Dialog Axiata PLC

Data Protection and Privacy Clauses

1. Purpose

The purpose of this document is to ensure adherence to the privacy and data protection provisions, as morefully set out herein, by any Contracting Party of Dialog.

2. Definitions

1.1 Definitions

In this document the following expressions shall, unless the context otherwise requires, have the meanings assigned to them below:

"**Affiliate**" means in relation to a party any entity which, directly or indirectly, controls or is controlled by, or is under common control with, that party, where control is the possession, directly or indirectly, of (a) alone or pursuant to an agreement with other members, a majority of the voting rights in it, (b) the power to direct or cause the direction of the management or operating policies of the entity through the exercise of voting rights, contract, trust or otherwise, or (c) a right to appoint or remove the majority of the directors of the entity, and "Affiliates" means any of them;

"**Best Industry Practice**" means, in relation to any undertaking and any circumstances, the exercise of the degree of skill, care, diligence, prudence, foresight and judgement which could reasonably be expected from highly skilled, experienced persons, entities and world leading suppliers and contractors engaged in comparable types of undertaking under similar circumstances, applying equivalent or better standards currently applied in the industry relevant to the Professional Services and any other products, works and services that may become available to ensure, without limitation, the objectives and obligations identified in the Agreement are achieved and performed that include best practices and value in respect of price, performance and time to market;

"**Contracting Party/s**" shall mean those parties that provide Professional Services to Dialog and shall also be referred to as Contractor/s and/or Service Provider/s.

"**Data Protection and Privacy Schedule**" means this schedule and any amendments effected by Dialog from time to time.

"**Data Subject**" means an individual who is the subject of the Personal Data;

"**Dialog**" means Dialog Axiata PLC and any of its subsidiaries and associated companies.

"**Dialog Data**" includes, but is not limited to, the data, text, drawings, diagrams, plans, statistics or images (together with any database made up of any of these) which are embodied in any electronic, magnetic, electromagnetic, optical, tangible or other media,:

(a) which are supplied to the Contracting Party by or on behalf of Dialog or

(b) which the Contracting Party accesses, processes, stores, transmits or replicates using or on the Contracting Party's systems or equipment pursuant to the Agreement; or

(c) which the Contracting Party has custody or control of for purposes connected to the Agreement,

including any Personal Data which Dialog controls the Processing of, or which comes into the knowledge, possession or control of the Contracting Party pursuant to the Agreement;

For the sake of clarity, Dialog Data includes Confidential Information as defined in the Agreement and Personal Data as defined in this Data Protection and Privacy Schedule.

"**Dialog Systems**" means the hardware (including computer hardware), software and telecommunications or information technology equipment, systems and networks used or owned by Dialog or licensed to Dialog by a third party;

"**Deliverables**" means the items set out in the Agreement identified as the scope of work and shall include any amendments and modifications as requested by Dialog from time to time and shall include anything compiled, written, provided, created and developed by the Contracting Party in relation to the Professional Services, including but not limited to materials, studies, methodologies, models or general industry perspective and practices, plans, drawings, diagrams, statistics and reports;

"**Malware**" means anything, software or device which may impair or otherwise adversely affect the operation of any computer or system, prevent or hinder access to any program or data (whether by rearranging within the computer or any storage medium or device, altering or erasing, the program or data in whole or in part, or otherwise), gain unauthorised access to any program, equipment, system or data or collect data or surveillance without authorisation, including worms, Trojan horses, computer viruses, ransomware, spyware or similar things;

"**Party**" means a party to the Agreement and "**Parties**" means the parties to the Agreement;

"**Personal Data**" means personal data, personal information or data relating to individuals;

"**Personnel**" means in relation to a party, the employees, directors, officers, agents, advisers, contractors and subcontractors of that party or of its Affiliates or associates, and the employees, directors and personnel of any such agents, advisers, contractors and subcontractors. The Contracting Party's Personnel shall, in addition to the foregoing, include Sub-Processors;

"**Process**" or "**Processing**" means collecting, recording, holding or storing Personal Data or carrying out any operation or set of operations on Personal Data, including:

(a) the organization, adaptation or alteration of Personal Data;

(b) the retrieval, consultation or use of Personal Data;

(c) the disclosure of Personal Data by transmission, transfer, dissemination or otherwise making available; or

(d) the alignment, combination, correction, erasure or destruction of Personal Data;

"**Professional Services**" means the services to be provided by the Contracting Party to Dialog which includes the Deliverables as more particularly set out in the Agreement;

