

The Guide to Privacy and electronic communications

ico.

Information Commissioner's Office

1

Rules on marketing

- 3 Key definitions
- 5 Automated calls
- 7 Telephone marketing
- 13 Fax marketing
- 16 Electronic mail
- 33 Viral marketing
- 35 Appending email addresses/ mobile numbers
- 36 Loyalty schemes
- 37 Pan European marketing
- 38 Marketing to more than one medium

2

Other rules

- 39 Security of services
- 43 Confidentiality of communications (cookies)
- 46 Traffic data
- 49 Location data
- 52 Itemised bills
- 53 Calling or connected line identification (CLI)
- 57 Directories of subscribers
- 60 Contracts
- 61 National security
- 62 Legal requirements

1

Rules on marketing

Key definitions

What is the definition of direct marketing?

Section 11 of the Data Protection Act 1998 refers to direct marketing as 'the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals'.

We regard direct marketing as covering a wide range of activities that apply not just to the offer for sale of goods or services, but also to the promotion of an organisation's aims and ideals. This would include a charity or a political party appealing for funds or support and, for example, an organisation that is encouraging individuals to write to their MP about something or to attend a public meeting or rally. This view was supported by the [UK Information Tribunal ruling](#) when they dismissed an appeal by the Scottish National Party, which argued that political campaigns were not covered.

How do the defined terms apply to marketing?

The Regulations refer to person, caller, subscriber, individual subscriber, and corporate subscriber, among other defined terms.

When the Regulations say:

person – this means a 'legal' person, for example, a business or a charity, or a 'natural' person, that is, a living individual;

caller – this means the instigator of a call. This is usually a legal person. The call would not be made or the fax, email, text or picture

message would not be sent unless this caller paid for it to be made or sent;

subscriber – this means the person who pays the bill for the use of the line (that is, the person legally responsible for the charges);

individual subscriber – this means a residential subscriber, a sole trader or a non-limited liability partnership in England, Wales and Northern Ireland;

corporate subscriber – this includes corporate bodies such as a limited company in the UK, a limited liability partnership in England, Wales and Northern Ireland or any partnership in Scotland. It also includes schools, government departments and agencies, hospitals and other public bodies, for example, the Information Commissioner's Office.

Does the phrase 'for the time being' mean consent only lasts a finite period?

Many of the Regulations refer to consent being given 'for the time being'. We interpret this as meaning that consent will remain valid until there is good reason to consider it is no longer valid; for example, if it has been withdrawn or it is otherwise clear that the recipient no longer wants to get such messages. The initial consent will remain valid if there are good grounds for believing that the recipient remains happy to get the marketing communications in question; for example, where the recipient has responded positively (that is, has not objected) to previous, reasonably recent marketing emails.

The phrase 'for the time being' is also used in the Regulations for notifications of objection. For example, Regulation 21(1) (a) says that unsolicited direct marketing calls should not be made if the subscriber has notified that such calls should not be made 'for the time being'. We interpret this as meaning that the objection will remain valid until there is good reason to ignore it; for example, if the individual has changed their mind and indicated that they now consent to receiving such calls.

Automated calls (Regulations 19 and 24)

How do the Regulations apply to automated calling systems?

The Regulations restate the requirement of the 1999 Regulations for marketing by automated calling or communication systems.

However, Regulation 19(4) clarifies the definition of 'automated calling system'. It refers to a system that is 'capable of automatically initiating a sequence of calls to more than one destination in accordance with instructions stored in that system' and that transmits 'sounds which are not live speech for reception by persons at some or all of the destinations so called'. [The UK Information Tribunal ruled on a case](#) where automated calls had been used to promote the Scottish National Party in the lead-up to the 2005 General Election.

It is important to note that automated calling systems do not cover marketing by text, picture or video message, by fax or by email. They also do not cover the technology some call centres use to dial target numbers automatically to initiate live telephone conversations, so-called 'power dialling'. Text, picture and video messages, faxes, live voice telephone calls and emails are covered elsewhere in the Regulations.

This is what the law requires:

- Marketing material may be transmitted by such a system only with the prior consent of a subscriber. This means the subscriber must have told the caller that they consent, for the time being, to the caller making or instigating such communications to be sent on that line (Regulations 19(1) and (2) apply).
- A subscriber must not permit their line to be used to contravene Regulations 19 (Regulation 19(3) applies).
- All marketing messages sent by this method of communication must include the identity of the caller and a contact address or Freephone number (Regulation 24(1)(a) applies).

The mischief that Regulation 19 aims to tackle is where a subscriber receives a marketing call that is a recorded message, with no opportunity to speak to a 'live' person. Such calls are particularly intrusive and can be unsettling for the recipient. So we take a firm line on this point. We believe that even if the recipient is given an opportunity to talk to a 'live' person at some point in the message, for example, 'to speak to a live operator, press 1', such a call would still be covered by the prior consent rule because recipients without touch-tone phones would be excluded from such an opportunity.

A subscriber is not registered with TPS and has not contacted us to tell us that they object to us marketing them by telephone. Can we call them with a pre-recorded marketing message?

No. You would need their prior consent to do so.

The regulation on automated calling systems does not spell out our obligation to respect an opt-out request from a subscriber. Does this mean we don't have to comply with such requests?

In our view, if you can send marketing by automated calling systems to a subscriber only if that subscriber has given their consent to such calls, this implies they can withdraw consent at a later stage. We would quote the inclusion of the phrase 'for the time being' (Regulation 19(2)) to support our view. We are likely to take enforcement action against companies in the UK jurisdiction who persistently fail to comply with opt-out requests from subscribers.

Telephone marketing (Regulations 21 and 24)

How do the Regulations apply to telephone marketing?

The Regulations restate the 1999 Regulations with respect to marketing by telephone, with two significant changes. First, from 11 December 2003, corporate subscribers have had an enforceable right to opt out of receiving marketing calls, which they can exercise by asking the caller to stop making further marketing calls to a particular number or particular numbers. Second, and with effect from 25 June 2004, corporate subscribers have been allowed to register their numbers on the Telephone Preference Service (TPS).

This is what the law requires:

- If any subscriber has told you to stop making telesales calls to their number, you must comply with that request (Regulation 21(1)(a) applies).
- You must not make or instigate the making of unsolicited telesales calls to any number listed on the TPS register (Regulation 21(1)(b) applies).
- TPS registration takes 28 days to come into force. Calls may be made to a number during the registration period unless an opt-out request has also been made to the caller (see 1 above) (Regulation 21(3) applies).
- You may make or instigate the making of unsolicited telesales calls to a TPS-registered subscriber if that subscriber has notified you that, for the time being, they do not object to receiving such calls on that TPS-registered number (Regulation 21(4) applies).
- A subscriber can withdraw that overriding consent at any time, in which case, further telesales calls must not be made to that number (Regulation 21(5) applies).
- You must identify yourself when making a telesales call. If asked, you must provide a valid business address or Freephone telephone number at which you can be contacted. When using a subcontractor, the subcontractor's call centre staff must identify the instigator of the call (that is, the organisation on whose behalf they are making the call) (Regulation 24(1)(b) applies).

- Subscribers must not let their lines be used to contravene Regulation 21 (Regulation 21(2) applies).

What is the TPS?

The Telephone Preference Service (TPS) list is a statutory list of telephone numbers where the subscriber to that number has registered a general objection to receiving unsolicited marketing calls on that number. From 25 June 2004, corporate subscribers have been allowed to register their numbers on the Corporate Telephone Preference Service (CTPS). [See our guidance for more information on the rules about calling corporate subscribers.](#)

Does TPS registration apply to mobile numbers?

Any mobile number can be registered on the TPS to block unwanted 'live' calls. If you wish to market by text, picture or video message, you do not need to screen against the TPS but you need prior consent before sending such messages. The rules on marketing by text, picture or video message are covered in the Electronic mail section of this guidance.

We pay a subcontractor to make the calls for us. Isn't it their responsibility to make sure we don't break the rules?

No, under the Regulations it's your responsibility as the instigator of the call. They may be contractually obliged to make sure you don't break the rules but if they let you down, you are responsible under the Regulations as the person who instigated the call. If we were to take enforcement action, we would usually take it against you not your subcontractor. You should check you have appropriate contracts to guard against such failures. If your subcontractor's failures cause you to break the rules, seek legal advice about an action for breach of contract and find another subcontractor who will make sure you don't break the rules.

The ICO could take action against subcontractors who allow their lines to be used in breach of the Regulations (Regulation 21(2) applies), but this is more likely to happen where the subcontractor and their clients work together to disregard the Regulations. It is

unlikely that this would apply, for example, to telemarketing activities conducted by an individual working at home on commission on behalf of a company, using telephone lists it provides. This is because the individual could not be expected to know all the company's legal obligations.

Do the rules mean our call centre staff have to give out their names?

No. The rules mean they have to give out the name of the company whose products or services they are promoting. If asked, they must also provide a valid address or freephone number at which the company can be contacted with an opt-out request.

If the subcontractor is making the calls on our behalf, do they have to provide their identity or ours?

They must provide your identity because you have instigated the call; the call would not be made unless you paid for it to be made. If asked, your subcontractor or their call centre staff must provide a valid address or freephone number at which you can be contacted with an opt-out request.

