



December 2003

BRIEFING

New UK E-Privacy Regulations

Executive summary

UK regulations implementing the E-Privacy Directive (2002/58/EC) will come into force on 11 December 2003. Key provisions include: (a) controls on sending unsolicited marketing emails ('spam') and SMS; (b) rules on the use of cookies by website operators; and (c) rules on the use and retention of electronic communications traffic data and location data. The new laws are the subject of initial guidance from the UK Information Commissioner.

UK regulations implementing the E-Privacy Directive (2002/58/EC) into national law come into force on 11 December 2003 (E-Privacy Regulations). Key provisions include: (a) controls on sending unsolicited marketing emails ('spam') and SMS text messages; (b) rules on the use of cookies by website operators; and (c) rules on the use and retention of electronic communications traffic data and location data.

In advance of the E-Privacy Regulations coming into force, the UK Information Commissioner's Office (ICO) issued initial guidance in November on how the new laws should be interpreted and applied (the ICO Guidance).

Although it is described as 'initial guidance' (and will be reviewed and probably refined in the light of comments), the ICO Guidance provides useful assistance to those who market by electronic means.

Electronic marketing

The E-Privacy Regulations apply to a wide range of electronic direct marketing. They apply to phone calls (including automated calling systems), faxes, emails, SMS text messages, picture messages and video messages. The rules on telephone calls, faxes and automated calling systems largely repeat (with some changes) the equivalent provisions in the Telecommunications (Data Protection and Privacy) Regulations 1999 (1999 Regulations). The E-Privacy Regulations repeal the 1999 Regulations.

A marketing communication that uses the above forms of electronic communication will be regulated under the E-Privacy Regulations if that communication is unsolicited

and the unsolicited message is sent to an individual recipient. The rules also protect corporate subscribers who receive unsolicited telephone calls (including calls made by automated calling systems) and faxes.

Direct marketing sent by electronic means must comply with the E-Privacy Regulations and, in some cases, also with the Data Protection Act 1998 (DPA). If any personal data is processed when carrying out this direct marketing (ie if the marketer uses the recipient's name), the marketer must also comply with the DPA (regulation 4). If, however, the marketer only has a list of telephone numbers (and not the names of individuals who can be reached on these numbers), the marketer only needs to comply with the E-Privacy Regulations when making marketing calls or sending faxes or text messages.

Prior consent to marketing

Under the E-Privacy Regulations, the marketer must obtain 'prior consent' before sending a marketing message (by automated call, fax, email, SMS, video or picture message) by electronic means to an individual. One possible method of obtaining valid consent is to use a tick-box on a website (recital 17 of the E-Privacy Directive). The ICO Guidance states that any form of communication whereby the individual knowingly indicates consent will be sufficient if it amounts to a 'freely given, specific and informed indication' of agreement. In short, the individual must 'fully understand that by the action in question they will be signifying consent' (ICO Guidance, part 1, page 5). However, the ICO cautions marketers against relying on an 'opt-out' box where the individual has not ticked the

box to indicate an objection to direct marketing. The fact that someone has not taken the opportunity to object is 'unlikely' in itself to indicate valid consent to this marketing. For the ICO, the other relevant factors are: the need for a 'suitably prominent' opt-out box and the presentation of a 'clear and prominent' message to accompany that box. The test is whether the message informs the individual that consent is being given and to what that consent is being given.

Under the E-Privacy Regulations, prior consent to receive direct marketing lasts 'for the time being'. The ICO interprets this to mean that an initial consent (if validly obtained – see above) will last for as long as there are good grounds for believing that consent has not been withdrawn.

The ICO Guidance also clarifies who is to be treated as an individual for the purposes of the prior consent provisions of the E-Privacy Regulations. It includes a sole trader and a non-limited liability partnership in England, Wales and Northern Ireland.

In summary, the effect of the E-Privacy Regulations on the various types of electronic marketing mentioned above is as follows.

Email and SMS marketing

Under the E-Privacy Regulations, text, voice, sound or image messages sent over a public electronic communications network are covered by the term 'electronic mail' (regulation 2). The ICO Guidance indicates that voicemail messages left by marketers making 'live' calls also count as electronic mail (ICO Guidance, part 1, page 20).

The rule introduced by the E-Privacy Regulations is that *individual* subscribers (not corporate subscribers) must have given prior consent to receiving direct marketing messages by electronic mail (regulation 22(2)). In the ICO's view, this means that marketers 'need to demonstrate that [an individual] positively opted into receiving further information from [that marketer]' (ICO Guidance, part 1, page 20).

