1. Introduction

Special data protection rules apply to the protection of Personal Data by Data Controllers in the electronic communications sector. These are ***in addition*** to the general obligations that apply to all data controllers under the Data Protection Acts. Obligations also arise for entities acting on behalf of data controllers in this sector.

The additional obligations are in the areas of data security (including data breaches), marketing, data retention and data disclosure. **Failure to comply with these obligations can lead to severe criminal penalties.**

2. Sectoral Areas Affected

The Regulations apply directly to electronic communications companies (telecommunications companies & internet services providers) and to any entity using such communications and electronic communications networks to communicate with customers, e.g. by telephone, via a website or over email, etc.

3. Data Security

The Regulations make more explicit the general requirement under the Data Protection Acts to keep personal data safe and secure. Data controllers in the electronic communications sector must give effect to a specific security policy which protects personal data*against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure* of personal data; ensure that personal data can only be accessed *by authorised personnel for legally authorised purposes*; and provide information to subscribers on any *particular risk of a breach of the security of [a] public communications network.*

4. Data Breach Requirements

The general effect of the Regulations is to make the provisions of the existing Code of Practice legally binding in the electronic communications sector. In addition, the Regulations provide that *all* breaches in this sector be reported to the Office of the Data Protection Commissioner.

5. Traffic Data

5a. Retention

The Regulations provide that "traffic data" – details of the calls, emails, text messages, fax messages, internet access via an IP address made by subscribers (excluding content) – may only be retained by the service provider for as long as necessary to enable bills and telecommunications providers interconnect payments to be settled and to meet specific legal requirements.

In applying this rule in practice, electronic communications service providers should be mindful of the strong privacy impact of logging such details. They should only store such privacy-sensitive data for a limited period to enable routine billing queries to be addressed, to satisfy the obligations in interconnect agreements and to meet legal requirements (notably the retention obligations set out in the Communications (Retention of Data) Act 2011.

Details of traffic data relating to subscribers should not routinely be kept for longer periods. However, it is permissible to retain such data for longer periods if –

- the particular subscriber has queried his or her bill, and the data need to be retained to enable the query or dispute to be resolved
- there is some other legitimate reason to believe that a query or dispute is likely to arise in a particular case.

5b. Itemised Bills

Subscribers also have the right not to receive detailed itemised bills, if they wish, as an extra step to safeguard their privacy.

5c. Use of Traffic Data

Prior consent is required if a service provider wishes to use traffic data for the purpose of marketing its own electronic communication services or for the provision of value added services. The subscriber must be informed in advance of the types of traffic data to be used, how long it will be used for and be given the possibility to withdraw at any time the consent they may have given for the use of their traffic data. A user must be informed of the means by which they can withdraw their consent.

6. Storing and Accessing information on terminal equipment e.g. "Cookies"

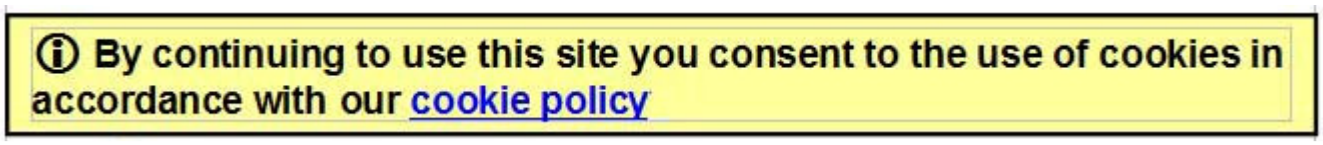
Various provisions concerning electronic communications, including the storing and accessing of information on terminal equipment e.g. cookies, is set out in SI 336 of 2011 which implemented the ePrivacy Directive into Irish law on the 1st of July 2011. In order to meet the legal requirements, the minimum requirement is that clear communication to the user as to what he/she is being asked to consent to in terms of cookies usage and a means of giving or refusing consent is required. The Regulations do not prescribe how consent to drop cookies is to be obtained but envisage that, where it is technically possible and effective, such consent could be given by the use of appropriate browser settings, as long as reliance is not placed on the default browser settings.