We delete numbers from our database whenever we get an opt-out request. Are we doing enough?

No. You must suppress details when you receive an opt-out request, not delete them. If you delete them, you have no record to show that you should not call that number. You or your subcontractor might collect it again from a list broker. The only way you can legally call that number again is if the subscriber tells you directly that they have changed their mind and are now happy to hear from you again.

If you use subcontractors, you must make sure they don't call numbers on your suppression list or numbers registered on the TPS.

Several members of a household use the same telephone number and may make different choices about who they want to hear from. How does the law apply?

If the subscriber to that phone line (that is, the person who pays the bill) has registered the number on the TPS, this indicates a general objection to receiving any unsolicited marketing calls on that number. This objection applies to the whole household but does not apply to calls that are 'solicited'.

Individual members of the household may invite (solicit) marketing calls from different companies, but those calls may only be made to the individual who has issued the invitation, not to other members of the household. This invitation can be revoked at any time.

Individual members of the household may also have existing relationships with a number of companies, which pre-date TPS registration. Unsolicited marketing calls from those companies may be a feature of that relationship. If the individual members of the household wish to prevent marketing calls from any of those companies, they must each contact the company concerned directly to inform them they no longer wish to receive marketing calls from them.

We have bought or rented a list of numbers where the subscribers have consented to receiving unsolicited marketing calls from third parties, but some of the numbers are TPS registered. Can we call those numbers?

TPS registration indicates a general objection to receiving unsolicited marketing calls. The TPS list is statutory. Subscribers can give consent to receiving unsolicited marketing calls from a caller, which overrides TPS registration, but this is only valid if that overriding consent is given to the particular caller.

If you obtain a list of numbers where you are assured that the subscribers consent to receiving unsolicited marketing calls, you should make sure you screen the list against the TPS and your own suppression list before making any telesales calls. If you buy or rent a list, regardless of the assurances you have been given, you will still breach the Regulations if you call a number listed on the TPS.

We would like to call existing customers who are registered on the TPS. Can we do so?

It depends. The Regulations say you may make marketing calls to a number registered with the TPS if the subscriber has notified you

that they do not object to receiving such calls. [See our guidance on calling existing customers.](#)

We are a charity / We are a fundraiser / We lobby for particular causes. Do we have to screen against the TPS when we conduct a telephone campaign?

Yes, you do. There is no exemption from the TPS rules for not-for-profit organisations. The ICO regards the term 'direct marketing' as covering a wide range of activities which will apply not just to the offer for sale of goods or services, but also to the promotion of an organisation's aims and ideals. This would include a charity or political party making an appeal for funds or support and, for example, an organisation that encourages individuals to write to their MP on a particular matter or to attend a public meeting or rally.

We only do business-to-business telesales and have a list of established contacts we regularly call; do we need to screen our list against the TPS list?

Are they all contacts to whom you regularly make a sale? Are you sure that any sales calls you make to those numbers would be welcomed? If so, you do not need to screen the list against the TPS or CTPS. You should remember that if those contacts change their mind and tell you they no longer wish you to call them, you are legally obliged to respect that request. Make sure you suppress rather than delete their numbers.

In any other case, you should screen the list against the TPS and CTPS lists.

We have a list of business-to-business telephone contacts we call regularly. They haven't told us to stop calling them before now, but we haven't sold anything to them yet. Do we have to screen our list against the TPS lists?

Yes, unless you can satisfy yourself that all those contacts would be happy to hear from you. If a company registers their numbers on the TPS list, that suggests they are unlikely to respond positively to telesales calls. If you have not had a positive response from that company in the past and they are registered on the TPS, it would be

difficult for you to show they would be happy to hear from you in the future. Unless you screen against the TPS list, if they have registered their numbers on the TPS list and you call them, you risk breaching the Regulations (and damaging your reputation).

We have a mix of established and potential business-to-business telephone contacts on our list. Do we still have to screen it against the TPS lists?

Yes. You should note our comments above about established contacts.

One of our potential business-to-business contacts has now registered their numbers on the TPS. Since then, one of their other employees has expressed an interest in our products and asked us to call with a quotation. Can we call that employee?

Yes, that would be a solicited call. TPS registration prevents unsolicited calls. If you want to make subsequent unsolicited calls to that company, you should explain the situation to your new contact at the company and ask them whether they wish to consent on their employer's behalf, which would override TPS registration. You should make a note of details of the conversation in case you are challenged in the future.

How do we know whether a person is authorised to give consent on their employer's behalf?

Unless you have reason to think they would not be authorised, you can take their authorisation in good faith. You may wish to take a note of their name and the date the authorisation was given.

Fax marketing (Regulations 20 and 24)

How do the Regulations apply to fax marketing?

The Regulations duplicate the 1999 Regulations for marketing by fax.

However, as a reminder, this is what the law requires:

- You must not send or instigate the sending of an unsolicited marketing fax to the line of an individual subscriber without their prior consent (Regulation 20(1)(a) applies).
- You must not send or instigate the sending of an unsolicited marketing fax to the line of a corporate subscriber if that subscriber has asked you not to fax on that line (Regulation 20(1)(b) applies).
- You must not send or instigate the sending of an unsolicited marketing fax to a number listed on the Fax Preference Service (FPS) register (Regulation 20(1)(c) applies).
- FPS registration takes 28 days to come into force. Faxes may be sent to a subscriber's number during the registration period unless an opt-out request has also been made to the caller (see 2 above) (Regulation 20(4) applies). If the subscriber is an individual subscriber, you must not do so unless you have their prior consent (see 1 above).
- You may send unsolicited marketing faxes to an FPS-registered subscriber if the subscriber has notified you that, for the time being, they do not object to receiving such calls (Regulation 20(5) applies).
- A subscriber may withdraw that overriding consent at any time, in which case, you must not send further marketing faxes to that number (Regulation 20(6) applies).
- You must provide your identity (the name of the business being promoted) and a valid business address or Freephone telephone number at which you can be contacted on each fax you send (Regulation 24(1)(a) applies).
- A subscriber must not allow their line to be used to breach Regulation 20 (Regulation 20(3) applies).

What is the FPS?

The Fax Preference Service (FPS) list is a statutory list of telephone numbers where the subscriber to that number has registered a general objection to receiving unsolicited marketing faxes on that number.

We delete numbers from our database whenever we get an opt-out request. Are we doing enough?

No. You must suppress details when you receive an opt-out request, not delete them. If you delete them, you have no record to show you should not fax that number. You or your subcontractor might collect it again from a list broker. The only way you can legally fax that number again is if the subscriber tells you directly they have changed their mind and are now happy to hear from you again. If you use subcontractors, you must ensure they screen against your suppression list and ensure they don't fax numbers registered on the FPS.

We pay a subcontractor to send faxes for us. Isn't it their responsibility to make sure we don't break the rules?

No, under the Regulations it's your responsibility. They may be contractually obliged to ensure you don't break the rules but if they let you down, you are responsible under the Regulations as the person who instigated the sending of a fax. If we were to take enforcement action, we would usually take it against you and not your subcontractor. You should check you have appropriate contracts to guard against such failures. If your subcontractor's failures cause you to break the rules, seek legal advice about an action for breach of contract and find another subcontractor who will make sure you don't break the rules.

The ICO could take action against subcontractors who allow their lines to be used in breach of the Regulations (Regulation 20(3) applies) but this is more likely if the subcontractor and their clients work together to disregard the Regulations. It is unlikely that this would apply, for example, to fax marketing activities conducted by an individual working at home on commission on behalf of a company using contact lists it provides. This is because the individual could not be expected to know all the company's legal obligations.

If the subcontractor is sending faxes on our behalf, do they have to provide their identity or ours?

They must provide your identity and a valid address or Freephone number at which you can be contacted with an opt-out request.

We have bought or rented a list of fax numbers where the subscribers have consented to receiving unsolicited marketing faxes from third parties. Some of the numbers are FPS registered – can we fax them?

FPS registration indicates a general objection to receiving unsolicited marketing faxes. The FPS list is a statutory list. Subscribers can give consent to receiving unsolicited marketing faxes from a caller, which overrides FPS registration, but this is only valid if that overriding consent is given to the particular caller.

If you obtain a list of numbers where you are assured that the subscribers consent to receiving unsolicited marketing faxes, you should make sure you screen the list against the FPS list and your own suppression list before sending any marketing faxes. If you buy or rent a list, regardless of the assurances you have been given, you will still breach the Regulations if you call a number that is listed on the FPS.

Electronic mail

How do the Regulations apply to marketing by electronic mail?

The Regulations define electronic mail 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' (Regulation 2 'Interpretation' applies).

In other words, email, text, picture and video marketing messages are all considered to be 'electronic mail'. Marketing transmitted in WAP messages is considered to be 'electronic mail'. WAP Push allows a sender to send a specially formatted SMS message to a handset which, when received, allows a recipient through a single click to access and view content stored online, through the browser on the handset.

We consider this rule also applies to voicemail and answerphone messages left by marketers making marketing calls that would otherwise be 'live'. So there are stricter obligations placed on you if you make live calls but then wish to leave messages on a person's voicemail or answerphone.