"**Sub-Processor**" means any party appointed by, or on behalf of, the Contracting Party to Process Personal Data of Dialog in connection with this Agreement

1.2 Interpretation

1.2.1 In this Agreement, unless the context otherwise requires:

a. words denoting the singular number include the plural and vice-versa;

b. words denoting a gender include every gender;

c. words denoting natural persons include bodies corporate and unincorporated;

d. reference to a clause, annexure or schedule is a reference to a clause, annexure or schedule to this Agreement;

e. references to any legislation or law or to any provision of legislation or law shall include any modification or re-enactment of that legislation or law or any legislative provision substituted for such provision of legislation or law and all regulations and statutory instruments issued under such legislation or law;

f. the table of contents, headings and bolding are inserted for convenience only and shall not affect the construction or interpretation of this Agreement;

g. the Recitals and Schedules hereto and any documents herein referred to shall be taken, read and construed as an essential and integral part of this Agreement; and

h. all references to time are to Sri Lanka time.

1.2.2 A rule of construction does not apply to the disadvantage of a Party because the Party was responsible for the preparation of this Agreement or any part of it.

2. Data Security and Protection

2.1 In supplying the Deliverables and performing the Professional Services, and in carrying out the other tasks allocated to it in this Agreement, the Contracting Party shall in accordance with Best Industry Practice:

(a) do all things that a reasonable and prudent entity would do to ensure that all Dialog Data are protected at all times from accidental, unauthorised or unlawful access, processing or Processing, use or transfer by a third party or loss, misuse, damage or destruction by any person, including adopt and implement all appropriate technical and organisational measures and controls;

(b) provide and implement protective policies, processes, measures and controls for the Dialog Data that are no less rigorous than accepted industry standards and commensurate with the consequences and probability of accidental, unauthorised or unlawful access to, processing or Processing, use or transfer of, or the loss, misuse, damage or destruction of, the Dialog Data. The Contracting Party shall provide Dialog with an up-to-date copy of its written physical, technical and organizational security measures;

(c) comply with Dialog's information technology, security, access and usage policies, procedures and directions set out in the Agreement or notified to it from time to time;

(d) take all necessary steps to prevent any Malware being introduced into any software or onto any of the Dialog Systems or any information technology equipment (including computer hardware), systems or networks used by the Contracting Party to access, process or Process, store, transmit or generate Dialog Data or to supply the Professional Services to Dialog;

(e) not access or attempt to access the Dialog Systems without the prior written consent of Dialog;

(f) procure that no unauthorised third party will, as a result of any act or omission of the Contracting Party or its Personnel, obtain access to any of the Dialog Data or Dialog Systems;

(g) apply security procedures, measures and controls to guard against the misuse, loss, damage, destruction, corruption or alteration of the Dialog Data in the possession or

control of (or accessed by) the Contracting Party or its Personnel;

(h) ensure that it does not deliberately or negligently misuse, lose, damage, destroy, corrupt, alter or erase the Dialog Data on the Dialog Systems or on its own equipment or systems;

(i) not disclose or share passwords, authentication tokens or credentials supplied by Dialog to access the Dialog Systems to any person other than its personnel with a need to know and revoke or remove such access immediately upon any such personnel no longer having the need to know or leaving the Contracting Party;

(j) immediately notify Dialog of any breach of (a) to (i) above; and

(k) develop or adapt for acceptance by Dialog a Data Protection Plan ("**DPP**") that sets out how the Contracting Party will deal with and discharge its obligations in respect of Dialog Data (including Personal Data) during the provision of the Professional Services. The DPP must:

(i) be consistent with the requirements of this Data Protection and Privacy Schedule (including this Clause 2);

(ii) be consistent with the requirements of all relevant privacy or data protection and other laws, including the privacy or data protection laws of jurisdictions where any Dialog Data is stored, managed or transited;

(iii) specifically deal with cybercrime or cybersecurity risks, including protecting against and monitoring actual, attempted or potential unauthorised access and rapidly responding to any unauthorised access, cybercrime or cybersecurity breaches in order to limit the effects of such access, crime or breach and the occurrence of any other such access, crime or breach;

(iv) set out the steps and processes that the Contracting Party and Dialog will follow to protect the Dialog Data from actual, attempted or potential unauthorised or unlawful access, use, processing or Processing, or transfer, or misuse, damage, destruction, loss or corruption and rapidly respond to any unauthorised or unlawful access, cybercrime or cybersecurity breaches; and

(v) include any comments from or requirements of Dialog from time to time,

and once accepted by Dialog, the Contracting Party must comply with the DPP.

