent out as an email. However, the fitness centre cannot assume that people may have changed their minds. They should assume that any objections they received recently are still an accurate reflection of the members' wishes.

For older objections, they could mention the changes to the newsletter and the possibility of receiving it by email in any 'usual course of business' contact they have with the member, such as a membership renewal letter. However, they should not contact those members with the specific intention of showing them "what they are missing".

Other considerations

195. The DPA and PECR rules on direct marketing do not cover leaflets, circulars, inserts, field marketing, media adverts or other marketing channels which are not individually addressed. However, organisations will still need to comply with other relevant codes and guidelines on marketing and advertising. See the section above on other regulation.

196. For more advice and guidance on providing privacy notices when collecting or using people's details for marketing purposes, see the Privacy notices code of practice.

197. If your company is receiving unwanted marketing calls or faxes and you want to register your company's number with CTPS or FPS, see our separate guidance for Companies receiving unwanted marketing.

198. Information for the public on what to do about nuisance calls or texts is available on the 'for the public' pages of our website.

More information

200. Additional guidance is available on our guidance pages with more information on other aspects of the DPA or PECR.

201. This guidance has been developed drawing on ICO experience. Because of this it may provide more detail on issues that are often referred to the Information Commissioner than on those we rarely see. The guidance will be reviewed and considered from time to time in line with new decisions of the Information Commissioner, Tribunals and courts.

202. It is a guide to our general recommended approach, although individual cases will always be decided on the basis of their particular circumstances.

203. If you need any more information about this or any other aspect of data protection, please contact us, or visit our website at www.ico.org.uk.