Faxes are not considered to be 'electronic mail'. Fax marketing is covered elsewhere in the Regulations. These regulations also do not cover so-called silent calls or calls where a fax or other electronic signal is transmitted; this is because no marketing material is transmitted during these calls.

This is what the law requires:

- You cannot transmit, or instigate the transmission of, unsolicited marketing material by electronic mail to an individual subscriber unless they have previously notified you, the sender, that they consent, for the time being, to receiving such communications. There is an exception to this rule which has been widely referred to as the soft opt in (Regulation 22(2) refers).
- You cannot transmit, or instigate the transmission of, any marketing by electronic mail (whether solicited or unsolicited) to any subscriber (whether corporate or individual) where:

- your identity has been disguised or concealed; or
 - you have not provided a valid address to which the recipient can send an opt-out request.
 - That electronic mail would contravene regulations 7 or 8 of the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013); or
 - That electronic mail encourages recipients to visit websites which contravene those regulations (Regulation 23 refers).
- A subscriber must not allow their line to be used to breach Regulation 22(2) (Regulation 22(4) refers).

For further information, read our [guidance on electronic mail marketing](#).

What is the difference between a ‘solicited marketing message’ and an ‘unsolicited marketing message that the subscriber consents to receiving’?

A ‘solicited message’ is one the subscriber has actively invited. We accept that this invitation can be given through a third party. An ‘unsolicited marketing message that a subscriber has opted into receiving’ is one they have not invited, but that for the time being they do not object to receiving. If challenged, you would need to demonstrate that the subscriber has positively opted into receiving further information from you.

What would be a ‘valid address’ for the purpose of Regulation 23?

Online, this could be a valid email address. We accept that short code numbers could be used as a ‘valid address’ in text messages, as long as they do not incur costs other than the cost of sending the message (that is, using the short code does not incur premium-rate charges). As good practice, promotional text messages should include a valid website address (where further valid contact details can be found) or a valid PO Box number.

Is there any difference between an individual subscriber and the recipient of marketing material by electronic mail (Regulation 22(2))?

Yes, there is a difference.

The Directive that these Regulations implement says unsolicited marketing should not be sent by electronic mail to an individual subscriber unless the subscriber has given consent. However, this Regulation refers to the recipient's consent. We consider 'the recipient' to mean the intended recipient. If a household member has an individual email address, then the consent of that individual is required unless the soft opt-in criteria are satisfied. If a household has a household email address (for example, familyname@domainname.com) then the consent of someone whom it is reasonable to believe speaks on behalf of the family is sufficient, unless the soft opt-in criteria are satisfied.

What is 'soft opt-in' (Regulation 22(3))?

This is what the law states:

You may send or instigate the sending of electronic mail for marketing purposes to an individual subscriber where:

- you have obtained the contact details of the recipient in the course of a sale or negotiations for the sale of a product or service to that recipient;
- the direct marketing material you are sending relates to your similar products and services only; and
- the recipient was given a simple means of refusing (free of charge except for the cost of transmission) the use of their contact details for marketing purposes when those details were initially collected and, if they did not refuse the use of those details, at the time of each subsequent communication.

If you satisfy these criteria, you do not need prior consent to send marketing by electronic mail to individual subscribers. If you cannot satisfy these criteria, you must not send marketing by electronic mail to individual subscribers without their prior consent.

How does the ICO interpret 'in the course of a sale or negotiations for the sale of a product or service'?

A sale does not have to be completed for this to apply. It may be difficult to establish when negotiations begin. However, you may continue to market someone by electronic mail:

- if they have actively expressed an interest in buying your products and services; and
- if they have not opted out of further marketing of that product or service or similar products and services when their details were collected (despite being offered the opportunity to do so); and
- unless and until they opt out of receiving such messages at a later date (despite being offered the opportunity to do so in each communication).

We do not consider that 'negotiations for the sale of a product or service' includes the use of cookie technology to identify someone's area of interest when they are browsing your website. Unless they have expressly communicated their interest to you by, for example, asking for a quote, no 'negotiations' can be said to have taken place for the purpose of these Regulations.

As another example, if you are a national retailer and someone emails you asking if you are going to open a branch in their town, the expected response would be 'yes' with details, or 'no', perhaps with details of your other stores in that area. This query does not do any of the following:

- form part of a negotiation for the sale of a product or service;
- form an invitation to you to send the person further information about your products or services;
- indicate consent to receive further promotional emails from you.

You could send a person emails promoting your products and services if they:

- expressly invited you to;
- consented to your suggestion that you send them promotional emails; or
- did not object to receiving emails during a sale or negotiations for a sale.

How does the ICO interpret 'similar products and services'?

We believe the intention of Regulation 22 is to ensure someone does not receive promotional material about products and services they would not reasonably expect to receive. For example, someone who has shopped online at a supermarket's website (and has not objected to receiving further email marketing from that supermarket) would expect at some point to receive further emails promoting other goods available at that supermarket.

A recipient can opt out if they think a company has gone beyond the boundaries of what they would reasonably expect that company to do – something most responsible marketers will be keen to avoid. So for the time being we will focus in particular on failures to comply with opt-out requests. We will continue to monitor how far marketers take account of the reasonable expectations of individual subscribers.

Regulation 22 does not spell out our obligation to respect an opt-out request from individual subscribers. Does this mean we don't have to comply with such requests?

In our view, if you can send marketing by electronic mail to individual subscribers only if they have provided prior consent, this implies the option to withdraw that consent at a later stage. We would quote the inclusion of the phrase 'for the time being' to support our view. We will take enforcement action against companies in the UK jurisdiction who persistently fail to comply with opt-out requests from individual subscribers.

Surely SMS marketing can't be subject to the same rules as conventional email – after all, the standard mobile phone screen can only hold 160 characters.

The practical limitations of standard mobile screens do not mean marketers can ignore the rules. You can give information about the marketing you intend to do before actually sending a marketing message or even before you collect the mobile number in question. For example, in an advert, or on a website where the recipient signs up for the service.

Assuming the recipient has clearly consented to receiving messages, each message will have to identify the sender and provide a valid suppression address. Originally, we took the view that only a postal or email address would satisfy this Regulation. We were concerned that 'pay as you go' mobile phone users may not

have a permanent record of any opt-out message they had sent (as opposed to an itemised bill available for users of contract phones which would, at the very least, be proof that a message of some kind had been sent). Given widespread use of 'pay as you go' mobile phones, particularly by children, we were concerned that 'pay as you go' users would not be able to present a strong case to us (or to a court if they sought to pursue an action for compensation) due to a lack of evidence showing they had asked the marketer to stop and that request was being ignored.

Many marketers have said that people are less likely to bother writing a formal letter and it would be easier for individuals if they could text an opt-out to a short code number at the bottom of a message. This would be more consistent with our approach regarding valid addresses for emails.

So we are now prepared to allow the use of short codes as a valid address, provided the sender ensures that:

- they clearly identify themselves in the message (for example, 'PJ Ltd');
- using the short code does not incur a premium-rate charge; and
- the short code is valid.

If you use a short code as a valid address, we suggest you use the format 'PJLtd2STOPMSGSTXT'STOP'TO (then add a 5-digit short code)'.

Marketing messages that claim to be from 'a good friend' or from 'someone who fancies you' and so on, are unlikely to comply with the Regulations if the company whose goods and services are being promoted, for example, the dating agency, does not clearly identify itself at some point in the message.

Do we have to screen against the TPS if we are sending unsolicited marketing by text, picture or video messages?

No. TPS registration indicates a general objection to receiving live marketing calls. Text, picture and video messages are defined as 'electronic mail' under the Regulations. They should not be sent without the prior consent of the individual subscribers unless the soft opt-in criteria are satisfied. So you do not have to screen against the TPS because you should already have established prior consent or satisfied the 'soft opt-in' criteria.

However, you must make sure you identify yourself in any text, picture or text messages you send and provide a valid address to which recipients can send an opt-out request. If you are sending the message on a soft opt-in basis, you must provide a simple means of refusing further messages that is free of charge except for the cost of transmitting the refusal. You will not satisfy this obligation if you only supply a premium-rate or national-rate number in these circumstances.

We will collect email addresses or mobile phone numbers as part of a competition. Could this be considered as being ‘in the course of negotiations for the sale of a product and service’?

It depends – on the context and on what you tell the person when you collect their details. If a competition is part of an inducement to raise interest in a product or service, it could be argued that this forms part of the negotiations for a sale. However, if you are unclear about what you will do with someone’s email address or mobile phone number when you collect those details, or if you are clear but your reasons are not readily accessible, you are less likely to be able to rely on the ‘soft opt-in’. If you have collected someone’s name with their email address or mobile phone number (or both) and you have not been clear about what you are going to do with that information, you may also breach [the first data protection principle](#).

Third-party electronic mailing lists

Do we always have to obtain any consent or invitation to market by electronic mail directly from the sender? If so, does this mean we can never use bought-in or rented lists?

Despite our view about overriding consent, the Regulations do not expressly rule out obtaining consent through a third party. However, if you are buying or renting a list from a broker, you will need to seek assurances from them about the basis on which the information was collected.