It is particularly important that the requirements are met where so called 'third party' or 'tracking' cookies are being deployed, such as when advertising networks collect information about websites visited by users in order to better target advertising. For cookie usage, this Office would be satisfied with a prominent notice on the homepage informing users about the website's use of cookies with a link through to a Cookie Statement containing information sufficient to allow users to make informed choices and an option to manage and disable the cookies. Practically, for Irish website operators we suggest the following for minimum compliance with these requirements:

- **Consent**

The consent of the user must be captured.
Consent may be obtained ***explicitly*** through the use of an opt-in check box which the user can tick if they agree to accept cookies.

Consent may also be obtained by ***implication***



Not all cookies require consent to be used. These are cookies essential to delivering the service requested by the user - session cookies, authentication cookies (for the duration of the session,) and user security cookies. For example, for storage of items in a shopping cart on an online website advance consent will not be required. This will generally be the case where the cookie is stored only for as long as the "session" is live and will be deleted at the end of the session.

Extensive guidance on the 'Cookie Consent Exemption' has been published by the Article 29 Data Protection Working Party..

- **Notification**

As best practice, a positive action may be deployed to dismiss the notification.
[Note: many websites have addressed this issue by providing a 'hide' button which dismisses the notification.]

- Consent should be sought as part of a "prominent notification" displayed on entry to a web site (this might be the home page of the site but may also be via a 'deep link' to an inner page, which a user has found from a search result, for example).

- The notification should contain a link to a Cookie Statement which will outline in greater detail how the site makes use of cookies.

- **Cookies Statement**

As best practice, the following information could also be provided in the Cookie Statement:

- The Cookie Statement should contain clear and comprehensive information on how cookies are used, including information on the types of cookies used and details on how to remove them
- Clear and comprehensive information
- Itemised cookie types, including their purpose e.g. preferences such as language or, font, browsing & search history, tracking, session security and any third party cookies
- Instructions on how to disable the cookies.

- **Third Party Cookies**

  Where third party cookies are being used, it is not sufficient to simply refer the user to third party websites. In such situations or where there are many cookies being created or read by the site (or its partners) we recommend the inclusion in the Cookies Statement of a tabulated explanation of all cookies with the following details:
- Type
- Name
- A description of their purpose
- Their expiry dates
- Links to advertising networks' opt-out mechanisms for third party cookies

In terms of who is the data controller when third party cookies are deployed, the website operator is regarded as a joint data controller alongside the advertising network because even though the cookies are created by the third party site, the website operator has chosen to host these 3rd party cookies on its website.
Guidance on Online Behavioural Advertising (and the use of cookies) has been published by the Article 29 Data Protection Working Party.

7. Calling Line Identification ("Caller ID")

Caller ID is the system that allows phone users to see the number of the person who is calling them. The Regulations set out rules to ensure that the system respects people's privacy rights.

The rules applying to Caller ID can be summarised as follows:

Rights for people making telephone calls

- Telephone subscribers have the right to hide or withhold their number on an 'across the board' basis to ensure that every time they make a call all called persons cannot see their number. This right must be easy to exercise and be free of charge. This is referred to as *'per-line' withholding.*

- Where a telephone subscriber has not opted for 'per-line' withholding, they still have a right to withhold their number on an individual call basis so that the called person cannot see it. This right must be easy to exercise and be free of charge. This is referred to as*'per-call' withholding.*

Rights for people receiving telephone calls

- People receiving telephone calls have the right to block Caller ID details of incoming calls from being displayed. This function must be available easily and free of charge for reasonable use.

- People receiving telephone calls can prevent their own number from being displayed to people who have called them – i.e. the right to block 'connected line identification.'

- People receiving telephone calls have the right to reject incoming calls by simple means, in cases where the caller has hidden or withheld the Caller ID.

