

**GUIDANCE TO THE PRIVACY AND  
ELECTRONIC COMMUNICATIONS  
(EC DIRECTIVE) REGULATIONS  
2003**

**Part 2: Security, Confidentiality,  
Traffic and Location Data, Itemised  
Billing, CLI and Directories**

<b>1. Security of Services</b> .....	3
1.1 Security Risks .....	3
<b>2. Confidentiality of Communications</b> .....	4
2.1 Cookies and Personal Data .....	4
2.2 Information to be Provided.....	5
2.3 Responsibility for Providing the Information .....	5
2.4 Refusal of Cookies .....	6
2.5 Exemptions from the Right to Refuse a Cookie.....	6
2.6 Wishes of Subscribers and Users .....	7
<b>3. Traffic Data</b> .....	7
3.1 Retention .....	7
3.2 Purposes for Processing .....	8
• Value Added Services .....	8
• The Marketing of the Service Provider’s own Electronic Communications Services ..	8
3.3 Consent to Process for the Above Purposes.....	8
3.4 General Provisions Relating to the Processing of Traffic Data .....	9
3.5 Disputes .....	9
<b>4. Location Data</b> .....	9
4.1 Restrictions on Processing.....	10
4.2 Consent to Process.....	10
<b>5. Itemised Bills</b> .....	11
<b>6. Calling or Connected Line Identification ("CLI")</b> .....	11
6.1 Outgoing Calls .....	11
6.2 Incoming Calls - Preserving Anonymity of Caller .....	12
6.3 Incoming Calls - Preserving Anonymity of Called Line .....	12
6.4 Anonymous Incoming Calls - Call Rejection . .....	13
6.5 Duty of an Electronic Communications Service Provider to advise that CLI is available	13
6.6 Malicious or Nuisance Calls .....	13
6.7 Calls to Emergency Services .....	14
6.8 Termination of Unwanted Automatic Call Forwarding .....	14
6.9 Charges .....	14
<b>7. Directories of Subscribers</b> .....	14
7.1 Individual Subscribers .....	15
7.2 Reverse Searching.....	16
7.3 Corporate Subscribers .....	16
7.4 Directory Enquiry Services and Ex-Directory Numbers .....	16
<b>8. Contracts</b> .....	17
<b>9. National Security</b> .....	17
<b>10. Legal Requirements</b> .....	17

## **1. Security of Services**

An "electronic communications service" is defined in the Communications Act 2003 as a service consisting in, 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 public electronic communications service provider must take appropriate technological and organisational measures to safeguard the security of its services. An "appropriate" measure is one which having regard to the state of technological development and the cost of their implementation, is proportionate to the risks against which it would safeguard.

These provisions compare with the obligations on a data controller under the seventh data protection principle (please see <http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>, *Data Protection Act 1998: Legal Guidance*, paragraph 3.7)

Regulation 5(2) states that if necessary, such measures should be taken by the electronic communications service provider in conjunction 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.

This Regulation is intended to ensure reasonable co-operation between service and network providers.

### **1.1 Security Risks**

Where appropriate measures are taken but there still remains a significant risk to the security of the service, the service provider shall proactively inform the subscribers concerned of-

- a) The nature of that risk;
- a) Any appropriate measures the subscriber may take to safeguard against that risk; and
- b) The likely costs to the subscriber involved in the taking of such measures.

Such information shall be provided to the subscriber free of charge except for any nominal costs which the subscriber may incur while receiving or collecting the information, for example through the downloading of an email.

Such security is not to be regarded as being compromised by reason of:

- a disclosure made in connection with the prevention or detection of crime (see <http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>, *Data Protection Act 1998: Legal Guidance*, paragraph 5.3)
- a disclosure made for the purposes of criminal proceedings (see <http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>, *Data Protection Act 1998: Legal Guidance*, paragraph 5.10)
- an order made by the Secretary of State to intercept any communications as may be specified in a warrant; or
- any disclosure made in the interests of national security or in pursuance of a court order.

## **2. Confidentiality of Communications**

Regulation 6 is concerned with 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 in order to gain access to information, store information or trace the activities of the user. The Regulation of the use of such devices reflects the growing concern about the use of covert surveillance mechanisms online.

It is, however, recognised in the Directive that the use of 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 the provision of many online services. The use of such devices is not, therefore, prohibited by the Regulations but they do require that subscribers and users should, to some extent, be given the choice as to which of their online activities are monitored in this way.