It is difficult to see how third-party lists can be compiled and used legitimately except where the individual subscriber expressly invites (solicits) marketing by electronic mail. This is because you may only send unsolicited marketing to an individual subscriber who has ‘previously notified the sender that they consent for the time being to such communications being sent by, or at the instigation of, the

sender.’ (Regulation 22(2) applies). Arguably, you may obtain a person’s consent through a third party, but a lot will depend on the clarity and transparency of the information that third party gave the intended recipient when it collected their contact details.

If we buy in or rent a list, can we use it?

We cannot see how the soft opt-in criteria could be satisfied with bought-in lists, even if you have an existing relationship with the intended recipient. This is because you can only satisfy the soft opt-in criteria if you, not someone else, collected the electronic mail contact details ‘in the course of a sale or negotiations for a sale.’ (Regulation 22 (3) (a) applies). If you didn’t collect that email address or mobile number yourself, then you can’t rely on the relaxation of the strict prior consent rule.

So if you wish to buy in or rent a list from a third party, you may only use it if the intended recipient has actively consented to receiving unsolicited messages by electronic mail from third parties. The following is a list of scenarios that may apply to a bought-in or rented list. It is not a complete list.

1) List of individual subscribers who have invited contact from third parties on a particular subject

You may send marketing material by electronic mail to contacts on this list provided that:

- this person has not already sent an opt-out request to you;
- you do not conceal your identity when you contact them; and
- you provide a valid contact address for subsequent opt-out requests.

Given individuals’ increased caution over disclosing their contact details to third parties for marketing purposes, you should seek assurances that these are genuine invitations for contact from anyone on a particular subject, as opposed to scenarios 2 or 3 below.

For example, you could use such a bought-in or rented list if the contact details were collected from recipients who had ticked a box next to wording such as:

'I want to receive emails from other companies that offer gardening products. Please pass my email address to them so they can contact me.

2) List of individual subscribers who have invited contact from third parties on unspecified subjects

You may send marketing material by electronic mail to contacts on this list provided that:

- this person has not already sent an opt-out request to you;
- you do not conceal your identity when you contact them; and
- you provide a valid contact address for subsequent opt-out requests.

Given individuals' increased caution over disclosing their contact details to third parties for marketing purposes, you should seek assurances that these are genuine invitations for contact from anyone on any subject, as opposed to scenario 3 below. For example, you could use such a bought-in or rented list if the contact details were collected from recipients who had ticked a box next to wording such as:

'I want to get emails from other companies about their online offers. Please pass my email address to them so they can contact me.

3) List of individual subscribers who have consented to receiving unsolicited marketing material by electronic mail from third parties on a particular subject (that is, a list compiled on an opt-in basis)

You may send marketing material by electronic mail to contacts on this list provided that:

- this person has not already sent an opt-out request to you; you do not conceal your identity; and
- you provide a valid contact address for subsequent opt-out requests.

Given individuals' increased caution over disclosing their contact details to third parties for marketing purposes, you should seek assurances on the accuracy of such a list.

For example, you could use such a bought-in or rented list if the contact details were collected from recipients who had ticked a box next to wording such as:

'If you'd like us to pass your email address onto other organisations working to protect the environment, tick here.

4) List of individual subscribers who have consented to receiving unsolicited marketing material by electronic mail from third parties on unspecified subjects (that is, a list compiled on an opt-in basis)

You may send marketing material by electronic mail to contacts on this list provided that:

- this person has not already sent an opt-out request to you;
- you do not conceal your identity; and
- you provide a valid contact address for subsequent opt-out requests.

Given individuals' increased caution over disclosing their contact details to third parties for marketing purposes, you should seek assurances on the accuracy of such a list.

For example, you could use such a bought-in or rented list if the contact details were collected from recipients who had ticked a box next to wording such as:

'We'd like to pass your email address to other companies so that they can send you on-line offers too. If you agree to this, tick here.

It may be difficult to demonstrate that the intended recipients have 'notified the sender' and a lot will depend on the wording of any statement given to individuals when their information was collected. So, if the recipient has not expressly invited marketing messages, you will need to consider whether any list you use forms a list of notifications of consent to you, the sender. Also, the older the list you buy or rent, the less likely it is that contacts on the list will respond positively to marketing messages. It may even damage the reputation of your business to send poorly targeted unwanted marketing messages. You have a general obligation to ensure the recipient is provided with a valid address for opt-out requests in every message. If you receive an opt-out request, you must ensure you suppress that individual's details immediately. We will pay particular attention to companies that fail to respect opt-out requests.

Can we advertise the products and services of third parties by electronic mail?

If you are offering a 'host mailing' service, you are not disclosing your mailing list to a third party but you are willing, for a fee, to promote their goods and services alongside yours. It is unlikely you could send such messages on a soft opt-in basis because they are not your similar products and services. However, you could send such material on a clear 'opt-in' basis, provided you make clear that you and not the third party are the sender.

Can we pass our list of email addresses or mobile numbers on to a third party for them to use for marketing purposes?

If the email addresses or mobile numbers in question are those of individual subscribers, the third party will not be able to use them to send unsolicited marketing material unless the subscriber has consented to receiving it from that third party (that is, 'the sender'). You must make clear who you are proposing to pass the details to and what sort of products and services they will be offering.

For example, a positive response to a question such as 'We would like to pass your details to specially selected third parties so they can send you more information about holidays in America. Do you agree to this?' is likely to be enough to allow third parties to use those contact details for promoting holidays in America by electronic mail.

A phrase such as 'We will pass your details to third parties unless you write to us and tell us you don't agree' will not be enough. You should not use contact lists that have been obtained like this. Only the individual should decide what happens to their electronic contact details. You must not disclose an individual's contact details to third parties for their marketing purposes unless that individual actively consents to this.

Group companies and trading names

How do the rules on marketing by electronic mail apply to marketing by different companies within a group of companies?

If you disclosed individual subscribers' contact information within your group in line with existing data protection rules before 11 December 2003 and those other group companies had already used that information before that date and have continued to use it and

not received an opt-out request, then those other group companies may still use that contact information as long as further opt-out opportunities are given with every subsequent message.

After this date and in the future, you must, as a minimum, ask individuals whether they consent to receiving unsolicited marketing by electronic mail from other group companies when you collect their contact details. Online, you could provide a link listing those group companies. You may even want to consider providing separate opt-in opportunities for each company on that list to give the individual greater choice and to target your group's marketing more efficiently. Another option may be to provide an opportunity for the individual to invite (solicit) contact from other companies in the group.

Our company has a number of different trading names; surely an opt-in for one of the trading names is an opt-in for all because there is only one legal entity?

If you trade under several different names, particularly where those names are strong brands, you should not assume that a customer who agrees to receive mailing from one trading entity is agreeing to receive marketing from your other trading entities. Customers may not even be aware of any connection between different trading names. Under the Data Protection Act, if you are collecting personal data, you will need to ensure the different entities are clearly explained to your customers. You would need to ensure they know that they will receive unsolicited marketing from all your trading names when they opt in to receiving marketing from you. Similarly, when an individual opts out of receiving unsolicited marketing from one of your trading names, this opt-out applies to all your trading names, unless they make it clear otherwise.

If you are collecting information on a soft opt-in basis, you may have considerable difficulty satisfying the similar products and services criteria if you want to send further unsolicited marketing relating to your full range of trading names. You could avoid this by providing an opportunity for the individual to invite contact from the wide range of trading names within the company.

Business to business

How do the Regulations apply to business-to-business marketing by electronic mail?

Your obligations are as follows:

- You must not conceal your identity when you send, or instigate the sending of, a marketing message by electronic mail to anyone (including corporate subscribers); and
- you must provide a valid address to which the recipient (including corporate subscribers) can send an opt-out request (Regulation 23 applies).

Only individual subscribers have an enforceable right of opt-out under these Regulations. This is where that individual withdraws the consent they previously gave to receiving marketing by electronic mail (that consent only being valid for the time being (Regulation 22(2) applies)). Corporate subscribers do not have this right.

Recipients who are corporate subscribers do not have an enforceable opt-out right under the Regulations. But where your sending of marketing material to the employee of a company includes processing their personal data (that is, you know the name of the person you are contacting), then that individual has a fundamental and enforceable right under Section 11 of the Data Protection Act to ask you to stop sending them marketing material.

In our view, it makes no business sense to continue sending marketing material to a business contact who no longer wishes to hear from you. Arguably, by failing to respect a business-to-business opt-out request you may appear indifferent to your commercial reputation.

How do these Regulations apply to unsolicited marketing material sent by electronic mail to individual employees of a corporate subscriber if that material promotes goods and services that are clearly meant for their personal or domestic use?

The 'Spam' report of an Inquiry by the All-Party Parliamentary Internet Group (APPIG) recommended that the Information Commissioner set out clear guidance as to how business-to-business communications are to be distinguished from messages intended for individual subscribers. This recommendation was prompted by an observation that an invitation to buy Viagra, sent to the sales address of a shipping company, could only be interpreted

as being sent to an individual, since it would be of no business relevance.

The problem is that the 'opt-in' and soft opt-in rules do not extend to sending marketing emails to corporate subscribers. In the example above the subscriber will be the shipping company, because that is the person who is party to a contract with a provider of public electronic communications systems. So this means that even an email addressed to an individual in the company will not be covered by the Regulations, although that email may be subject to the DPA, and an opt-out request under Section 11 of the DPA could be issued. For the purposes of the Regulations, it is irrelevant that an email sent to a corporate subscriber's address is obviously aimed at an individual because it promotes a product that is for personal or domestic use.

