Data Processing Agreement

This Data Protection Agreement ("DPA") is entered into by and between Mobileum, Inc. and its Affiliates ("Mobileum"), and the Service Provider and its Affiliates identified in the Agreement and/or on the face of the purchase order and duly referenced and accepted by the Service Provider ("Service Provider") while accepting the Purchase Order. This SDPA is effective as of the date when a Purchase Order issued by Mobileum is accepted by the Service Provider (the "Effective Date") and remain in force for the term of the Agreement. Mobileum and Service Provider may be referred to individually as a "Party" or collectively as the "Parties."

This DPA is incorporated into and governed by the terms of the applicable Agreement entered into by and be-tween the Parties for the supply of Products and/or Services by Service Provider to Mobileum or any other terms wherein parties have agreed to this document (e.g. Mobileum's online purchase order terms (the "Agreement). Unless stated otherwise, in the event of a conflict between this DPA, including any attachments thereto, and the Agreement, the provisions of this DPA will control but only to the extent that Supplier Processes or has access to Protected Data in the Performance of its obligations to Mobileum.

Parties shall comply with all Applicable Laws, rules, policies, procedures, and all licenses, registrations, permits, and approvals required by any government or authority and any ambiguity in this DPA shall be resolved to permit Mobileum to comply with all Applicable Laws. In the event and to the extent that Applicable Laws impose stricter obligations on the Service Provider than under this DPA, the Applicable Laws shall prevail. Capitalized terms used herein and not otherwise defined shall have the meanings ascribed to them in the Agreement or as defined under Applicable Laws.

Unless otherwise specified in this DPA, the Agreement Terms will continue in full force and effect.. Any privacy or data related clauses previously entered by Mobileum and Service Provider, with regards to subject matter of this DPA will be superseded and replaced with this DPA. No one other than a Party to this DPA, successors and permitted assignees will have any right to enforce any of its terms.

Whereas,

A. Service Provider and Mobileum has entered into an Agreement whereby Service Provider has agreed to provide Services involving the Processing of Mobileum Personal Data, and such list will be updated from time to time. This DPA between Mobileum and the Service Provider shall

apply to all Processing of Mobileum Personal Data by Service Provider in order to provide the Services under the Agreement;

B. Mobileum may act as a Controller and/or Processor, on behalf of Other Controller, of the Mobileum Personal Data;

C. The Service Provider may be a Processor and/or Subprocessor processing Mobileum Personal Data on behalf of Mobileum.

The Parties agree as follows:

Article 1 – Definitions

i. **Controller** shall mean the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data;

ii. **Data Exporter** means the Controller located in a Member State whose Personal Data is being transferred to a Data Importer;

iii. **Data Importer** means a Subprocessor established in a country that is neither a Member State nor considered by the European Commission to have adequate protection;

iv. **Data Protection Laws** means the GDPR and all applicable Member State data protection laws and regulations, as amended, altered or replaced from time to time, as well as other regulatory requirements to which Mobileum or Mobileum's clients are subject, and any binding guidance or statutory codes of conduct issued by the relevant Privacy Authority(ies);

v. **Data Subject** is the identified or identifiable natural person, the Personal Data is relating to;

vi. **EU Standard Contractual Clauses** means the standard contractual clauses for the transfer of personal data to processors established in third countries (Commission Decision 2010/87/EC);

vii. **GDPR** means the General Data Protection Regulation 2016/679;

viii. **Member State** means a country that is a member of the European Union or the European Economic Area;

ix. **Other Controller** means any entity other than Mobileum that is Controller of the Mobileum Personal Data, such as Mobileum's Client's;

x. **Personal Data** shall mean any information relating to an identified or identifiable natural person ("Data Subject") which information is subject to the GDPR or the laws of non-EU EEA countries that have formally adopted the GDPR; an identifiable

natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, 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 natural person;

xi. **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;

