Guidelines on the Privacy of Individuals and Data Protection in the Telecommunications Sector

Guidelines Issued by the Telecommunications Regulatory Authority

Guidelines on the Privacy of Individuals and Data Protection in the Telecommunications Sector

Introduction

The Telecommunications Regulatory Authority (the "**TRA**") issued these guidelines on the privacy of individuals and data protection in the telecommunications sector (the "**Guidelines**") pursuant to Article 3(b) of the Telecommunications Law which requires the TRA *"to protect the interests of subscribers and users in respect of protection of personal particulars and privacy of services".* On this basis the TRA has now drafted these Guidelines which will assist in the Processing, retention and transferring of Personal Data related to Subscribers or Users by providers of Telecommunications Services or operators of Telecommunications Networks (or by Processors on their behalf).

The purpose and scope of these Guidelines is therefore to provide a framework that regulates the processing of personal data in the telecommunications sector. These Guidelines therefore enhance the rules for Processing Personal Data when that processing is carried out in the course of providing a telecommunications service. These Guidelines define the obligations of Data Controllers and Data Processors and also define the rights of Data Subjects. In so doing these Guidelines seek to protect Personal Data against any act of misuse, or accidental loss or destruction and to prevent any unlawful Processing.

These Guidelines will be kept under review and amended by TRA as appropriate in the future. These Guidelines do not serve to act as a substitute to the provisions of the Personal Data Protection Law. Data Processors remain responsible to ensure compliance with the provisions of that law.

1. Definitions

Any word, phrase or expression used in these Guidelines shall, unless it is expressly defined herein, have the same meaning as in the Telecommunications Law or the Personal Data Protection Law. The terms and phrases below shall have the following meaning, unless the context requires otherwise:

Communication/s: means any information exchanged or transmitted between a finite number of parties by means of a telecommunications service. This does not include any information conveyed as part of a broadcasting service to the public over a

Telecommunications Network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;

Consent: means any freely given specific, informed and explicit indication of a Data Subject's wishes by which the Data Subject explicitly in writing signifies agreement to Personal Data relating to him or her being processed;

Licensed Operator: means an operator of a Telecommunications Network or the provider of Telecommunications services, as the case may be, which determines the purposes, conditions and means of the Processing of Personal Data;

Directory of Data Subjects or Directory: means a Directory of Data Subjects to Public Telecommunications services, whether in printed form or in electronic form, which is generally available to the public and for a fee or free of charge and is based on data obtained directly or indirectly from a Licensed Operator in the Kingdom of Bahrain which assigns telephone numbers to Data Subjects;

Infrastructure: means the basic physical and organizational systems and facilities (e.g. buildings, network equipment, power supplies, people and processes) needed for the operation of a Telecommunications Services;

Location Data: means any data processed in a Telecommunications Network or by means of Telecommunications services, indicating the geographic position of the Terminal Equipment of a Data Subject using telecommunications services;

Personal Data: means any information in any form relating to an identified or identifiable natural person (the "Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a user name or subscriber information, an identification number, Location Data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

Personal Data Breach: means a breach of security, including unauthorized access to data, applications, networks and/or facilities that results in a potentially significant impact on the operation of an Infrastructure, leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed, in connection with a telecommunications service;

Processor: a natural or legal person, other than an employee of the Data Controller or data Processor, who processes personal data for the Data Controller's benefit and on the Data Controller's behalf;

Recipient: means a natural or legal person or any other body to who or to which the Personal Data is disclosed;

Terminal Equipment: means a product, or a component of a product, which is intended to be connected directly or indirectly to interfaces of public telecommunications networks;

Traffic Data: means any data processed for the purpose of the conveyance of a Communication, or for the use of a telecommunications service on a Telecommunications Network or for the billing thereof;

Value Added Service: means enhanced or value added telecommunications data and/or voice services, which require the Processing of Traffic Data or Location Data other than Traffic Data beyond what is necessary for the transmission of a Communication, or for the use of a telecommunications service, or the billing thereof.

2. Scope of these Guidelines

2.1 These Guidelines apply to the Processing of Personal Data in connection with the operation of Telecommunication Networks and the provision of telecommunications services in the Kingdom.