8. Processing Location Data

Information giving a user's location - other than traffic data - may only be processed if made anonymous or with the **prior** consent of the individual to the extent and for the duration necessary for the provision of a value added service.

Full information must be given to users and subscribers, prior to obtaining their consent, of the type of location data that will be processed, the purposes and duration of processing and whether the data will be passed to any third party for the purpose of providing the value added service. The user can withdraw the consent given to process location data and must also be given the option - using a simple means and free of charge - of temporarily refusing processing for each connection to the public communications network or for each transmission of a communication. A user must be informed of the means by which they can withdraw their consent.

8a. Overriding Caller ID & location processing rules – exceptional circumstances

In certain exceptional circumstances, people's preferences regarding Caller ID and location data may need to be overridden, so that the number and/or location of the person making the call is available to the person receiving the call. These circumstances, provided for in the Regulations, are as follows –
For overriding Caller-ID rules
- Where An Garda Síochána are investigating malicious or nuisance phone calls
For overriding Caller-ID and location data rules
- Where an emergency call is made (by dialling 999 or 112), to enable the emergency services, including law enforcement agencies, to respond to the call.

8b. Information about Caller ID and location data

The Regulations provide that telecommunications companies must inform their subscribers about Caller ID services. The companies are obliged to publish a notice giving these details, and to display the details on their websites. The companies must also provide information, on request, about the circumstances in which the normal Caller ID settings and the withholding of location data can be overridden.

9. Public telephone directories

The Regulations contain rules for the publication of telephone directories, to ensure that the privacy of individual subscribers, whether natural persons or otherwise, is safeguarded. The rules are as follows:

Before being included in a directory subscribers are to:
- be informed of the purpose including any embedded search functionality in electronic versions of the directory,
- be given the option of being included or not and
- be able to choose which of their personal details, for example, gender are included.

10. Direct marketing

The Regulations cover the making of unsolicited phone calls and the sending of unsolicited fax messages, e-mail and SMS ("text messages") for direct marketing purposes. The requirements extend to all forms of marketing carried out by means of a publicly available electronic communications service – including, for example, the soliciting of support for charitable organisations or political parties.

Varying rules apply to phone, fax, text message and e-mail marketing. The rules are more restrictive in the case of marketing by electronic mail of individuals (natural persons) who are not customers. Unlike in the case of postal marketing, certain restrictions also apply to electronic marketing to businesses and other corporate entities.

If the call is made by automated calling machine or fax the information provided must include the name, address and telephone number of the person making the communication and, if applicable, the name, address and telephone number of the person on whose behalf the communication is made.

The sender of an e-mail or SMS must include in the message their name and a valid address at which they can be contacted including to opt-out of such messages.

11. Phone (All Subscribers)

A marketing phone call may not be made to the telephone line of an individual subscriber or a business subscriber if (a) the subscriber's telephone line is a mobile phone line and prior consent for such a call was not received, or (b) the subscriber's telephone line is a landline and his/her/its preference not to receive such calls is noted in the National Directory Database..

A marketing phone call may not be made to an individual or business telephone line if s/he/it has previously told the caller that s/he/it does not consent to the receipt of such calls.

The person making a marketing call must include in the call their name and, if applicable, the name of the person on whose behalf the call is made.

12. Automated Calling Machines

12a. Individual Subscriber

An automated calling machine may not be used for the purpose of direct marketing to the line of an individual subscriber unless that individual has previously consented to the receipt of such a communication by this means.

12b. Business Subscriber

An automated calling machine may not be used for the purpose of direct marketing to the line of a business subscriber if that subscriber has its preference not to receive marketing calls noted in the National Directory Database.

An automated calling machine may not be used for the purpose of direct marketing to the line of a business subscriber if that subscriber has previously indicated to the caller that it does not consent to the receipt of such calls.

12c. General

Where an automated marketing call is permitted, the name, address and telephone number of the person making the call must be given and, if applicable, the name, address and telephone number of the person on whose behalf the communication is made.