xii. **Process, Processing or Processed** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

xiii. **Processor** means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller;

xiv. **Service(s)** means the services provided by Service Provider as agreed in the Agreement(s);

xv. **Subprocessor** means any subcontractor engaged by Service Provider for the Processing of Mobileum Personal Data in accordance with this DPA;

xvi. **Supervisory Authority** means an independent public authority which is established by a Member State pursuant to the GDPR;

xvii. **Client** shall mean an enterprise customer of a Mobileum group company in relation to whom the Service Provider might Process Personal Data;

xviii. **Mobileum Personal Data** means the Personal Data which Service Provider is Processing as Processor on behalf of Mobileum in order to provide the Services. Mobileum Personal Data may include both Personal Data controlled by Mobileum and Personal Data Mobileum is Processing on behalf of Other Controllers as Processor.

Article 2 – Mobileum Processing Instructions

1. This DPA applies if and to the extent Service Provider is Processing Mobileum Personal Data.
2. Service Provider warrants and undertakes in respect of all Personal Data Processed:
    a. It shall only Process Mobileum Personal Data for the sole purpose of providing the Services in accordance with Mobileum's documented instructions. The initial

scope of Mobileum's instructions for the Processing of Mobileum Personal Data is defined by the Agreements including, in particular, this DPA. In addition, Partis further agree to sign and fill **Exhibit 1 [Processing Details]** as and when required. The Exhibit 1 is only a sample and to be used as a template and once signed, **Exhibit 1** will form an integral part of the Agreement and this DPA.

b. Mobileum may provide further instructions that the Service Provider has to comply with. In case Service provider does not accommodate an instruction, Mobileum may terminate the affected part of the Service by providing Service Provider with a written notice. If Service Provider believes an instruction violates the Data Protection Laws, Service Provider will inform Mobileum without undue delay;

c. It shall not Process Mobileum Personal Data for its own purposes or include Mobileum Personal data in any product or service offered to third parties;

d. It shall not itself exercise control, nor shall it transfer, or purport to transfer, of Mobileum Personal Data to a third party, except as it may be specifically instructed, in documented form, to do so by Mobileum;

e. Mobileum shall serve as a single point of contact for Service Provider. Similarly, Service Provider will serve as a single point of contact for Mobileum and is solely responsible for the internal coordination, review and submission of instructions or requests from Mobileum to any Subprocessors;

f. Service Provider will comply with all Data Protection Laws in respect of the Services applicable to Processors and is responsible for the lawfulness of Service Provider's Processing of Mobileum Personal Data.

Article 3 - Transfer of Mobileum Personal Data and Processing outside of the EEA

1. Service Provider is not authorized, without prior written authorization by Mobileum and in accordance with its documented instructions, to transfer Mobileum Personal Data to third countries or international organizations, unless required to do so by Union or Member State law to which the Service Provider is subject; in such a case, the Service Provider shall inform Mobileum of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.
2. Where Mobileum Personal Data originating in the European Economic Area (EEA) shall be Processed by the Service Provider outside the EEA or in a territory that has not been designated by the European Commission as ensuring an adequate level of protection pursuant to the Data Protection Laws, the EU Standard Contractual Clauses shall apply to that Processing. The Service Provider shall ensure that the Processing of Mobileum Personal Data does not commence until has confirmed that it has obtained any approvals required from Mobileum, Mobileum's Clients and/or the relevant Supervisory

Authority, as applicable. If a Service Provider's approved Subprocessor is a Data Importer, in addition to the obligations set out in Article 4, Service Provider, on behalf of such Data Importer(s), shall enter into EU Standard Contractual Clauses with Mobileum. If this is not possible, Service Provider shall inform Mobileum and shall obtain such Data Importers' agreement to the EU Standard Contractual Clauses as an additional Data Importer.