2.2 These Guidelines do not apply to the Processing of Personal Data that is exempted by virtue of Article 2(4) of the Personal Data Protection Law.

2.3 Nothing in these Guidelines should be interpreted as precluding the furnishing by Data Controllers of Personal Data to any competent public authority in the Kingdom in accordance with any laws and regulations that may be applicable in the Kingdom.

3. Territorial Scope of these Guidelines

These Guidelines shall apply to the Processing of Personal Data carried out in the context of (i) the provision of a telecommunications service or the operation of a telecommunications network in the Kingdom including communications networks supporting data collection and identification devices; or (ii) when a Subscriber is using an international telecommunications roaming service provided by a mobile network operators licensed to provide telecommunications services in the Kingdom.

4. Requirements Imposed on Data Controllers

4.1 Without prejudice to any applicable law in the Kingdom, Data Controllers may, without the Data Subject's Consent, Process Personal Data for the following purposes:

(a) the provision of telecommunications services to Data Subjects;

(b) activities concerning Data Subject billing;

(c) activities concerning the payment of interconnection and roaming settlements;

(d) activities concerning access to Data Subject Terminal Equipment in accordance with section 14 of these Guidelines;

(e) activities concerning Traffic Data in accordance with section 15 of these Guidelines;

(f) for instances of fraud and cybersecurity attacks;

(g) activities concerning Location Data in accordance with section 16 of these Guidelines; and

(h) reporting a Personal Data Breach.

4.2 Data Controllers who Process Personal Data for the purposes indicated in section 4.1 of these Guidelines should not Process that Personal Data for any other purpose.

4.3 Except where Personal Data is processed under Section 4.1, Data Controllers should only process Personal Data in adherence with the requirements of sections 5, 6 and 7 of these Guidelines.

4.4 Data Controllers should ensure that:

(a) Personal Data is Processed fairly and lawfully;

(b) Personal data is collected for specific, explicit and legitimate purpose and shall not be further processed in a way incompatible with the purpose for which it was collected. Further processing of Personal Data for historical, statistical or scientific purposes shall not be considered incompatible with this requirement subject to

ensuring that the data is not processed for supporting any decision or measure regarding a particular individual.

(c) any Personal Data that is Processed is adequate, relevant, and limited to the minimum necessary in relation to the purposes for which it is Processed;

(d) any Personal Data that is Processed is accurate and kept up to date, and that every reasonable step is taken to ensure that any inaccurate Personal Data is erased or rectified without delay;

(e) all reasonable measures are taken to complete, correct, block or erase Personal Data to the extent that such data is incomplete or incorrect;

(f) Personal Data that is transferred outside of the Kingdom is subject to appropriate and necessary privacy safeguards in accordance with Article 12 of the Personal Data Protection Law; and

(g) Personal Data is kept in a form which permits identification of Data Subjects for no longer than is necessary, in accordance with laws applicable in the Kingdom.

5. Criteria of Processing Personal Data

5.1 Personal Data should only be Processed in accordance with the criteria set out in Article 4 of the Personal Data Protection Law (as may be amended from time to time):

(a) the Data Subject has given Consent to the Processing of his Personal Data for one or more specific purposes; or

(b) Processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract; or

(c) Processing is necessary for compliance with a legal or regulatory obligation to which the Data Controller is subject; other than an obligation imposed by contract,

or the compliance with orders issued by a competent court or the Public Prosecution; or

(d) Processing is necessary in order to protect the vital interests of the Data Subject; or

(e) Pursuing the legitimate interests of the Data Controller or any third party to whom personal data has been disclosed to, provided that it is not in conflict with fundamental rights and freedoms of the data subject.

5.2 Where a Data Controller obtains from Data Subjects, Personal Data in the context of the provision of a telecommunications service, the Data Controller may use that Personal Data for its own direct marketing. Provided that Data Subjects are given the opportunity to opt-out, free of charge and in an easy manner, from such Processing for direct marketing. In so doing, Data Controllers must, at all times, conduct themselves in accordance with Article 20 of the Personal Data Protection Law.