2.2 If the Contracting Party becomes aware of any actual or suspected:

(a) action taken through the use of computer networks that attempts to access the Contracting Party's information system or Dialog Data residing on that system or that results in any actual or potential adverse effect on the Contracting Party's information system or Dialog Data residing on that system (a **"Cyber Incident"**);

(b) any other unauthorised access or use by a third party or misuse, damage or destruction by any person (an **"Other Incident"**); or

(c) breach of any applicable law by the Contracting Party (a "**Breach**"),

the Contracting Party shall:

(i) notify Dialog in writing immediately (and no longer than 2 hours after becoming aware of the Cyber Incident, Other Incident or Breach) providing full details of the Cyber Incident, Other Incident or Breach and keep Dialog updated at all times thereafter in relation to the Cyber Incident, Other Incident or Breach; and

(ii) provide sufficient information and assistance to allow Dialog to meet their respective obligations to report the Cyber Incident, Other Incident or Breach to the relevant authorities or inform the Data Subjects under the applicable privacy or data protection and other laws. The Contracting Party shall co-operate with Dialog and the relevant authorities to take all reasonable steps to assist in the investigation, mitigation and remediation of the Cyber Incident, Other Incident or Breach;

(iii) comply with the DPP and all other directions issued by Dialog in connection with the Cyber Incident, Other Incident or Breach, including in relation to:

(1) notifying any relevant body, as required by the DPP or Dialog;

(2) obtaining evidence (including digital forensic evidence) about how, when and by whom the Contracting Party's information system or Dialog Data has or may have been compromised, providing it to Dialog on request, and preserving and protecting that evidence for a period of at least 12 months;

(3) implementing any mitigation strategies to contain and reduce the impact of the Cyber Incident, Other Incident or Breach or the likelihood or impact of any future similar event, incident or breach; and

(4) recovering and restoring the Professional Services (if affected) and preserving and protecting Dialog Data (including as necessary reverting to any backup or alternative site or taking other action to recover Dialog Data).

2.3 The Contracting Party shall take out and maintain insurance to protect against the risks of a Cyber Incident, Other Incident or Breach and comply with the provisions of that insurance.

2.4 The Contracting Party shall ensure that:

(a) all subcontracts, other supply chain arrangements and contracts with Sub-Processors, which may allow or cause access to Dialog Data, contain provisions that are at least as stringent as those in this Clause 2 and do not contain any provisions that are inconsistent with this Clause 2; and

(b) all the Contracting Party's Personnel who have access, directly or indirectly, to Dialog Data or Dialog Systems comply with this Clause 2 as if the Personnel were the Contracting Party.

2.5 The Contracting Party shall at all times comply with the relevant laws in Sri Lanka and legislation in other jurisdictions on personal data (collectively "**Personal Data Laws**") in respect of the Processing, dealing, remote access or transfer of Personal Data of Dialog, including but not limited to Personal Data of the customers or employees of Dialog. The Contracting Party shall not do or omit to do anything that would cause Dialog to contravene, or that would result in Dialog contravening, any Personal Data Laws.

2.6 The Contracting Party shall only Process Personal Data of Dialog for the sole purpose of performing the Professional Services and in accordance with the respective instructions and policies of Dialog. The Contracting Party shall immediately notify Dialog if it believes that the data Processing instruction infringes the applicable privacy or data protection laws.

2.7 The Contracting Party shall not transfer or remotely access Personal Data of Dialog without the prior written consent of Dialog. The Contracting Party shall ensure that any transfer of, or remote access to, Personal Data of Dialog does not contravene any provisions of this Agreement or any applicable laws and that such Personal Data is adequately protected at all times. All transfer of such Personal Data shall be encrypted or be secured in other ways.

2.8 The Contracting Party shall not engage a Sub-Processor to Process any Personal Data of Dialog or change any Sub-Processor without the prior written consent of Dialog. Where the Contracting Party engages any such Sub-Processor, the Contracting Party shall ensure that

the Sub-Processor adheres to the same obligations as the Contracting Party's obligations with respect to Dialog Data (including Personal Data) and Confidential Information in the Agreement. The Contracting Party shall be responsible for verifying the Sub-Processor's compliance. The Contracting Party shall be fully responsible to Dialog for any non-compliance by any Sub-Processor with the aforesaid obligations or any applicable laws.