Article 4 - Subprocessors

1. The engagement of Subprocessor(s) by Service Providers requires Mobileum's explicit prior written approval. The fact that Mobileum has agreed to the involvement of a respective subcontractor regarding the provision of Services, cannot be considered as an approval for such subcontractor to Process Mobileum Personal Data as Subprocessor.
2. Service Provider shall impose the same data protection obligations as set out in this DPA on any approved Subprocessor prior to the Subprocessor Processing any Mobileum Personal Data, and ensure that the relevant obligations (including but not limited to the information and audit rights provided for in this DPA) can be directly enforced by Mobileum or Other Controllers against the Service Provider's Subprocessors.
3. Where a breach of this DPA is caused by the actions of a Subprocessor, the Service Provider shall – if requested by Mobileum - assign to Mobileum the rights of the Service Provider to take action under the Service Provider contract with the Subprocessor. Mobileum may take action as it deems necessary in order to protect and safeguard Mobileum Personal Data.
4. Service Provider remains responsible for its Subprocessors and liable for their acts and omissions as for its own acts and omissions and any references to Service Provider's obligations, acts and omissions in this DPA shall be construed as referring also to the Service Provider's Subprocessors..

Article 5 - Third Party Requests and Confidentiality

1. Service Provider will not disclose Mobileum Personal Data to any third party, unless authorized by Mobileum or required by mandatory law. If a government or Supervisory Authority demands access to Mobileum Personal Data, Service Provider will notify Mobileum prior to disclosure unless prohibited by law.
2. Service Provider shall require all of its personnel authorized to process Mobileum Personal Data to commit themselves to confidentiality or assure that are under an appropriate statutory obligation of confidentiality and not Process such Mobileum Personal Data for any other purposes, except on instructions from Mobileum and/or

Other Controllers or unless required by applicable law, namely, Data Protection Laws. Such an obligation of confidentiality shall continue indefinitely. Service Provider shall demonstrate its compliance with this obligation by providing sufficient proof to Mobileum upon Mobileum's written request.

3. If a Data Subject brings a claim directly against Mobileum for damages suffered in relation to Service Provider's breach of this DPA or Data Protection Laws with regard to the processing of Mobileum Personal Data, Service Provider will indemnify Mobileum for any cost, charge, damages, expenses or loss arising from such a claim, provided that Mobileum has notified Service Provider about the claim and is giving the Service Provider the possibility to cooperate with Mobileum in the defence and settlement of the claim.
4. The Service Provider will remain liable for any disclosure or violation of Mobileum Personal Data by each of its personnel authorized to process Mobileum Personal Data as if it had made such disclosure or violation.

Article 6 - Security Measures

1. Service Provider shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, considering the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals.
2. The Service Provider shall implement and comply with the technical and organizational security measures identified **Exhibit 2 [Mobileum Security Requirements].**
3. Service Provider shall implement, namely, all necessary measures to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Mobileum Personal Data transmitted, stored or otherwise Processed under the Services and shall keep Mobileum Personal Data logically separated from data processed on behalf of any other third party.

Article 7- Assistance and Cooperation with Mobileum

1. Considering the nature of the Processing and the information available, the Service Provider shall assist Mobileum:
   a) Taking into account the nature of Processing, Service Provider will assist Mobileum by appropriate technical and organizational measures in the fulfillment of Mobileum's and/or Other Controllers' obligation to comply with the rights of Data Subjects and in ensuring compliance with Mobileum's and/or Other Controllers' obligations relating to the security of Processing, the notification of a Personal Data Breach and the data protection impact assessment, taking into account the information available to Service Provider.

b) To the extent permitted by law, Service Provider will inform Mobileum without undue delay of requests from Data Subjects exercising their Data Subject rights addressed directly to Service Provider regarding Mobileum Personal Data. If Mobileum is obliged to provide information regarding Mobileum Personal Data to Other Controllers or third parties (e.g. Data Subjects or the Supervisory Authority), Service Provider shall assist Mobileum in doing so by providing all required information. If Mobileum or Other Controllers are obliged to provide information about the processing of Mobileum Personal Data to a Data Subject, Service Provider shall assist Mobileum in making the required information available.