The Regulations simply do not cover emails sent to a corporate subscriber, except that you must identify yourself and to provide contact details. However, such emails are likely to be covered by the individual's right to object to direct marketing under the Data Protection Act.

We understand that the Committee of Advertising Practice (CAP) Code restricts the sending of such emails to corporate email addresses. For more on the CAP Code visit their website www.cap.org.uk.

How do the Regulations apply to sending text, picture and video messaging to mobile phones that are supplied to individual employees by corporate subscribers?

The law applies in exactly the same way as it does to sending emails to corporate subscribers.

Electronic mail marketing to partnerships

How do the Regulations apply to sending marketing messages by electronic mail to partnerships?

Under these Regulations, a non-limited liability partnership in England, Wales or Northern Ireland is an individual subscriber. This means that such a partnership (which may consist of several individuals and which may have a large number of employees) is given the same protection under these Regulations as a residential

subscriber or a sole trader. This protection is not available to limited liability partnerships, to Scottish partnerships or to corporate subscribers that include small- and medium-sized limited companies.

Strictly speaking, you must get prior consent to send emails to any email address used by an unincorporated partnership, unless the soft opt-in criteria apply. This may be the generic contact email address of the partnership, for example, mail@partnershipname.com or it may be the separate email addresses used by individuals (partners, associates, other employees) working at that partnership.

This issue was debated during the Department of Trade and Industry's consultation exercise before these Regulations were implemented.

What does this mean in practice?

Strictly speaking, the partnership could be viewed as the commercial equivalent of a large household. Yet we recognise there may be circumstances when the wishes of the subscriber, that is, the unincorporated partnership (which is legally responsible for charges incurred on its lines) might override the wishes of the employee. For example, an employer may insist that an employee keeps in regular contact with conference organisers. The employer's wishes for unsolicited emails from conference organisers would override the wishes of the employee.

However, if someone working at the partnership consents to receiving unsolicited marketing material from the organiser, this does not mean everyone working at the partnership has consented to it.

Marketers must also remember that where they know the name of the person they want to contact, that person's contact details must be processed in accordance with the eight data protection principles of the Data Protection Act. For example, where the Act applies, all individuals have a fundamental opt-out right under Section 11.

Who can give consent on behalf of individuals working at a partnership?

If you are targeting an individual working at a partnership, you must make sure you obtain the consent of the individual (or someone who can be reasonably assumed to be entitled to give consent on that individual's behalf, for example, a secretary or assistant) before sending unsolicited electronic mail to that individual, unless the soft opt-in criteria apply.

Partnerships may wish to make sure their key frontline staff, for example, switchboard operators, receptionists, administrators, secretaries are informed of any office policy regarding the disclosure of employee contact details.

Individuals employed by partnerships must remember that for their work email address and mobile phone, it is ultimately their employer's consent choices that take precedence.

Who can give consent on behalf of the partnership?

You must make sure you have obtained consent from someone working for that partnership who it is reasonable to assume has the authority to give such consent. Partnerships may wish to make sure their key frontline staff, for example, switchboard operators, receptionists, administrators, secretaries, are informed of any office policy regarding the disclosure of office contact details.

Electronic mail marketing to sole traders

How do the Regulations apply to sending marketing messages by electronic mail to sole traders?

Under the Regulations, sole traders are also individual subscribers. That said, we have recognised in earlier enforcement that marketers may have difficulty distinguishing sole traders from small limited companies, particularly where a sole trader's contact details are available in business directories. However, you should do your best to ensure you do not send marketing messages by electronic mail to sole traders, in breach of the Regulations. For example, you can check free of charge on the [Companies House website](#) whether or not a trading entity is a limited company.

Charities, political parties and not-for-profit organisations

We are a charity, political party, or not-for profit organisation; can we take advantage of ‘soft opt-in‘?

Only if you are promoting commercial goods and services, for example, those offered by your trading arm. We recognise that this disadvantages you and we raised this point in our response to the consultation by the Department of Trade and Industry in advance of these Regulations. However, the EU Directive from which these Regulations are derived specifies that the soft opt-in rules on marketing by electronic means apply to commercial relationships.

You may wish to look again at the wording of your data protection and privacy statements so that you are asking a person to actively ‘invite’ promotional information from you through electronic mail. As outlined above, there is a difference between someone actively soliciting promotional material by electronic mail and consenting to receiving any promotional material you choose to send them by electronic mail (unsolicited marketing material). One option would be to ask them if they consent to receiving unsolicited marketing material.

You must still identify yourself and provide a valid address for opt-outs in each electronic mailing.

Viral marketing

How do the rules apply to 'viral marketing'?

So-called 'viral marketing' is where:

1. you ask a person to send the original marketing message to a friend or friends; or
2. you ask a person to give you their friends' contact details.

This process may or may not be incentivised in some way.

Some companies mistakenly see these options as ways of avoiding the prior consent rule.

We recognise that your customer might recommend a good deal to a friend, whether you prompt them to or not. We also know that a customer may check with their friends first before passing their details to you. People tend to do so when acting in good faith and in the interests of their friends.

Arguably, in scenario 1 you are encouraging one of your customers to break the law to promote your name (send an unsolicited message to an individual subscriber without prior consent).

Clearly, this would be a bad way to promote your name and your products and services and we strongly advise you to tell your customers only to forward emails to people they know would be happy to receive them. If you give them an incentive to do so, there is a strong argument that you are the 'instigator' of the message; in other words, they wouldn't forward emails in this way without the promise of a reward from you. Remember that it is the instigator of the message who is liable for sending that message. Anyone who allows their line to be used to break the law (your customer who is passing your message on) may also be liable in this scenario.

In scenario 2, you will be sending a message to someone who you assume has consented, through a third party (the friend who passed on their details to you), to receiving messages from you. Under the legislation, you are liable for any messages sent to email addresses or mobile numbers obtained using scenario 2.

As with all third-party electronic mailing lists, you may not use this list unless you are satisfied that the recipient has notified you that they consent to receiving such messages from you. So you should

ask your customer to confirm they have the consent of the individuals whose details they are passing on. You should also check that the recipient hasn't already asked you to suppress their details. If those contact details appear on your suppression list, you may have cause to question whether consent has been obtained at all. Finally, you should also tell your customer that you propose to let those individuals know how you got their details. The Data Protection Act would not prevent you doing this. This is particularly important if you propose to offer your customer incentives for passing their friends' details to you.

Even if you do not offer incentives to achieve scenarios 1 or 2, you should bear in mind that one of your customers could use 1 or 2 maliciously. For example, someone could give the contact details of another person to a whole range of companies as a prank. Although it is hard to see how you are directly responsible for the malicious activities of one of your customers, you should bear in mind that, at the very least, the recipient may forever associate your organisation's name with that unpleasant experience. In any event, you should make sure you immediately suppress the recipient's contact details to avoid further distress.

Appending email addresses or mobile numbers

We have a list of established customers who haven't given us their mobile number or email address but those details have appeared on an opt-in list we have bought in. We'd like to start contacting them online or by text message. Can we do so?

The intended recipient has, for reasons of their own, not started doing business with you online or by text message. You may be able to argue that this customer has notified you through a third party that they are happy to hear from you by email or text message. But you should consider the possible effects of such an 'out of the blue' message on your relationship with that customer. A frequent comment in complaints we receive is:

'Where did they get my email address or mobile number from? I certainly didn't give it to them.'

You may wish to send a 'low-key' message explaining where you have got their details from and politely asking whether they are happy to hear from you in this way. You could not assume consent if they don't respond.

Loyalty schemes

**We operate a loyalty scheme for our own products and services.
How do the Regulations apply here?**

If someone participates in a loyalty scheme, the least they can expect from you is an update on how many points or vouchers they have earned. In our view, under the soft opt-in rule, you may send them further information about other incentives that are available under the scheme, until they opt out of receiving it. Once they have opted out, you should not send such further information until they opt back into receiving it again.

**We operate a loyalty scheme in partnership with other companies.
A lot of information is transferred across the scheme and the partners do not necessarily offer similar products and services.
How do the Regulations apply here?**

We assume you have collected any contact information you already have in line with your obligations under the Data Protection Act.

If you are collecting information to conduct marketing exercises electronically, you may need to re-read the data protection and privacy wording of your application form. You must make sure individuals are fully aware of the nature of the promotions you propose to send. The least an individual can expect is an update on how many points or vouchers they have earned.

In our view, under the soft opt-in rule, you may send them further information about other incentives offered by all the participating companies in the scheme, until they opt out of receiving it. If there are several partners in a loyalty scheme, you may find it easier to provide an opportunity for the individual to invite (solicit) further marketing contact from each partner if those partners propose to contact the individual independently of this scheme.

Pan-European marketing

We plan to conduct a pan-European marketing campaign. Which jurisdiction's rules do we need to comply with?

You should also comply with the laws in other countries. However, you should bear in mind that when implementing the EU Directive, each member state could decide whether the rights given to individual subscribers should extend to corporate subscribers. Some jurisdictions have chosen to do so to a greater extent than the UK. You may create a bad impression of your business if you don't respect the laws of the country where you are sending your messages.