2.9 The Contracting Party shall assist Dialog to handle and comply with their respective obligations in complying with Data Subjects' rights. If the Contracting Party or its Sub-Processor receives a complaint or any request (including any request for access to Personal Data) from any Data Subject or his/her agents, or from any authority, the Contracting Party must, without undue delay, inform Dialog of the complaint or request. Upon request by Dialog, the Contracting Party shall, without undue delay, supply the information to Dialog to enable them to respond to such complaint or request. The Contracting Party shall not respond to these complaints or requests unless instructed in writing by Dialog.

2.10 The Contracting Party shall establish and maintain a record of Personal Data Processing activities in electronic form. Such record shall, at the minimum, contain the following information:

(a) types/categories of Personal Data Processed;
(b) transfer details, including countries transferred to and the safeguards for the transfer;
(c) information of the Sub-Processor and details of the Processing activity;
(d) specific data security requirements;
(e) information of the Contracting Party and its Data Protection Officer or appointed officer responsible for the Processing of Personal Data;
(f) technical and organizational security measures employed by the Contracting Party to safeguard Personal Data.

The Contracting Party shall furnish a copy of the up-to-date record to Dialog upon request.

2.11 The Contracting Party shall provide reasonable assistance to Dialog with any data protection impact assessment and consultation with supervisory authority, when required by Dialog.

2.12 (a) Dialog may conduct, or require a third party nominated by them to conduct, a security audit of the Contracting Party's facilities, safeguards, policies, procedures and security measures in place to protect the Dialog Data and Confidential Information at any time and from time to time during the Term, including if directed by the data protection authority or if necessary due to any accidental, unauthorised or unlawful access to, processing or Processing, use or transfer of, or loss, misuse, damage or destruction of, any Dialog Data. The Contracting Party shall make available all information necessary to demonstrate compliance with the provisions of this Agreement and privacy or data protection laws. The Contracting Party may engage its own auditor, provided such auditor is acceptable to Dialog, and shall furnish the auditor's report to Dialog for their review. Subject to Clause 2.12(b), each Party will bear its own cost of audit.

(b) Dialog will review the results of the security audit with the Contracting Party. If such results demonstrate that the Contracting Party has breached any of its obligations, or that the Contracting Party's safeguards and security measures in place to protect Dialog Data or Confidential Information do not meet industry best practice standards, or there is a reasonable risk of material security breaches, the Contracting Party shall (without limiting Dialog's rights and remedies):

i. pay Dialog's costs associated with the security audit; and

ii. promptly take such steps as are necessary to remediate the issues identified in respect of the safeguards and security measures to at least the industry standard identified as adequate in the security audit and will provide to Dialog regular status updates of such remediation. The frequency of such status updates will be agreed upon by the Contracting Party and Dialog but in any event will be at least once every seven (7) days.

2.13 In respect of Personal Data:

(a) if compliance with any mandatory Personal Data Laws will result in any conflict with any provisions in this Agreement, the Contracting Party shall comply with such mandatory Personal Data Laws to the extent of the conflict; and

3. Consequences of Termination

3.1 Where the Agreement is terminated:

(a) the Contracting Party shall permanently destroy, or return to Dialog , all Confidential Information or deal with the same in the manner instructed by Dialog , within the earlier of the time period required under law (if any) and fourteen (14) days after the termination or expiry of this Agreement ("**Execution Date**"), and shall provide a written confirmation to this effect to Dialog within seven (7) days of the Execution Date;

(b) the Contracting Party shall, at no cost and expense to Dialog, make available Personnel and take immediate steps to assist Dialog to ensure a smooth transition if a third party has been appointed to replace the Contracting Party in the performance of its obligations under the Agreement. The Contracting Party shall support Dialog with any transfer of Personal Data to a third party if required by them;

(c) the Contracting Party shall take immediate steps to cease the Professional Services in a prompt and orderly manner, discontinue from making commitments and shall proceed to cancel all existing orders and terminate all works under the Agreement as promptly as is practicable and hand over all Deliverables and other related materials to Dialog; and

(d) Dialog shall not be liable to the Contracting Party by virtue of early termination of the Agreement including but not limited to any claim for loss of profits and revenue or prospective profits.

3.2 The termination or expiry of the Agreement shall not prejudice the rights of Dialog to sue for damages or to obtain any other relief in respect of any antecedent breach of the terms of this Data Protection and Privacy Schedule prior to such termination or expiry.

End of Document.