### **2.1 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 be required to ensure that they comply with the additional requirements of the Data Protection Act 1998. This includes the requirements of the third data protection principle which states that data controllers shall not process personal data that is excessive (see <http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>, *Data Protection Act 1998: Legal Guidance*, paragraph 3.3). 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 of particular relevance where the data is to be processed for a purpose other than the provision of the service directly requested by the user, for example the counting of visitors to a website.

## 2.2 Information to be Provided

Cookies or similar devices shall 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) is given the opportunity to refuse the storage of, or access to, that information.

The Regulations are not prescriptive about the sort of information that should be provided but the text should be sufficiently full and intelligible to enable individuals to gain a clear appreciation of 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 (see <http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>, *Data Protection Act 1998: Legal Guidance*, paragraph 3.1.7)

The requirement that the user or subscriber should be “given the opportunity to refuse” the use of the cookie type device may be subject to differing interpretation. At the very least, however, the user or subscriber should be given a clear choice as to whether or not they wish to allow a service provider to engage in the *continued* storage of information on the terminal in question.

The fact that an “opportunity to refuse” such storage or access must be provided imposes a greater obligation on the relevant party than that they should simply make such a refusal a possibility. The mechanism by which a subscriber or user may exercise their right to refuse continued storage should, therefore, be prominent, intelligible and readily available to all, not just the most computer literate or technically aware. Where the relevant information is to be included in a privacy policy, for example, the policy should be clearly signposted at least on those pages where a user may enter a website. The relevant information should be appear in the policy in a way that is suitably prominent and accessible and it should be worded so that all users and subscribers are capable of understanding, and acting upon it, without difficulty.

The Interactive Advertising Bureau (IAB) is an industry body that develops standards and guidelines to support online business processes. It has produced a series of web pages ([www.allaboutcookies.org](http://www.allaboutcookies.org)) which explains to users how cookies work and can be managed. The IAB welcomes website owners who wish to link their cookie policies directly to these pages.

Regulation 6(3) states 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 in Regulation 6(2) (and discussed above) on subsequent occasions, provided that these requirements were met in respect of the initial use. Although the Regulations do not require the provision of the relevant information on each occasion, they do not prevent this.

## 2.3 Responsibility for Providing the Information

The Regulations do not define who should be responsible for providing the information outlined in Regulation 6(2). 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 providing the information in question.

We recognise that it is possible for organisations to use cookie type devices on websites seemingly within the control of another organisation, for example through a third party advertisement on a website. In such cases the organisation to whom the site primarily refers will be obliged to alert users to the fact that a third party advertiser operates cookies. It will not be sufficient for that organisation to provide a statement to the effect that they cannot be held responsible for any use of such devices employed by other persons they allow to place content on their websites. In addition, the third party would also have a responsibility to provide the user with the relevant information.

## **2.4 Refusal of Cookies**

The Regulations are also non-prescriptive about the way in which a user or subscriber should be able to refuse the use of a cookie type device. Again, although a standard approach would be beneficial, whether service providers choose to make their own switch off facilities available or else explain to the user or subscriber how they can use the facilities specific to their browser type is less important than that the mechanism is uncomplicated, easy to understand and accessible to all.

There is, in addition, nothing to prevent service providers from requiring users to “opt in” to receipt of the cookie as opposed to providing them with the opportunity to “opt out”.

## **2.5 Exemptions from the Right to Refuse a Cookie**

The Regulations specify that service providers should not have to provide the information specified in Regulation 6(2) where that device is to be used

- a) for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network; or
- b) where such storage or access is strictly necessary for the provision of 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, as opposed to reasonably necessary, for this exemption to apply. It will also, however, be restricted to what is essential for the provision of 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 for compliance with any other legislation to which the service provider might be subject, for example, the security requirements of the seventh data protection principle (see <http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>, *Data Protection Act 1998: Legal Guidance*, paragraph 3.7)

Where the use of a cookie type device is deemed “important” as opposed to “strictly necessary” the user of the device is still obliged to provide information about the device to the potential service recipient so that they can decide whether or not they wish to

proceed. The information provided to the user about the uses the collector intends to make of that data should be of sufficient clarity to enable the user to make a truly informed decision.