We cannot offer guidance on how to comply with the legislation of other countries and you should seek your own legal advice if you wish to conduct pan-European marketing campaigns.

Marketing by more than one medium

We collect individuals' addresses, telephone numbers, mobile numbers and email addresses for marketing purposes on a paper form. We have limited room on the form and we have to provide other information to comply with other legislation. What is the minimum amount of information we have to provide to comply with data protection rules?

You do not need to provide lots of legal wording to comply with your data protection obligations. If you are collecting information to market someone using a variety of media, the simplest method is to adopt the highest standard and apply it even where you do not need to.

Under the Data Protection Act, the bare minimum you are obliged to tell people is who you are and what you plan to do with their information, including any unexpected uses, such as processing for marketing purposes and disclosures to third parties. Because you plan to market by electronic means, you also need to provide consent options. The highest standard would be to give the individual the opportunity to solicit information from you, for example:

'Please contact me by post , by telephone , by text/picture/video message with further information about your products and services (tick , by email as applicable).'

However, if you use this wording, you may not send marketing material to them by post, telephone, text message or email unless the individual ticks the box to invite further contact from you.

2

Other rules

Security of services

An electronic communications service is defined in the Communications Act 2003 as 'a service consisting of, or having as its principal feature, the conveyance by means of an electronic communications network of signals, except in so far as it is a content service'. A public electronic communications service is any such service that is provided so as to be available for use by members of the public.

A provider of a public electronic communications service must take appropriate technological and organisational measures to safeguard the security of its services. An appropriate measure is one that is proportionate to the risks it would safeguard against, taking account of the state of technological development and the cost of implementing the measure.

These measures must at least:

- a) ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;
- b) protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure; and
- c) ensure the implementation of a security policy with respect to the processing of personal data.

These provisions are similar to the obligations on a data controller under the [seventh data protection principle](#).

Regulation 5(2) states that, if necessary, such measures should be taken by the electronic communications service provider with the provider of the electronic communications network. An electronic communications network is defined in the Communications Act 2003 as:

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

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

(i) apparatus comprised in the system;
(ii) apparatus used for the switching or routing of the signals;
and

(iii) software and stored data'.

The Regulation aims to ensure reasonable co-operation between service and network providers.

Security risks

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

- the nature of the risk;
- any appropriate measures the subscriber may take to safeguard against the risk; and
- the likely costs to the subscriber involved in taking such measures.

They must provide this information to the subscriber free of charge except for any nominal costs the subscriber may incur while receiving or collecting the information, for example through downloading an email. Security is not to be regarded as compromised if:

- a disclosure is made in connection with [the prevention or detection of crime](#);
- a disclosure is made for [the purposes of criminal proceedings](#);
- the Secretary of State makes an order to intercept any communications as may be specified in a warrant; or
- any disclosure is made in the interests of national security or in response to a court order.

Personal data breach notification

If a personal data breach occurs, the service provider must, without undue delay, notify that breach to the Information Commissioner. The notification must include:

- a) a description of the nature of the breach;
- b) a description of the consequences of the breach; and
- c) a description of the measures taken or proposed to be taken by the provider to address the breach.

In certain circumstances the service provider must also, without undue delay, notify subscribers or users about the breach. This requirement would apply if a personal data breach is likely to adversely affect the personal data or privacy of a subscriber or user but it does not apply if the service provider has demonstrated to the satisfaction of the Information Commissioner that:

- a) it has implemented appropriate technological protection measures which render the data unintelligible to any person who is not authorised to access it, and
- b) that those measures were applied to the data concerned in that breach.

In other cases the notification to subscribers or users must include:

- a) a description of the nature of the breach;
- b) information about contact points within the service provider's organisation from which more information may be obtained; and
- c) recommendations of measures to allow the subscriber to mitigate the possible adverse impacts of the breach.

In cases where subscribers or users have not been notified the Commissioner can require a service provider to do so.

Personal data breach inventory

Service providers are also required to maintain an inventory or log of personal data breaches which includes:

- a) the facts surrounding the breach
- b) the effects of that breach, and
- c) remedial action taken

This inventory must be sufficient to enable the Information Commissioner to verify compliance with the requirements of this regulation.

Audit

The Regulations provide the Commissioner with the power to audit:

- The measures taken by a provider of a public electronic communications service to safeguard the security of that service.
- The compliance of service providers with the data breach notification requirements

See our [statement on how the Commissioner intends to use his powers in this area](#). We will be producing more guidance shortly.

Confidentiality of communications

The law which applies to how you use cookies and similar technologies for storing information on a user's equipment such as their computer or mobile device changed on 26 May 2011. Our [advice on the new cookies regulations](#) sets out these changes and explains what steps you need to take now to ensure you comply.

Regulation 6 covers the use of electronic communications networks to store information or gain access to information stored in the terminal equipment of a subscriber or user. So-called spyware can enter a terminal without the knowledge of the subscriber or user to gain access to information, store information or trace the activities of the user. This Regulation reflects the growing concern about the use of covert surveillance mechanisms online.

However, it is recognised in the Directive that using such devices will not necessarily be harmful or unwarranted. The use of devices such as cookies, for example, has for some time been commonplace and cookies are important to provide many online services. Using such devices is not, therefore, prohibited by the Regulations but they do require that subscribers and users should be given the choice as to which of their online activities are monitored in this way.

Cookies and personal data

Although devices which process personal data give rise to greater privacy and security implications than those which process data from which the individual cannot be identified, the Regulations apply to all uses of such devices, not just those involving the processing of personal data.

Where the use of a cookie type device does involve the processing of personal data, service providers will need to make sure they comply with the additional requirements of the Data Protection Act 1998 (the Act). This includes the requirements of the [third data protection principle](#) which states that data controllers must not process personal data that is excessive. Where personal data is collected, the data controller should consider the extent to which that data can be effectively processed anonymously. This is likely to be particularly relevant where the data is to be processed for a purpose other than the provision of the service directly requested by the user, for example, counting visitors to a website.

Information to be provided

Cookies or similar devices must not be used unless the subscriber or user of the relevant terminal equipment:

- a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and
- b) has given his or her consent.

The Regulations are not prescriptive about the sort of information that should be provided, but the text should be sufficiently full and intelligible to allow individuals to clearly understand the potential consequences of allowing storage and access to the information collected by the device should they wish to do so. This is comparable with the transparency requirements of [the first data protection principle](#).

The Regulations state that once a person has used such a device to store or access data in the terminal equipment of a user or subscriber, that person will not be required to provide the information described and obtain consent (and discussed above) on subsequent occasions, as long as they met these requirements initially. Although the Regulations do not require the relevant information to be provided on each occasion, they do not prevent this.

Responsibility for providing the information and obtaining consent

The Regulations do not define who should be responsible for providing the information and obtaining consent. Where a person operates an online service and any use of a cookie type device will be for their purposes only, it is clear that that person will be responsible for complying with this Regulation.

Exemptions from the right to refuse a cookie

The Regulations specify that service providers should not have to provide the information and obtain consent where that device is to be used:

- for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network; or
- where such storage or access is strictly necessary to provide an information society service requested by the subscriber or user.

In defining an 'information society service' the Electronic Commerce (EC Directive) Regulations 2002 refer to 'any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service'.

The term 'strictly necessary' means that such storage of or access to information should be essential, rather than reasonably necessary, for this exemption to apply. However, it will also be restricted to what is essential to provide the service requested by the user, rather than what might be essential for any other uses the service provider might wish to make of that data. It will also include what is required to comply with any other legislation the service provider might be subject to, for example, the security requirements of the [seventh data protection principle](#).

Where the use of a cookie type device is deemed 'important' rather than 'strictly necessary', those collecting the information are still obliged to provide information about the device to the potential service recipient and obtain consent.

Wishes of subscribers and users

Regulation 6 states that consent for the cookie type device should be obtained from the subscriber or user but it does not specify whose wishes should take precedence if they are different. There may well be cases where a subscriber, for example, an employer, provides an employee with a terminal at work along with access to certain services to carry out a particular task, where to effectively complete the task depends on using a cookie type device. In these cases, it would not seem unreasonable for the employer's wishes to take precedence. However, it also seems likely that there will be circumstances where a user's wish should take precedence. To continue the above example, an employer's wish to accept such a device should not take precedence where this will involve the unwarranted collection of personal data of that employee.

Traffic data

Traffic data means any data which is processed:

- to convey a communication on an electronic communications network; or
- for the billing in respect of that communication ('billing data' under the Telecommunications (Data Protection and Privacy) Regulations 1999).

It includes data relating to the routing, duration or time of a communication.

Retention

Data processed to establish communications could potentially contain personal information that should only be stored for limited purposes and retention periods in line with the [second](#) and [fifth](#) principles of the Data Protection Act 1998. The Regulations provide for the protection of individual and corporate subscribers with regard to the processing of traffic data. If such data is no longer needed to transmit a communication, when the communication is terminated, that data must be erased or dealt with in such a way that

- it is no longer personal data, in the case of an individual subscriber; or
- in the case of a corporate subscriber, it is modified so that it is no longer data that would be personal data in the case of an individual.