2. Service Provider shall cooperate with Mobileum whenever there is a need to respond to requests from a Supervisory Authority in the performance of its tasks.
3. Service Provider shall make available to Mobileum all information necessary to demonstrate compliance with the obligations under the Data Protection Laws concerning Mobileum Personal Data protection and information security.
4. Service Provider shall inform Mobileum immediately if, in his opinion, any instruction violates the Data Protection Laws.

Article 8 - Data Retention

Unless otherwise required by applicable law, Service Provider will, at Mobileum's choice, either delete or return the Mobileum Personal Data upon termination or expiration of the relevant Agreement/Services, or earlier upon request from Mobileum. Before termination or expiration of the relevant Agreement/Services, Service Provider shall contact Mobileum, requesting if the Mobileum Personal Data shall be deleted or returned. If applicable, Service Provider will return the Mobileum Personal Data within a reasonable period in a reasonable and common format upon receiving written instructions from Mobileum.

Article 9 - Audits and Inspections

1. The Service Provider is obliged to provide information in writing about the Processing of Mobileum Personal Data, including but not limited to the technical and organizational measures implemented and any Subprocessors engaged.
2. Service Provider shall allow for and contribute to audits, including inspections, conducted by Mobileum and/or Other Controllers and the respective Supervisory Authorities or another auditor legally mandated by Mobileum and/or Other Controllers to demonstrate compliance with Service Provider's obligations set out in this DPA and the Data Protection Laws applicable to Service Provider in the performance of the Services. Service Provider can provide proof of the adherence to an approved code of conduct or an approved certification mechanism, or otherwise provide information to Mobileum which may be used as an element to demonstrate compliance with Service Provider's obligations. Mobileum or Other Controllers may reasonably assure itself of Service Provider's compliance at Service

Provider's business premises involved in the Processing of Mobileum Personal Data during Service Provider's normal business hours after prior notification. Service Provider will provide Mobileum and/or Other Controllers access to Mobileum Personal Data accordingly and/or access to its business premises involved in the Processing of Mobileum Personal Data. To the extent Mobileum is mandating another auditor, such other auditor shall not be a direct competitor of Service Provider with regard to the Services and shall be bound to confidentiality.

3. Upon Mobileum's request, Service Provider shall provide information on the material terms of the contracts in relation to the implementation of the data privacy obligations by Service Provider's approved Subprocessors, including, if necessary, by means of granting access to the relevant contract documents. Service Provider shall ensure that any audit and information rights towards Service Providers Subprocessors also apply directly to Mobileum and/or Other Controllers as well as the respective Supervisory Authorities.

Article 10 - Record of Processing Activities

4. Service Provider and, where appropriate, its representatives or Subprocessors, shall maintain an up to date record of all categories of Processing activities, carried out on behalf of Mobileum.
5. This record shall, at least, include:

   (a) the name and contact details of Service Provider and, where applicable, the Subprocessor, the Service Provider 's representative and, where applicable, the data protection officer;

   (b) the categories of Processing carried out on behalf of Mobileum;

   (c) where applicable, transfers of Mobileum Personal Data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of article 49(1) GDPR, the documentation of suitable safeguards;

   (d) a general description of the technical and organizational security measures referred to in article 32(1) GDPR and in this DPA.
6. The records referred shall be in writing, including in electronic form.
7. Service Provider and, where available, his Subprocessors shall, on request, make the record available to Mobileum and/or to the Supervisory Authority.