## **2.6 Wishes of Subscribers and Users**

Regulation 6 states that the relevant information and the opportunity to refuse the cookie type device should be provided to “the subscriber or user” but it does not specify whose wishes should take precedence in the event that they do not coincide. 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 in order to carry out a particular task, where the effective completion of this task depends upon the use of a cookie type device. In such cases it would not seem unreasonable that the employer’s wishes should take precedence. It also, however, seems likely that there will be circumstances where a user’s wish should prevail. To continue the above example, an employer’s wish to accept such a device should not prevail where this will involve the unwarranted collection of personal data of which that employee is the data subject.

## **3. Traffic Data**

Traffic data means any data which are processed

- for the conveyance of 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.

### **3.1 Retention**

Data processed to establish communications could potentially contain personal information which should only be stored for limited purposes and retention periods in accordance with the second and fifth principles of the Data Protection Act 1998 (see <http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>, *Data Protection Act 1998: Legal Guidance*, chapter 3). The Regulations provide for the protection of individual and corporate subscribers with regard to the processing of traffic data. Where such data are no longer required for the purpose of the transmission of a communication, on the termination of that communication, that data must be erased or dealt with in such a way that they cease to be personal data in the case of an individual subscriber, or in the case of a corporate subscriber, modified so that they cease to be data that would be personal data in the case of an individual.

Data required by the communications network or service provider for the purpose of calculating 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 that a limitation period of six years plus appeals applied. However, the Commissioner's view is that this provision merely permits retention of such data where circumstances require it, for example, where a challenge is made to the bill during the time 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 regard must be had to the fifth data protection principle which provides that personal data shall not be kept for longer than is necessary for the purpose for which they are processed.

### **3.2 Purposes for Processing**

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

- **Value Added Services**

To provide value added services to the subscriber or user. A value added service means any service which requires the processing of traffic data or location data beyond that which is necessary for the transmission of a communication or the billing of that communication, for example a service which 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.

- **The Marketing of the Service Provider's own Electronic Communications Services**

Under the Regulations, the consent of the subscriber or user must be obtained before the service provider can market its own electronic communications services. Such marketing need not necessarily be carried out over the telephone and might include, by way of an example, an analysis of a subscriber's usage patterns to provide that subscriber with the best tariff available.

Such processing may only be undertaken by the communications provider or by a person acting under his authority. Given that ultimate responsibility for compliance with the Regulations regarding the processing of traffic data will lie with the communications provider, the requirements of the seventh data protection principle should be observed. The provisions concerning contracts are of particular relevance (see <http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>, *Data Protection Act 1998: Legal Guidance*, paragraph 3.7). Although the Act applies only to the processing of personal data there is nothing to stop service providers imposing such contracts as regards the processing of traffic data relating to corporate subscribers.

### **3.3 Consent to Process for the Above Purposes**

Where 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 holding himself out as capable of giving consent on the part 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, in order to obtain valid informed consent, the subscriber or user should be given sufficient clear information in order for them to have a broad appreciation of how the data are going to be used and the consequences of giving consent to such use (see <http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>, *Data Protection Act 1998: Legal*

*Guidance*, paragraph 3.1.7). 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 rather will be required to obtain specific informed consent for each value added service requested and for the marketing of their own electronic communications services.

Where, for example, a value added service is provided by a communications provider in conjunction with a third party, in the interests of transparency the consent to process for such a purpose should be obtained by the person who will be seen to be responsible for providing that service. Whether this will be the service provider, the third party or both will depend on the specific circumstances. The point is that the way in which a service is provided should be consistent with the expectations of the subscriber or user. Where the user provides consent to one party for the purpose of the provision of a particular service, they should not then be surprised when they are contacted by another party relating to the provision of that service.

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

Any such consent given by the subscriber or user to process related traffic data may be withdrawn at any time by that subscriber or user.

### **3.4 General Provisions Relating to the Processing of Traffic Data**

In addition to 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:

- the management of billing or traffic;
- customer enquiries; and
- the prevention and detection of fraud.

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

### **3.5 Disputes**

Nothing is to prevent the furnishing of traffic data to a person who has been given statutory authority to resolve disputes, for example OFCOM.

## **4. Location Data**

“Location data” means any data processed in an electronic communications network indicating 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 section 5 above.

#### **4.1 Restrictions on Processing**

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

- the subscriber or user cannot be identified from that data or
- Where it is necessary for the provisions of a value added service (see section 5 above) with the consent of the relevant user or subscriber.