Data required by the communications network or service provider to calculate the subscriber's bill or for interconnection charges can only be retained until the end of the period during which the bill may lawfully be challenged or payment pursued. In terms of contract law, this would normally mean a limitation period of six years plus appeals applied. However, in the Commissioner's view, this provision merely permits such data to be kept only when circumstances require it, for example, if the bill is challenged during a period when a communications network or service provider would normally retain the data for their own billing purposes. It does not permit the wholesale retention of such traffic data in every case. As mentioned above, the fifth data protection principle states that personal data must not be kept for longer than is necessary for the purpose for which it is processed.

Purposes for processing

Traffic data may be processed only for the restricted purposes outlined in the Regulations.

- **To provide value-added services to the subscriber or user**

A value-added service means any service that requires the processing of traffic data or 'location data' beyond what is necessary to transmit a communication or the billing of that communication – for example, a service that locates the driver of a broken-down vehicle. There is no restriction on the type of service that can be provided, but such processing may only take place with the prior consent of the subscriber or user.

- **To market the service provider's own electronic communications services**

Under the Regulations, the service provider must get the consent of the subscriber or user before they can market their own electronic communications services. Such marketing does not necessarily have to be carried out over the phone and might include, for example, an analysis of a subscriber's usage patterns to provide that subscriber with the best tariff available.

Only the communications provider or a person acting under their authority can carry out this processing. The communications provider has ultimate responsibility for complying with the Regulations about processing traffic data, so they should observe the requirements of the seventh data protection principle. The provisions about contracts are particularly relevant – see the [seventh data protection principle](#). Although the Act applies only to processing personal data, there is nothing to stop service providers imposing such contracts for processing traffic data relating to corporate subscribers.

Consent to process for the above purposes

If traffic data is processed for the above purposes, the prior consent of the subscriber or user of the line or account must be obtained. In the case of a corporate subscriber, it is reasonable for the communications provider to accept at face value the assurances of a person giving consent on behalf of the company, unless the communications provider has reasonable grounds to believe otherwise.

The Regulations do not prescribe how service providers should obtain this consent. However, to obtain valid informed consent, the subscriber or user should be given enough clear information for

them to have a broad appreciation of how the data is going to be used and the consequences of consenting to such use (see the [first principle in the guide to data protection](#)). In light of this, the service provider will not be able to rely on a blanket 'catch all' statement on a bill or a website but must get specific informed consent:

- for each value-added service requested; and
- to market their own electronic communications services.

If, for example, a communications provider offers a value-added service using a third party, then in the interests of transparency the person who will be regarded as responsible for providing that service should get the consent to process for this purpose. Whether this will be the service provider, the third party or both will depend on the circumstances. If the communications provider offers a value-added service jointly with a third party, the user should be made aware of both parties. The point is that the way a service is provided should be consistent with the expectations of the subscriber or user. If the user gives consent to one party to provide a particular service, they should not then be surprised when they are contacted by another party about that service.

The Regulations also specifically require that the subscriber or user is provided with information about the types of traffic data to be processed, and the duration of such processing.

The subscriber or user may withdraw any such consent given to process related traffic data at any time.

General provisions on the processing of traffic data

As well as the above two purposes, the Regulations allow the processing of traffic data by a public communications provider in the course of its business for the following purposes:

- To manage billing or traffic.
- To handle customer enquiries.
- To prevent and detect fraud.

The processing of traffic data must be restricted to what is necessary for these activities and by people acting under proper authority.

Disputes

The Regulations do not prevent providing traffic data to a person who has been given statutory authority to resolve disputes, for example, Ofcom.

Location data

Location data means any data processed in an electronic communications network or by an electronic communications service that indicates the geographical position of the terminal equipment of a user of a public electronic communications service, including information relating to:

- the latitude, longitude or altitude of the terminal equipment;
- the direction of travel of the user; or
- the time the location information was recorded.

Regulation 14 does not apply to the processing of traffic data discussed in Traffic data.

Restrictions on processing

Location data relating to a subscriber or user of a public electronic communications network may only be processed if:

- the subscriber or user cannot be identified from that data; or
- where it is necessary to provide a value-added service with the consent of the relevant user or subscriber.

Location data must only be processed by the communications provider in question; the third-party provider of the value-added service; or a person acting on behalf of either of the above. The processing of location data to provide a value-added service must be restricted to what is necessary for those purposes.

The communications provider has ultimate responsibility for complying with the Regulations about processing location data, so they should observe the requirements of the seventh principle of the Data Protection Act, particularly for processing personal data carried out by a data processor.

Although the Act applies only to processing personal data, there is nothing to stop service providers imposing such contracts for processing location data from which an individual cannot be identified.

Consent to process

The public communications provider must get the prior consent of the user or subscriber to process location data to provide a value-added service (if the user or subscriber can be identified from that data). Before getting consent, the communications provider must give the user or subscriber the following information:

- the types of location data that will be processed;
- the purposes and duration of the processing of those data; and
- whether the data will be transmitted to a third party to provide the value-added service.

In the case of a corporate subscriber, a person making decisions on behalf of the company is likely to be able to give consent, unless the communications provider has reasonable grounds to believe otherwise.

The Regulations do not prescribe how service providers should get this consent. However, to get valid informed consent, the subscriber or user should be given enough clear information for them to have a broad appreciation of how the data is going to be used and the consequences of consenting to such use (see the [first principle in the guide to data protection](#)).

In light of this, the service provider will not be able to rely on a blanket 'catch all' statement on a bill or a website but must get specific informed consent:

- for each value -added service requested; and
- to market their own electronic communications services.

If a public communications provider offers a valued-added service with a third party, then in the interests of transparency the person who will be regarded as responsible for providing the service should get the consent to process location data for such a purpose. Whether this will be the service provider or the third party will depend on the circumstances. The point is that the way a service is provided should be consistent with the expectations of the subscriber or user.

If the user consents to one party to provide a particular service, they should not then be surprised when they are contacted by another party about that service.

If a user or subscriber has given informed consent to the processing of location data, they can withdraw that consent at any time – the communications provider should make them aware of this. The user or subscriber should also be given an opportunity to withdraw their consent each time they connect to the network or on each transmission of a communication.

The Regulations state that the service provider must give the user the opportunity to permanently withdraw consent. But there is

nothing in those Regulations preventing the service provider also offering the user the chance to suspend their consent for a limited, specified period. If the user chooses to accept such an option, there is similarly nothing to prevent the provider reactivating their consent after that time has elapsed – provided they made it clear to the user when the user chose to suspend their consent for a limited period that this would happen.

Itemised bills

A subscriber is entitled, on request, to receive bills that are not itemised. This recognises the fact that itemised bills may put at risk the privacy of users even though they are also useful for subscribers to verify the amount of the bill.

In exercising functions under Chapter 1 Part 2 of the Communications Act 2003, Ofcom has a duty to reconcile the rights of subscribers receiving itemised bills with the rights to privacy of calling users and called subscribers. It may do this, for example, by making sure that sufficient alternative ways to make calls or pay for calls are available to such users and subscribers, to facilitate anonymous calls in particular. The Telecoms Directive suggests this may be achieved by providing anonymous pre-paid telephone cards. Pre-paid phones and cash payphones are also relevant in this context.

Calling or connected line identification (CLI)

The Regulations deal with the prevention and restriction of calling or CLI, for both incoming and outgoing calls.

The Regulations cover 'call return' and 'call display' facilities, such as the display on certain telephone equipment that alerts the subscriber to the identity of the caller before the connection is made, and the 1471 service. CLI services are governed by an Ofcom-published code (the Code of Practice for Network Operators in relation to Customer Line Identification Display Services and Other Related Services). Following the Code will help ensure compliance with the Regulations.

Outgoing calls

The communications service provider must ensure that:

- a user originating a call, has a simple way of preventing the identity of the calling line for that call appearing on the connected line;
- a subscriber has, in relation to their line and all calls originating from that line, a simple way of preventing the identity of their line appearing on any connected line.

You should note the distinction between the user and the subscriber: Users only have the right to block their identity in relation to a particular call, whereas subscribers have the right to block their identity in relation to their line and all calls originating from that line. In either case, users or subscribers must not be charged for this facility.

Incoming calls – preserving the anonymity of the caller

For incoming calls, the communications service provider must ensure the called subscriber has a simple way of preventing the identity of a calling line appearing on the connected line. There must be no charge for reasonable use of the facility.

This is particularly likely to be used where the caller's anonymity is guaranteed, such as on helplines like the Samaritans, Alcoholics Anonymous or police information lines.

Incoming calls – preserving the anonymity of the called line

Under the Regulations, the relevant telecommunications service provider must ensure the subscriber to whose line a call is

forwarded has a simple way of preventing, without charge, the identity of the connected line appearing on any calling line. This facility preserves the privacy of someone to whose line a call is forwarded, where the connected line has a different number from the number called. This is a facility used by many businesses and medical practices; for example, a call to a doctor's surgery after hours may be forwarded to the number of a doctor or locum service. This facility will enable the number of the line to which the call is forwarded to remain private.

Anonymous incoming calls – call rejection

If a caller has prevented the identity of the calling line appearing on the connected line, the called subscriber must be given a simple way of rejecting those calls. The Regulations do not mention charging for this facility.