In practical terms, therefore, once a marketing call made by an automated calling machine is answered by the subscriber or the subscriber's voicemail answering service, the automated calling machine must identify who is making the call and provide their contact details.

13. Fax

13a. Individual Subscriber

A fax for the purpose of direct marketing may not be sent to the line of an individual subscriber unless that individual has previously consented to the receipt of such a communication.

13b. Business Subscriber

A fax for direct marketing purposes may not be sent to a business fax number if that subscriber has its preference not to receive marketing calls to that number noted in the National Directory Database..

A fax for direct marketing purposes may not be sent to a business fax number if that subscriber has previously indicated to the caller that it does not consent to the receipt of such faxes.

13c. General

Where a marketing fax communication is permitted, the information provided must include the name, address and telephone number of the person making the communication and, if applicable, the name, address and telephone number of the person on whose behalf the communication is made.

14. Electronic Mail

Electronic mail includes text messages (SMS), voice messages, sound messages, image messages, multimedia message (MMS) and email messages.

14a. Individual Customers

Where a data controller has obtained contact details in the context of the sale of a product or service, it may only use these details for direct marketing by electronic mail if the following conditions are met:

1. The product or service is of a kind similar to that which was sold to the customer at the time their contact details were obtained

2. When these details were collected, the customer was given the opportunity to object at that time, in an easy manner and without charge, to their use for marketing purposes

3. Each time a marketing message is sent, the customer must be given the right to object to the receipt of further messages

4. The details were collected within the previous 12 months or the subscriber has received a marketing electronic mail within the previous 12 months to which they did not unsubscribe using the cost free means provided to them by the direct marketer

A data controller can also obtain prior opt-in consent from its customers or other individuals to send electronic marketing relating specifically to its own business or services. Each marketing message sent on foot of that consent must contain a means to opt-out and it must

identify the sender. Such opt-in consent expires after twelve months unless it is renewed in the interim.

14b. Individuals ("Natural Persons") who are not Customers

If an individual is not a customer, electronic mail may not be used to send a marketing message to their contact address unless the prior opt-in consent of that individual has been obtained to the receipt of such messages – a consent that can be withdrawn at any time.

14c. Business Contacts (Customers and non Customers)

Electronic mail may not be used to send a marketing message to a business contact address/number if the subscriber has notified the data controller that they do not consent to the receipt of such communications.

14d. SMS Messages with "tagged on" marketing

A non-marketing SMS message may not have marketing material "tagged on" unless the recipient has given prior consent to the receipt of such messages. This would apply, for example, to such messages "tagged on" to communications from clubs or societies and information messages from service providers.

15. Enforcement and Compliance

The Data Protection Commissioner enforces the data protection aspects of the Regulations, and the Commission for Communications Regulation (ComReg) is responsible for ensuring compliance with some technical and practical elements of implementing the Regulations. In carrying out his functions, the Commissioner has broadly the same: powers of inspection, information gathering and enforcement that he has under the Data Protection Acts.

16. Offences and Penalties

Failure to comply with certain provisions of the Regulations are criminal offences:

· Data Security and Data Breaches
· Unsolicited Marketing Communications
· Requirements specified in Information and Enforcement Notices issued by the Commissioner
· Requirements imposed by the Commissioner's authorised officers.

The offences attract a fine of up to €5,000 – per message in the case of unsolicited marketing – when prosecuted by the Commissioner in the District Court.

Unsolicited marketing offences may be prosecuted on indictment and attract fines of up to €250,000 in the case of a company and €50,000 in the case of an individual. A data security offence may similarly be prosecuted on indictment and attract the same level of penalty.

(1) Directive 2002/58/EC, as amended by Directive 2006/24/EC and Directive 2009/136/EC

(2) A cookie is a small file that can be downloaded to a PC or other device when the user accesses certain websites. A cookie allows a website to "recognise" the user's device.