6. Conditions for Consent

6.1 Without prejudice to Section 4.1 of these Guidelines, Consent to the Processing of Personal Data should be obtained prior to the commencement of any Processing activity by the Data Controller and it should be:

(a) clear;

(b) specific to the purpose;

(c) unambiguous; and

(d) freely given by the Data Subject.

6.2 Consent must be in writing, or in electronic format, including but not limited to, by means of a tick box or signature box, signifying the Data Subject's Consent.

6.3 A Data Subject has the right, at any time, free of charge, to object to the Processing of his or her Personal Data and to withdraw his or her Consent. The withdrawal of Consent should not affect the lawfulness of Processing that has been carried out on the basis of that Consent before its withdrawal.

7. Information to Data Subjects

7.1 When Processing Personal Data, Data Controller should provide Data Subjects with, at least, the following information:

(a) the identity and habitual residence or principal place of business of the Data Controller and of the Processor;

(b) clear and comprehensive information about the purposes of Processing;

(c) any further information that enables the Data Subject to pursue his/her rights as prescribed under the provision of the Personal Data Protection Law and these Guidelines;

(d) any further information relating to matters including:

I. the Recipients or categories of the Recipients of Personal Data;
II. whether the Personal Data will be used for direct marketing purposes; and
III. the existence of the right to access, the right to rectify, and the right to erase the Personal Data concerning the Data Subject and any other right that a Data Subject may have under these Guidelines or the Personal Data Protection Law.

8. Right of Access

8.1 Any Data Subject has the right to request, at reasonable intervals, information about his or her Personal Data from any Data Controller. Data Controllers should provide to the Data Subject in the manner set out in section 8.3 of these Guidelines information about the Processing of their Personal Data, without excessive delay and without expense for the Data Subject:

(a) written or electronic confirmation as to whether Personal Data concerning the Data Subject is processed;

(b) details of the Personal Data about the Data Subject which is Processed;

(c) the purpose of the Processing;

(d) the right of Data Subjects to lodge a complaint to the TRA or to the Personal Data Protection Authority;

(e) where possible, the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period; and

(f) Recipients or categories of Recipients to whom the data is disclosed.

8.2 An application under section 8.1 of these Guidelines should be made in writing to the Data Controller and is to be signed by the Data Subject provided that where an application under section 8.1 is deemed to be disproportionate, then the Data Controller may reject the application in accordance with Article 18 of the Data Protection Law.

8.3 The information provided under section 8.1 should be provided in a concise, transparent, intelligible and easily accessible form using clear and plain language.

8.4 Data Controllers should fulfil the request made by the Data Subject under section 8.1 of these Guidelines as soon as possible and in any event within the timeframe set out in the Personal Data Protection Law.

8.5 The information may be provided in any of the following methods/modalities:

(a) Hard copy;

(b) Electronically by email; and

(c) Layered approach, in the event of large quantity of data.

9. Rectification and Erasure of Personal Data

9.1 Data Controllers should, without undue delay (and in all instances within the timeframe set out in the Personal Data Protection Law where this is possible and achievable), upon request from a Data Subject rectify inaccurate, incomplete, outdated, or illegal Personal Data concerning that Data Subject.

9.2 Data Controllers should, without undue delay (and in all instances within the timeframe set out in the Personal Data Protection Law), upon request from a Data Subject erase Personal Data concerning that Data Subject where one of the following grounds applies:

(a) the Personal Data is no longer necessary in relation to the purposes for which it was collected or otherwise Processed;

(b) the Data Subject withdraws his or her Consent to the Processing and where there is no other legal ground for Processing; or

(c) the Personal Data has been unlawfully Processed.

10. Processing by the Processor

10.1 The Processor, and any other person acting under the authority of the Data Controller, who has access to Personal Data, should not Process the Personal Data except on instructions from the Data Controller or to cover the performance of a contract with the Data Controller where that contract satisfies the requirements of Art. 5.1 (b) of these Guidelines or unless required to do so by an obligation provided by a law applicable in the Kingdom.

10.2 Where a Processing operation is to be carried out on behalf of a Data Controller, the Data Controller should appoint a Processor who is capable of providing appropriate technical and organisational measures in such a way that the Processing will meet the requirements of these Guidelines and the Data Protection Law.