Location data shall 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. Where the processing is carried out for the purposes of the provision of a value added service, the processing of location data should be restricted to what is necessary for those purposes.

Again as ultimate responsibility for compliance with the Regulations regarding the processing of location data lies with the communications provider, the requirements of the seventh data principle of the Data Protection Act should be observed particularly as regards the processing of personal data carried out by a data processor (see <http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>, *Data Protection Act 1998: Legal Guidance*, paragraph 3.7. Although the Act applies only to the processing of personal data there is nothing to stop service providers imposing such contracts with regard to the processing of location data from which an individual cannot be identified.

#### **4.2 Consent to Process**

The public communications provider must obtain the prior consent of the user or subscriber to process location data for the purposes of providing a value added service (where the user or subscriber can be identified from that data). Before consent can be obtained the communications provider must provide the user or subscriber with 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 for the purposes of providing the value added service.

In the case of a corporate subscriber, a person holding himself out as capable of making decisions on the part 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 obtain this consent. However, in order to obtain valid informed consent, the subscriber or user should be given sufficient clear information in order for them to have a broad appreciation of how the data are going to be used and the consequences of giving consent to such use (see <http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>, *Data Protection Act 1998: Legal Guidance*, paragraph 3.1.7). 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 rather will be required to obtain specific informed consent for each value added service requested and for the marketing of their own electronic communications services.

Where a valued added service is provided by a public communications provider in conjunction with a third party, in the interests of transparency it is likely that the consent to process location data for such a purpose should be obtained by the person who will be seen to be responsible for providing the service. Whether this will be the service provider or the third party will depend on the specific circumstances. The point is that the way in which a service is provided should be consistent with the expectations of the subscriber or user. Where the user provides consent to one party for the purpose of the provision of a particular service, they should not then be surprised when they are contacted by another party relating to the provision of that service.

Where a user or subscriber has given informed consent to the processing of location data the user or subscriber shall be able to withdraw that consent at any time and the communications provider should make the user or subscriber aware of that fact. The user or subscriber should also be provided with an opportunity to withdraw their consent on the occasion of each connection to the network or on each transmission of a communication. Although the obligation is to provide for a permanent withdrawal of consent, there is nothing in the Regulations that will prevent the service provider from also offering the user the chance to suspend their consent for a limited, specified period of time. If the user chooses to accept such an option, there is similarly nothing to prevent the provider from “reactivating” their consent after the specified period of time has elapsed, providing the intention to do so was made sufficiently clear at the time at which the user opted for a time bound suspension.

## **5. Itemised Bills**

A subscriber is entitled, upon request, to receive bills which are not itemised, in recognition of the fact that such bills may jeopardise the privacy of users even though they are also useful for subscribers to verify the amount of the bill.

In exercising their functions under Chapter 1 Part 2 of the Communications Act 2003 Ofcom have a duty to reconcile the rights of subscribers receiving itemised bills with the rights to privacy of calling users and called subscribers, for example, by ensuring that sufficient alternative means for the making of calls or methods of paying for calls are available to such users and subscribers to facilitate anonymous calls in particular. The Telecoms Directive suggests that this may be achieved by the provision of pre-paid telephone cards. Pre-paid phones would also be relevant in this context.

## **6. Calling or Connected Line Identification ("CLI")**

The Regulations address the prevention and restriction of calling or connected line identification ("CLI") for both incoming and outgoing calls.

The Regulations cover Call Return and Call Display facilities, for example the display on certain telephone equipment which alerts the subscriber to the identity of the caller before the connection is made and the "1471" service. CLI Services are governed by an OFTEL published code entitled the "Code of Practice for Network Operators in relation to Customer Line Identification Display Services and Other Related Services". Adherence to the Code will assist with compliance with the Regulations.

## **6.1 Outgoing Calls**

The onus is on the communications service provider to ensure that:-

- a user originating a call, has, in relation to that call, a simple means to prevent presentation of the identity of the calling line on the connected line;
- a subscriber has, as respects his line and all calls originating from that line, a simple means to prevent presentation of the identity of his line on any connected line.

The distinction between the user and the subscriber is to be noted here as the user only has the right to block his identity in relation to a particular call, whereas a subscriber has the right to block his identity as respects his line and all calls originating from that line. In either case, the user or subscriber is not to be charged for this facility.