Article 11 - Personal Data Breach

1. Service Provider shall implement an incident management system for Personal Data and Information Security.
2. In case of a Personal Data Breach in respect of the Services, Service Provider shall:

(a) Immediately investigate the Personal Data Breach and identify, prevent and make best efforts to mitigate the effects of it in accordance with its obligations under this DPA and carry out any recovery or other action necessary to remedy the Personal Data Breach, and will provide Mobileum with reasonable assistance to satisfy any legal obligations (including obligations to notify Supervisory Authorities or Data Subjects) of Mobileum and/or Other Controllers in relation to the Personal Data Breach;

(b) Notify Mobileum without undue delay and, whenever possible, not later than twelve hours after becoming aware of the Personal Data Breach. If the said notification is not executed within twelve hours, the reasons for the delay must be furnished to Mobileum. The notification referred to, shall at least:

i. Describe the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Mobileum Personal Data records concerned;

ii. Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained by Mobileum;

iii. Describe the likely consequences of the Personal Data Breach;

iv. Describe the measures taken or proposed to be taken by the Service Provider to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

3. The Service Provider shall not release or publish any filing, communication, notice, press release, or report concerning any Personal Data Breach without Mobileum prior written approval.
4. Service Provider shall document the Personal Data Breaches, comprising the facts relating to each Personal Data Breach, its effects and the remedial action taken, making such documentation available to Mobileum, at request.
5. The actions and steps described in this clause shall, without prejudice to Mobileum ´s right to seek any legal remedy (including the claim for reimbursement of Mobileum's costs of legal action against Service Provider or Subprocessor) as a result of the Personal Data Breach, be undertaken at the expense of the Service Provider and the Service Provider shall pay for or reimburse Mobileum for all costs, losses and expenses relating to the cost of preparing and publishing publicity.
6. If the Personal Data Breach impacts other of the Service Provider's customers, the Service Provider shall prioritise Mobileum in providing support and implementing necessary actions and remedies.

Article 12 - Liability

Service Provider shall defend, indemnify and hold Mobileum and its employees, agents, and contractors, harmless from and against any and all claims, losses, damages, expenses, and all

other liabilities, including, but not limited to, costs and attorney's fees, arising from or resulting from any damages resulting from Service Provider Processing of Personal Data, his performance or the performance of any of his Subprocessors, whether such damages are due to breach of the terms of this DPA, or whether such damage result from breach of the applicable Data Protection Laws.

Article 13 - Term and Termination

1. This DPA shall remain in effect for the term of the provision of Services by Service Provider to Mobileum.
2. Obligations that by their nature are intended to survive after termination of the DPA shall remain in force after termination, such as confidentiality, liability, retention period, return and destruction of Personal Data.
3. Each Party may terminate this DPA and the relevant Agreement, if the other Party demonstrably fails to fulfil its obligations under this DPA and the imputable failure is not rectified within thirty days after written notice by the non-defaulting Party to the defaulting Party of such breach.

Article 14 – General

1. Mobileum and Service Provider agree that this DPA is part of the relevant Agreement and is governed by its terms and conditions, unless otherwise required by applicable law. In case of conflict, the order of precedence in respect of the Processing of Mobileum Personal Data shall be: Exhibits to this DPA, this DPA and then the relevant Agreement. Where EU Standard Contractual Clauses are an integral part of this DPA, the EU Standard Contractual Clauses shall prevail.
2. If an amendment to this DPA, including its Exhibits, is required in order to comply with applicable law or comply with requirements set out by Mobileum's Clients, Mobileum will provide an amendment to this DPA with the required changes to Service Provider. Both Parties will work together in good faith to promptly execute a mutually agreeable amendment to this DPA reflecting the requirements set out by Mobileum's Client. In case Service Provider is not able to accommodate the requested changes, Mobileum may terminate all or part of the relevant Agreements and this DPA with thirty (30) days' written notice.
3. This DPA shall not restrict any applicable Data Protection Laws. If any provision in this DPA is ineffective or void, this shall not affect the remaining provisions. The Parties shall replace the ineffective or void provision with a lawful provision that reflects the business purpose of the ineffective or void provision. In case a necessary provision is missing, the Parties shall add an appropriate one in good faith.
4. Service Provider guarantees the prompt and satisfactory performance of its obligations and responsibilities under this DPA by Service Provider and Service Provider agrees that it shall be

responsible for all costs associated with its compliance of such obligations. Service Provider is responsible and liable for its acts and omissions under this DPA.