10.3 The Processing of Personal Data by a Processor should be governed by a contract or other legal instrument binding the Processor to the Data Controller and stipulating that the Processor should:

(a) act only on instructions from the Data Controller;

(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;

(c) take all required security measures pursuant to section 11 of these Guidelines;

(d) insofar as this is possible, given the nature of the Processing, create, in agreement with the Data Controller, the necessary technical and organisational requirements, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the Data Subject's rights;

(e) assist the Data Controller in ensuring conformity with the requirements under section 11 and section 13 of these Guidelines;

(f) at the choice of the Data Controller, delete or return all the Personal Data to the Data Controller after the end of the provision of services relating to Processing, and delete existing copies; and

(g) make available to the Data Controller and the TRA all information necessary to verify the adherence to these Guidelines.

11. Security of Processing

11.1 Without prejudice to any other obligation imposed on Data Controllers under the laws and regulations of the Kingdom, Data Controllers and Processors should:

(a) take reasonable steps to ensure a level of security appropriate to the risks represented by the Processing, and the nature of the Personal Data to be protected;

(b) take appropriate technical and organisational measures required to protect Personal Data against unintentional or unlawful destruction or accidental loss, and to prevent any unlawful forms of Processing, in particular, any unauthorised disclosure, dissemination or access, or alteration of Personal Data; and

(c) take reasonable steps to ensure that Personal Data can be accessed only by authorised personnel.

12. Notification of a Personal Data Breach to the TRA

12.1 In the case of a Personal Data Breach, the Data Controller should without undue delay, and not later than seventy-two (72) hours after having become aware of it, notify the Personal Data Breach to TRA. The notification to the TRA must be accompanied by a reasoned justification in cases where it is not made within seventy-two (72) hours.

12.2 Data Controllers are required to submit a detailed report to the TRA within five (5) working days after becoming aware of any Personal Data Breach.

12.3 The detailed report submitted pursuant to section 12.2 of these Guidelines should include the following information:

(a) the date and time that the Personal Data Breach commenced;

(b) the date and time that the Personal Data Breach was resolved completely. Where the breach is ongoing at the time of reporting, the expected resolution time should be provided when it is available;

(c) physical location of the Personal Data Breach, which as a minimum, should contain the address; and

(d) a brief description of the Personal Data Breach, including the cause, resultant damage, the estimated financial loss and mitigation action taken by the Data Controller.

12.4 Where TRA receives a report under this section, the TRA may, where it thinks it appropriate, inform:

(a) the Subscriber or Data Subject of the occurrence of the Personal Data Breach or require the Data Controller to inform the Subscriber or Data Subject; and/or

(b) the public of the occurrence of the Personal Data Breach, or require the Data Controller to inform the public; and/or

(c) Personal Data Protection Authority or security organs or concerned government entities of such report.

13. Confidentiality of Communications

13.1 Data Controllers must ensure the privacy and confidentiality of Communications and related Traffic Data generated by means of a Telecommunications Network and telecommunications services.

13.2 Data Controllers should not use or allow to be used any apparatus contained in the Telecommunications Network which is capable of recording, listening, tapping, silently monitoring, or intruding into Communications of a Data Subject, and of any related Traffic Data, unless this complies with the laws of the Kingdom.

14. Access to Data Subject Terminal Equipment

14.1 The storing of information, or the gaining of access to information already stored, in the Terminal Equipment of a Subscriber or User is only allowed on condition that the Subscriber or User concerned has given his or her consent, having been provided with clear and comprehensive information, including, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over a Telecommunications Network, or as strictly necessary in order for the provider of telecommunications services explicitly requested by the Subscriber or User to provide the service.

14.2 Nothing in these Guidelines should preclude a Processor from Processing Personal Data for the purpose of carrying out the transmission of Communication over a Telecommunication Network, where that Processing is carried out in accordance with Article 5 of these Guidelines.

14.3 Nothing in these Guidelines should preclude Data Controllers instructed by a competent authority, from storing information or gaining access to information stored in the Terminal Equipment of a Data Subject, for the purposes established by the laws and regulations applicable in the Kingdom.