The current technical standards do not distinguish between a situation where CLI has been deliberately withheld and where CLI is unavailable, for example, for incoming international calls. So a subscriber who chooses not to receive calls with CLI withheld may also not receive all international calls.

If calls are rejected because the CLI has been withheld, the caller should receive an automatic message explaining why the call has not been connected and how to lift the block on CLI to enable the call to go through.

The Telecommunications (Data Protection and Privacy) Regulations 1999 obliged service providers to give called parties a simple way of rejecting a call where the CLI has been withheld. The Commissioner understood at that time that there were technical problems associated with offering a fully automatic call-rejection system to all subscribers. In the case of most mobile phone subscribers, the only way to reject a call made with CLI withheld was not to answer, or to press 'line busy'. On some networks this resulted in the call being transferred to the subscriber's voice mail.

The Privacy and Electronic Communications (EC Directive) Regulations 2003 contain a clearer requirement to provide automatic call rejection. The Commissioner's current understanding, based on Ofcom's advice, is that as the relevant Regulation applies to the automatic rejection of voice calls only, automatic call rejection can be implemented relatively simply by using a recorded voice message to explain what has happened.

Duty of an electronic communications service provider to advise that CLI is available

A communications service provider who offers CLI facilities must take all reasonable steps to publicise that they do so and to explain the consequences of the Regulations about CLI.

Malicious or nuisance calls

There are provisions to help trace malicious or nuisance calls where a subscriber has notified the relevant communications service provider that such calls on their line should be traced.

In these situations, the communications service or network provider, as appropriate, may override anything done to prevent the identity of the calling line appearing on the subscriber's line, if the provider in question thinks it necessary to trace malicious or nuisance calls.

For these calls, the provider, as appropriate, may hold and make available to a person with a 'legitimate interest' in this information, data containing the identity of a calling subscriber. Sometimes the service or network provider may not be able to reveal the identity of the person making the call, but merely the location from which the calls were made. For example, it would be difficult for a telecommunications service provider to provide the identity of a caller using a number attached to an unregistered pre-paid mobile.

It is important to distinguish a person with a 'legitimate interest' under the Regulations, from the reference to 'legitimate interests' referred to in paragraph 6 of Schedule 2 of the Act. The Commissioner has given a wide interpretation to 'legitimate interests' under the Act. It relates to the 'legitimate interests pursued by the data controller or by the third party ... to whom the data are disclosed'. In the Regulations 'a person with a legitimate interest' is not defined, but it probably includes the police or other law enforcement body and even the subscriber himself or herself.

However, there may be cases where a service provider would wish to exercise some caution with a request for information about the identity of a calling subscriber. For example, if the service provider is not satisfied that the calling subscriber has abused the service in the way referred to in Regulation 15, it may choose not to release that information to the called subscriber. However, it may not rule out releasing it to the police if any further request provides an extra level of reassurance.

Calls to emergency services

CLI cannot be excluded from all outgoing calls using the national emergency call number 999 or the single European emergency call number 112. This is to enable the emergency services to deal with such calls and easily identify the caller's location.

The restriction on processing of location data under Regulation 14(2) shall be disregarded.

Termination of unwanted automatic call forwarding

If calls are being forwarded as outlined in incoming calls – preserving the anonymity of the called line, the subscriber has the right to ask the relevant communications service provider to stop that service without unavoidable delay. Any other network or service provider must also comply with all reasonable requests for this.

Charges

Some of the Regulations require a facility to be provided free of charge. Where the Regulations do not mention that a charge may be made for a service, then if a person must provide a facility, or ensure it is provided, they can ask for a reasonable charge unless there is an indication to the contrary.

Directories of subscribers

The Regulations contain provisions relating to directories of subscribers to publicly available electronic communications services, which are made available to the public or to a section of the public. We interpret this to mean any directory whose sole or main function is to list the phone, fax or email contact details of network subscribers, where this information can be obtained by any person who has a minimum amount of information (such as name and approximate address). We take the view that the Regulations do not apply to other forms of directory (for example trade directories) where electronic communications are not the sole or main part. This means the Regulations cover only directories of the electronic contact details of residential and business subscribers.

It has been suggested that the Regulations about directories may cover a WHOIS 'lookup' service. From the description above, it is difficult to see that they will do so, as the main purpose of WHOIS is to give the searcher information about the identity of the person who operates a website (a person who may well not be party to a contract with the WHOIS provider). For now, the Commissioner intends to interpret Regulation 18 as applying only to directories of phone numbers (including mobile phone numbers), fax numbers and email addresses.

The Regulations make it clear that these directories may be in printed or electronic form or may be those relied on by a directory enquiry service, for example the '118' services. The provisions do not apply to any edition of a directory first published before 11 December 2003.

Individual subscribers

The personal data of an individual subscriber must not be included in a directory unless that subscriber has, free of charge, been:

- informed of the directory's purposes by the collector of the personal data; and
- given the opportunity to decide whether the personal data that the directory producer considers relevant should be included in the directory.

The first requirement outlined above is in line with the fair processing requirements of the Data Protection Act. [the first data protection principle](#) requires the data controller to be transparent about what they want to use the data for, any intended disclosures to third parties, and any further information that is necessary,

taking into account the specific circumstances of the processing so that it is fair.

To meet the transparency requirements, those collecting information from subscribers that is to be made available in public directories will need to ensure subscribers understand that:

- their information will be made available through various directory products and services, and
- this will enable those who know their name and address to get their phone number.

Where there are a range of ex-directory options, the subscriber should be told about all of them. So subscribers should understand the consequences of choosing particular directory options. Although subscribers must be given the opportunity to choose whether or not they are included in a directory, the Regulations do not specify whether subscribers should be required to positively 'opt in' to such inclusion or whether it would be enough for them to 'opt out'. In the Commissioner's view, it is reasonable for inclusion in a directory to be the default position, provided:

- subscribers are made fully aware that this is so; and
- it is simple and straightforward for them to opt out, if they choose.

In line with the second requirement listed above, there is an established competitive market in telephone directory information services and products. So, in the interests of practicality, the producer of a directory can decide the personal data they think is relevant to include in their directory. In other words, there should be a core list of the minimum information reasonably needed to run a directory service efficiently. But the Commissioner's view is that the more the data included in a directory differs from that traditionally published in such products, the more information the directory producer is likely to have to provide to the data subject to ensure the processing of that data is fair.

If the data of an individual subscriber has been included in a directory, that subscriber may verify, correct or withdraw that data free of charge at any time. Amendments as a result of a withdrawal or correction request will apply only to editions of a directory produced after the directory producer has received that request.

Reverse searching

Directory information should only be made available in line with subscribers' wishes and expectations. Generating a name or address

(or both) from a phone or fax number (reverse searching) has not traditionally been offered in the UK and is not what subscribers generally expect. So the Regulations prohibit reverse searching unless the subscriber has given their prior informed consent. This requirement was originally set out in the 1998 Code of Practice on Telecommunications Directory Information Covering the Fair Processing of Personal Data.

The idea of reverse searching may not be fully and generally understood, so additional specific consent must be obtained from subscribers agreeing to allow their information to be made available on this basis. It will not be enough for this consent to be combined with various other terms and conditions, which someone might agree to without fully appreciating the consequences.

Corporate subscribers

The Regulations do not give corporate subscribers the full range of rights available to individual subscribers, although a corporate subscriber may ask for their number to be excluded from the directory if they want to.

Directory enquiry services and ex-directory numbers

If there is no entry relating to a subscriber or no entry relating to their number, the Regulations do not prevent the enquirer being told the reason or the possible reason why there is no such entry. This means the enquirer can be told that the subscriber has asked for their number to be excluded from the directory (as has traditionally been the position in the UK), rather than merely being told that a number is not listed. The Commissioner understands that directory providers are considering whether there is any scope for giving subscribers a choice of having a listing, without this fact being given to an enquirer. If this choice is offered, enquirers would have to be told that there is no public listing for the name and address concerned.

Contracts

Any term in a contract between a subscriber and the provider of a communications service or network that is inconsistent with a requirement of the regulations is void.

National security

A communications service or network provider is neither required to carry out nor not required to carry out an act (including processing data) if an exemption from the requirement in question is needed to safeguard national security. A certificate signed by a Minister of the Crown certifying this is conclusive evidence of that fact. Any person directly affected by the issuing of a certificate may apply to [the Information Tribunal](#) against the certificate.

Legal requirements

A telecommunications service or network provider is not neither required to do nor required not to do, anything:

- if compliance would be inconsistent with any requirement:
 - imposed by any enactment;
 - imposed by any rule of law;
 - imposed by court order; or
 - that would be likely to prejudice [the prevention or detection of crime](#) or the apprehension or prosecution of offenders; or

- if exemption from the requirement in question:
 - is necessary for the purposes of obtaining legal advice;
 - is required in connection with legal proceedings (including prospective legal proceedings); or
 - is otherwise necessary for the purposes of establishing, exercising or defending legal rights, (Regulation 33).

Directive 2002/58/EC, which these Regulations implement, is designed to 'particularise and complement' Directive 95/46/EC which has been implemented by the Data Protection Act 1998 (the Act). So, where personal data is being processed, the Act must be complied with. In other words, the above provisions must not be interpreted as in any way overriding' the Act.