5. This DPA applies to all Service Provider or any Service Provider Affiliate (*understood as companies which are controlled by Service Provider, which control Service Provider or which are under common control with Service Provider. "To control" or "to be controlled" means to hold, directly or indirectly, more than 50% of the respective shares with voting rights*) Services involving the Processing of Mobileum Personal Data. To the extent Service Provider Affiliates need to execute a participation agreement or other document, Service Provider will work with Mobileum to promptly execute such documents.
6. This DPA, including the Exhibits attached hereto and any subsequent properly executed Processing Exhibits agreed between the Parties, constitutes the entire agreement between the Parties pertaining to the subject matter hereof and supersedes all prior agreements, understandings, negotiations and discussions of the Parties..

Sample Exhibit 1 - Processing Details

Sample Exhibit 2 – Mobileum Security Requirements

Exhibit 1

Processing Details

THIS IS A SAMPLE EXHIBIT—SERVICE PROVIDER SHALL EXECUTE THIS EXHIBIT SEPERATELY FOR EACH PURCHASE ORDER (IF REQUIRED) AND ONCE SIGNED, IT WILL FORM AN INTEGRAL PART OF THE AGREEMENT AND THE DPA.

1. Nature, Purposes and Subject Matter of the Processing

The nature, purpose and subject matter of the Processing is the provision of the Services, including the following basic Processing activities:

Processing activities	Purpose(s)	Contact details of Service Provider contact person

2. Duration of the Processing and data retention period

The duration of the Processing corresponds to the duration of the Services provision by Service Provider to Mobileum. If deviating from the duration of the said Services provision, the Parties agree, that the duration of the Processing is the following:

Agreed retention period

3. Categories of Data Subjects

Categories of Data Subjects

4. Types of Mobileum Personal Data

Types of Mobileum Personal Data

5. Data transfers

Data transfers			
Country	Entity	Safety Measure	Others

Exhibit 2

Mobileum Security Requirements

Background to this Exhibit

Purpose

This Exhibit describes the minimum security measures that have to be adopted for the purpose of protecting Personal Data and information, primarily with a view to meeting minimum pre-defined requirements of applicable data protection and privacy law across Mobileum's markets. These requirements have largely been derived from national legislation across Mobileum's markets mandating the minimum security measures for the protection of Personal Data, and are intended to provide a harmonised and single standard.

Compliance with these minimum security measures does not guarantee that an appropriate level of protection has been provided - a holistic and comprehensive assessment of security must be undertaken depending upon the circumstances, type of data and Processing to be performed.

Information security techniques, and the threats to security, are continually evolving. Security must therefore be continually assessed in the light of the specific circumstances at hand to determine the appropriate level of protection.

These requirements are to be applied by entities that Process Personal Data on behalf of Mobileum companies, such entities referred to as "Processors". The corresponding Mobileum company concerned is referred to as the "controller".

These requirements are also to be read in conjunction with any other general security requirements agreed with Mobileum, such as any further security requirements as are identified in any pre or post contract security assessment.

Many of these requirements are not intended to be specific to the Processing operations undertaken on behalf of Mobileum companies. Rather, Processors are expected to adopt these standards as appropriate standards to ensure a secure operating environment to handle Personal Data on behalf of Mobileum.

Definitions

In this document, the following definitions are used:

Authorised Users has the meaning defined in security requirement 16.