15. Processing of Traffic Data

15.1 Without prejudice to section 15.2, 15.3 and 15.4 of these Guidelines, and unless required by any other provision of the laws and regulations of the Kingdom or any regulation published by the TRA or Licence, Traffic Data relating to a Data Subject that is Processed for the purpose of the transmission of a Communication, and stored by a Data Controller, must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a

Communication following the lapse of one year from the date of the Data Subjects' Communication.

15.2 Traffic Data necessary for the purposes of Data Subject billing and interconnection payments may be Processed, provided that such Processing should only be permissible up to the end of the period during which the bill may lawfully be challenged or payment pursued, in accordance with the laws of the Kingdom.

15.3 For the purpose of marketing its own Telecommunications services or for the provisions of Value Added Services to the Data Subject, the Data Controller may process the data referred to in section 15.1 of these Guidelines to the extent and for the duration necessary for such services.

15.4 Upon a request for information by a Data Subject, a Data Controller must inform the Data Subject of the types of Traffic Data that are processed and of the duration of such Processing for the purposes mentioned in section 15.1 and 15.2 of these Guidelines.

15.5 Processing of Traffic Data in accordance with this section 15 of these Guidelines must be restricted to persons acting under the authority of the Data Controller and any Processor, including, undertakings which provide telecommunications services handling billing or traffic management, customer enquiries, fraud detection, marketing or providing a Value Added Service.

15.6 Nothing in these Guidelines will preclude the furnishing of Traffic Data to any competent authority for the purposes of settling disputes, in particular interconnection or billing disputes.

16. Processing of Location Data

16.1 Data Controllers may process Location Data, other than Traffic Data, relating to Data Subjects using a Telecommunications Network or a telecommunications service, in accordance with section 4.1 of these Guidelines, provided that the Data Controller provides the Data Subject with clear and comprehensive information prior to that use in accordance with section 7 of these Guidelines, including the following information:

(a) the type of Location Data other than Traffic Data processed;

(b) the purposes and duration of the Processing; and

(c) transmission of any Traffic Data to a third party for the purpose of providing the Value Added Service.

16.2 Location Data should, where possible, be processed when it is made anonymous, to the extent and for the duration necessary for the provision of a Value Added Service.

16.3 Data Subjects may, at any time, withdraw their Consent to the Processing of Location Data, other than Traffic Data.

17. Directory Services

17.1 Any Licensed Operator who produces a Directory of Data Subjects must ensure that:

(a) the Data Subject is informed about the Directory of Data Subjects where available;

(b) the Data Subject is given the opportunity to allow or refuse for their data to be included in the Directory by the Licensed Operator, free of charge;

(c) the Data Subject should be given the opportunity to access, verify, correct or withdraw such Personal Data from the Directory, free of charge, as provided in these Guidelines;

(d) Data Subjects' information is updated regularly; and

(e) the Personal Data in such a Directory relating to a Data Subject is limited to what is necessary to identify the Data Subject and the number allocated to him.

17.2 These Guidelines do not apply to an edition of a Directory that has been already produced or placed on the market in printed or off-line electronic form before the issuance date of these Guidelines.

17.3 Licensed Operators must provide any other Licensed Operator access to its Directory information on request, in such form as may be determined by the TRA, on reasonable, fair and non-discriminatory terms, including reimbursement of the Licensed Operator's direct costs reasonably incurred in granting the access, provided that:

(a) the Licensed Operator to whom Personal Data is disclosed, should process the information only to provide Directory information services or for the routing of calls;

(b) the Licensed Operator must not disclose Personal Data related to Data Subjects who have refused for their Personal Data to be included in the Directory or withdrawn their Consent to the inclusion of their Personal Data in the Directory; and

(c) the provision by the Licensed Operator to other Licensed Operators of the information is in line with the provisions of these Guidelines.

18. Itemised billing

Subscribers should have the right to receive non-itemised bills.

19. Confidentiality

The TRA may request a Data Controller to furnish information or documents in its possession, to satisfy the TRA that the privacy and confidentiality procedures adopted by the Data Controller satisfy the requirements under these Guidelines.

20. Effective date

These Guidelines will come into effect after the lapse of 6 months from the date of their publication.