Importantly, there is a 'soft opt-in' exception dispensing with the need for prior consent from *individuals* if:

- there is a previous customer relationship with the recipient – ie that individual's contact details were obtained 'in the course of a sale or negotiations for

- the sale of a product or service to that recipient';
- the direct marketing material concerns 'similar goods or services'; and
- the recipient is given a simple means of refusing consent to future marketing in each marketing communication (regulation 22(3)).

In respect of 'similar goods or services', the ICO expects marketers to take the 'reasonable expectations' of individual subscribers into account when sending marketing in this category (ICO Guidance, part 1, page 22).

The ICO Guidance indicates that electronic mail mailing lists compiled in accordance with the DPA before 11 December 2003 can continue to be used unless the intended recipient has already opted out (ICO Guidance, part 1, page 24).

Under regulation 23, any subscriber (individual or corporate) is entitled to receive two pieces of information in any solicited or unsolicited electronic mail: the identity of the sender and a valid address to which to send an opt-out request. In the ICO's view, as few as 18 characters would be needed in a text message to identify the sender and provide a valid address for suppression requests (eg PJLtdPOBox97SK95AF). The identifying contents of emails may need to comply with other laws (eg the Business Names Act 1985).

Automated calls

Automated calls involve the transmission of recorded messages (and not live speech).

The E-Privacy Regulations restate the requirement of the 1999 Regulations to obtain prior consent from subscribers (individuals or companies) before transmitting marketing material by means of an automated calling system (regulation 19(2)). The ICO indicates it is going to take a 'firm line' on the need for prior consent to automated calls.

All marketing messages sent by automated calling systems must include the caller's identity and an address or a freephone number at which the caller can be contacted (regulation 24(1)(a)).

Telephone marketing

The E-Privacy Regulations restate the requirements of the 1999 Regulations on telephone marketing. In summary, this means complying with all 'stop' requests (from

individuals or companies) and not calling any number listed on the Telephone Preference Service (TPS) database (regulation 21(1)). The TPS register is a statutory 'do not call' list of landline and mobile telephone numbers that is maintained by Ofcom. It is currently open to residential subscribers, sole traders and unincorporated partnerships who wish to register a general objection to receiving unsolicited marketing calls. With effect from May 2004, the E-Privacy Regulations will be amended to extend the TPS register to corporate subscribers (ie companies, limited liability partnerships, government departments and agencies). The Department for Trade and Industry (DTI) has yet to publish full details of these changes.

As with automated calling systems, callers must give the identity of the company on whose behalf a telesales call is made. If asked, the caller must provide a valid address or freephone telephone number at which the company initiating the call can be contacted with a 'stop' or opt-out request. Sub-contractors making calls on a company's behalf, for example, must identify the company (regulation 24(1)(b)). However, the ICO Guidance emphasises that responsibility for compliance with the rules on telesales marketing lies with the instigator of the calls, and not its sub-contractor. The ICO expects companies to ensure that sub-contractors do not call numbers registered on the TPS register or numbers listed on the company's suppression list (see below). Normally enforcement action will be taken against the instigator of the call only, unless there is evidence that the sub-contractor acted in concert with the company to breach the E-Privacy Regulations (ICO Guidance, part 1, page 13).

When responding to an opt-out request, the ICO Guidance indicates that it is not enough for a marketer to delete the relevant numbers from its database. Rather, the numbers must be entered on a 'suppression list' so that a record is maintained that these numbers should not be called. This is important, for example, if the marketer periodically buys lists of numbers from list brokers. The ICO expects the company to check any lists it receives from brokers against the TPS register and the company's own suppression list (ICO Guidance, part 1, page 14).

Fax marketing

The E-Privacy Regulations restate the 1999 Regulations on marketing by fax. In summary, this means that marketing faxes cannot be sent to an individual without that individual's prior consent. In the case of corporate

subscribers, opt-out requests must be respected. Where a general objection to unsolicited faxes has been registered by an individual or corporate subscriber on the statutory Fax Preference Service database, no unsolicited faxes should be sent to the listed fax numbers (regulation 20(1)).

Each fax must identify the name of the business being promoted and give a valid business address or freephone telephone number at which the sender can be contacted.

Where a company uses sub-contractors to send marketing faxes, the ICO views the company as being responsible for compliance with the E-Privacy Regulations unless there is evidence that the company and its sub-contractors have acted in concert to breach the law (ICO Guidance, part 1, page 19).