## **6.2 Incoming Calls - Preserving Anonymity of Caller**

In the case of incoming calls the communications service provider is obliged to ensure that the called subscriber has a simple means to prevent presentation of the identity of a calling line on the connected line. In this instance, there is to be no charge for reasonable use of the facility.

This is particularly likely to be used for cases in which the caller's anonymity is guaranteed, namely, various help-lines such as the Samaritans, Alcoholics Anonymous or Police information lines.

## **6.3 Incoming Calls - Preserving Anonymity of Called Line**

This preserves the privacy of an individual 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 where the call may be forwarded to the number of an individual doctor or locum service. This facility will enable the number of the line to which the call is forwarded to remain private.

Under the Regulations the relevant telecommunications service provider is under an obligation to ensure that the subscriber to whose line a call is forwarded has a simple means to prevent, without charge, presentation of the identity of the connected line on any calling line.

## **6.4 Anonymous Incoming Calls - Call Rejection**

Where a caller has eliminated the presentation on the connected line of the identity of the calling line the called subscriber must be provided with a simple means to reject the calls in question. There is no mention of any charge for the provision of 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, in relation to incoming international calls. Therefore, a subscriber who chooses not to receive calls with CLI withheld will also not receive international calls.

Where calls are rejected on the basis that 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 provide called parties with a simple means of rejecting a call where the CLI has been withheld. It was the understanding of the Commissioner 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. It is the Commissioner's current understanding, on the basis of advice received from Oftel, that as the relevant Regulation applies to the automatic rejection of voice calls only, this can be implemented relatively simply using a recorded voice message.

## **6.5 Duty of an Electronic Communications Service Provider to advise that CLI is available**

A communications service provider who offers CLI facilities is obliged to take all reasonable steps to publicise that he does so and also to explain the consequences of the Regulations in relation to CLI.

## **6.6 Malicious or Nuisance Calls**

There are provisions to assist with the tracing of malicious or nuisance calls where the relevant communications service provider has been notified by a subscriber that he or she requires the tracing of such calls on his or her line.

In such situations, the communications service or network provider as appropriate may override anything done to prevent the presentation of the identity of the calling line, to calls in relation to which the subscriber's line is the called line, in so far as it appears to the provider in question to be necessary or expedient for the purposes of such action.

In relation to such calls, the relevant communications service or network provider as appropriate may hold and make available to a person with a "legitimate interest" in this information, data containing the identification of a calling subscriber obtained pursuant to these provisions. 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 where the number from which the call was made related 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. Under the Act, the expression "legitimate interests" has been given a relatively wide interpretation by the Commissioner. 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 the expression "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.

It is, however, worth pointing out that there may be cases where a service provider would wish to exercise some circumspection where a request for information regarding the identity of a calling subscriber is made. Where, for example, the service provider is not satisfied that the calling subscriber has in fact abused the service in the manner to which Regulation 15 refers, he may well choose not to release that information to the called subscriber although he might not rule out releasing it to the police where any such further request provides an extra level of reassurance.

### **6.7 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 facilitate the dealing with such calls by the emergency services to enable easier identification of the caller's location.

The restriction on processing of location data under Regulation 14(2) shall be disregarded (see section 6 above).

### **6.8 Termination of Unwanted Automatic Call Forwarding**

If calls are being forwarded as outlined in 4.3 above, the subscriber has the right to request of the relevant communications service provider, that such forwarding shall cease without unavoidable delay and that any other network or service provider shall comply with all reasonable requests in this connection.

### **6.9 Charges**

Some of the Regulations require that a facility be provided free of charge. Where there is no mention in the Regulations that a charge may be made for a service, the Regulations permit that where a person is required to provide, or ensure the provision of, a facility, a reasonable charge may be made unless there is an indication to the contrary.

## **7. 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 is in possession of 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 do not constitute the sole or major component. This means that only directories of residential, and also business, subscribers are covered by the Regulations.

It has been suggested that a WHOIS lookup service may be caught by the Regulations relating to directories. From the description above, it is difficult to see that a WHOIS lookup will clearly be caught in that the main purpose of WHOIS is to provide the searcher with information as to the identity of the person who operates a website, a person who may well not be party to a contract with the WHOIS provider. The Commissioner intends, for the time being, to interpret Regulation 18 as applying only to directories of telephone numbers (including mobile telephone numbers), fax numbers and e-mail addresses.

The Regulations make it clear that such directories may be in printed or electronic form or may be those relied upon by a directory enquiry service, for example the “118” services. The provisions do not apply to an edition of a directory first published before 11<sup>th</sup> December 2003.