Again, the ICO Guidance emphasises the need to use suppression lists when receiving opt-out requests.

Cookies

Under regulation 6(2), cookies or similar devices cannot be used unless the subscriber or user (individual or corporate) of the relevant terminal equipment has been given 'clear and comprehensive' information about the reasons for storing or accessing information collected by the cookies. The ICO Guidance indicates that the text used on a website should be 'sufficiently full and intelligible' to enable subscribers to gain 'a clear appreciation of the potential consequences' of allowing cookies to be used (ICO Guidance, part 2, page 5).

Subscribers should also be given 'an opportunity to refuse' the storage of, or access to, information collected by cookies. The ICO expects the mechanism by which the user exercises this right to be prominent, intelligible and 'readily available to all, not just the most computer literate or technically aware'. For example, if this information is included in a website privacy policy, the policy should be clearly signposted on those pages where a user may enter the website (ICO Guidance, part 2, page 5).

The information requirements on cookies are disapplied where the cookie is 'strictly necessary' to provide a service requested by the subscriber or user. In the ICO's view, this means that the cookie must be essential for the provision of the requested service (ICO Guidance, part 2, page 6).

Traffic data

The E-Privacy Regulations regulate the use and retention by public communications providers of so-called 'traffic data' (regulations 7 and 8). This is data that relates to the routing, duration or time of a communication. Individual and corporate subscribers are entitled to have traffic data erased or anonymised where the data is no longer required for the purpose of transmitting a communication (unless retention of traffic data is permitted under crime-fighting or anti-terrorism provisions – eg the Regulation of Investigatory Powers Act 2000 or the Anti-terrorism, Crime and Security Act 2001). There is an exception that allows data to be retained for billing purposes – ie data can in effect be retained for the limitation period of six years during which a bill may be challenged or payment pursued. There is another exception that allows data to be retained and used for billing fraud detection purposes.

If traffic data is going to be used for marketing purposes or to provide a requested value added service, prior informed consent must be obtained. According to the ICO, a blanket 'catch all' statement on a bill or website will not be sufficient: a specific informed consent would be required (ICO Guidance, part 2, page 9).

Location data

The E-Privacy Regulations introduce controls on the use of 'location data'. Essentially this is any data that allows the geographical location of a person using a mobile phone or mobile device to be identified. Location data can only be used to provide a value added service (eg tourist information, or weather or traffic updates) if it is used to provide this service with the customer's prior informed consent (regulation 14).

A person may only use location data for any other purpose if the user or subscriber cannot be identified from the location data. Where the user's consent is needed for the provision of a value added service, the user must have received information about the use of the location data, including whether the data will be transmitted to a third party, and must be given the opportunity to withdraw consent in respect of any particular communications, using simple means and free of charge.

Only public communications providers, third parties providing value added services or persons acting under their authority may lawfully process location data.

Sanctions

Where the E-Privacy Regulations are breached, any affected person or Ofcom can complain to the ICO, which may launch an investigation and possibly take enforcement action using the Information Commissioner's enforcement powers under the DPA. This could result in adverse publicity for the marketer. A person who suffers quantifiable damage may be entitled to claim compensation through the civil courts (regulation 30). It is, however, a defence to show that the party alleged to be in breach did what could reasonably be required to comply with the E-Privacy Regulations.

If the marketer is alleged to have breached the DPA, the ICO may investigate and possibly take enforcement action. This could result in adverse publicity and, in serious cases, the imposition of fines on the company and its directors or senior officers.

Going forward

The new privacy rules place a considerable additional compliance burden on marketers. It is clear that the ICO expects marketers – and not their sub-contractors – to ensure compliance with these rules, and the ICO Guidance provides useful assistance in this respect.

The ICO Guidance may well be revised in the light of industry and consumer comments, as there was no time for the ICO to consult on draft guidance before the E-Privacy Regulations came into force. Anyone with strong views or comments on the ICO Guidance should email the ICO at: mail@ico.gsi.gov.uk.

The E-Privacy Regulations are at www.dti.gov.uk/industry_files/pdf/regulations_20030918.pdf and the ICO Guidance is at www.informationcommissioner.gov.uk/eventual.aspx?id=786.

For further information please contact

Avril Martindale
T + 44 20 7832 7496
F + 22 20 7427 3716
E avril.martindale@freshfields.com