## 7.1 Individual Subscribers

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

- a) informed by the collector of the personal data of the purposes of the directory, and
- b) given the opportunity to determine whether such of his personal data as are considered relevant by the producer of the directory should be included in the directory.

The requirement outlined in (a) above is in accordance with the fair processing requirements of the Data Protection Act. The first data protection principle requires transparency on the part of the data controller regarding the purposes for which the data is to be used, intended disclosures to third parties and any further information which is necessary taking into account the specific circumstances in which the data are to be processed to enable the processing in respect of that data to be fair (see <http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>, *Data Protection Act 1998: Legal Guidance*, paragraph 3.1.7).

In order to satisfy transparency requirements, those collecting information from subscribers which is to be made available in public directories will need to ensure subscribers appreciate that their information will be made available via a variety of directory products and services that will enable those who know their name and address to obtain their phone number. Where there are a range of ex-directory options these should be drawn to the subscribers attention. In summary, subscribers should appreciate the consequences of choosing particular directory options.

Although subscribers must be given the opportunity to choose whether or not they are listed 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 sufficient for them

to “opt out”. It is the Commissioner’s view that it is not unreasonable for inclusion in a directory to be the default position provided that subscribers are made fully aware that this is the case and it is simple and straightforward for them to opt out if they choose.

In accordance with (b) above, given that there is an established competitive market in telephone directory information services and products and in the interests of practicality, it is within the gift of the producer of a directory to determine those personal data he believes are relevant for inclusion in a directory insofar as there should be a core list of the minimum information reasonably necessary to run a directory service efficiently. It is the Commissioner’s view, however, 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 be required to provide to the data subject to enable the processing of that data to be fair.

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

## **7.2 Reverse Searching**

Directory information should only be made available in line with the wishes and expectations of data subjects. The generation of a name and/or address from a telephone or fax number (reverse searching) has not traditionally been offered in the UK and as is outside the general expectations of subscribers. The Regulations therefore prohibit reverse searching unless the data subject 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 (see <http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>, Codes of Practice, Telecommunications Directory Information).

The concept of the term “reverse search” may not be fully and generally understood. For this reason an additional specific consent must be obtained from subscribers agreeing to allow their information to be made available on this basis. It will not be sufficient for this consent to be bundled up with a variety of other terms and conditions to which an individual might agree without a full appreciation of the consequences.

## **7.3 Corporate Subscribers**

The Regulations do not extend the full range of rights available to individual subscribers, although a corporate subscriber may request that their number be excluded from the directory if he so wishes.

## **7.4 Directory Enquiry Services and Ex-Directory Numbers**

Where there is no entry relating to a subscriber or no entry relating to his or her number there is nothing in the Regulations to prevent the enquirer being told the reason or the possible reason why there is no such entry. This means that the enquirer can be told that the subscriber has requested that a number be excluded from the directory (as has traditionally been the position in the UK) rather than merely being advised that a number is not listed. It is, however, the Commissioner’s understanding that directory providers

are currently considering whether there is any scope for giving subscribers a choice of having a listing the existence of which will not be confirmed to the enquirer. If this choice is offered in due course then enquirers would have to be advised that there is no public listing in the name and address concerned.

## **8. 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 shall be void.

## **9. National Security**

A communications service, or network, provider is not required to carry out or refrain from carrying out an act (including the processing of data) if exemption from the requirement in question is required for the purpose of safeguarding national security. A certificate signed by a Minister of the Crown certifying the same shall be conclusive evidence of that fact. Any person directly affected by the issuing of a certificate may apply to the Information Tribunal against the certificate.

## **10. Legal Requirements**

A telecommunications service, or network, provider is not required to do, or refrain from doing, anything

1) if compliance would be inconsistent with any requirement:

- imposed by any enactment;
- imposed by any rule of law;
- imposed by court order; or
- which would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders; or

2) if exemption from the requirement in question:

- is necessary for the purposes of obtaining legal advice; or
- 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

It should be noted that Directive 2002/58/EC which these Regulations give effect to is designed to “particularise and complement” Directive 95/46/EC which has been implemented by the Data Protection Act 1998 (DPA98). Therefore where the processing of personal data are involved, the requirements of the DPA98 must be complied with. In other words the above provisions must not be construed as in any way “over-riding” the DPA98.