Content means the content of an electronic communication by a Mobileum user, including the content of electronic messages, such email, and web pages requested and references to Personal Data shall include Content;

Information Systems means all systems used to access, store or otherwise Process Personal Data, including temporary files;

Judicial Data means any Personal Data processed in the context of judicial administration or judicial investigation;

Location Data means any data Processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service, geographic location derived from mobile network cell ID data, and coordinates provided by GPS, pico-cell, femto-cell or WiFi hotspots with known or presumed coordinates for the cells or hotspots to which users are connected, and references to Personal Data shall include Location Data;

Media means a physical object likely to be Processed in an Information System and on which data may be recorded or from which they may be retrieved;

Security document means the document containing the security plan;

Security plan means the measures adopted to comply with these minimum security requirement;

Sensitive Personal Data means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and data consisting of information as to the commission or alleged commission of any offence or any proceedings for any offence or alleged offence or the disposal of such proceedings or the sentence of any court in such proceedings; and references to Personal Data shall include Sensitive Personal Data;

Traffic Data means any data Processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof, and references to Personal Data shall include Traffic Data; and

User ID has the meaning defined in security requirement 18.

All other definitions used are defined in Article 1 of the Data Processing Agreement.

Security Categories

These minimum security requirements are divided into three categories to reflect the sensitivity of different types of data – Standard, Medium and High. The data types to which these three security categories apply are described below.

Standard

The standard security requirements apply to all Personal Data as identified by Mobileum, including those categories of Personal Data referred to below in relation to the Medium and High categories.

Medium

The medium security requirements apply to Personal Data as identified by Mobileum, including those categories of Personal Data referred to below in relation to the High category:

- relating to Judicial Data or investigations, enquiries or disclosures for law enforcement purposes.
- sufficient to permit an assessment of an individual's personality.
- bank account, debit, credit or other payment card information.

High

The high security requirements apply to the following data categories as identified by Mobileum:

- Sensitive Personal Data.
- Judicial Data or data relating to investigations, enquiries or disclosures for law enforcement purposes where such data is also Sensitive Personal Data and/ or Traffic Data.

- Traffic Data.
- Location Data.
- Content.

Order of precedence

In the event that the security requirements conflict, the higher standard shall take precedence.

Scope of these requirements

The security measures required for access to Personal Data via communications networks must guarantee a level of security equivalent to that applying to local access. Such remote access shall be expressly authorised by the controller.

In accordance with Article 6. of this DPA, Service Provider shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, considering the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals.

The Service Provider shall implement and comply with the following measures, subject to change in accordance with the documented instructions transmitted by to Service Provider under this DPA.

Standard Security Measures

Organisational measures

Security Officer

1. A person responsible for the overall compliance with these minimum security requirements shall be designated as the Security Officer. This person shall be suitably trained and experienced in managing information security and provided with appropriate resources to effectively ensure compliance.

2. The contact details of the Security Officer shall be provided to the controller within ninety (90) days of the parties entering into the relevant processing agreement and any amendment to such details shall be communicated promptly.

Security Plan and Document

3. The measures adopted to comply with these minimum security requirements shall be the subject of a security plan and set out in a security document, which shall be kept up to date, and revised whenever relevant changes are made to the Information System or to how it is organised. The security document shall record significant changes to the security measures or the Processing activities.

4. The security plan shall address: Security measures relating to the modification and maintenance of the system used to Process Personal Data, including development and maintenance of applications, appropriate vendor support and an inventory of hardware and soft Physical security, including security of the buildings or premises where data Processing occurs, security of data equipment and telecommunication infrastructure and environmental controls.

5. Data security mechanisms for securing the integrity and confidentiality of the data, classification of the data.

6. Security of computers and telecommunication systems including procedures for managing back-up copies, procedures dealing with computer viruses, procedures for managing signal/codes, security for software implementation, security related to databases, security for connecting systems to the Internet, inspection of circumvention of data system, mechanisms for keeping account of attempts to break system security or gain unauthorized access.

7. The security plan shall include:

a. a Disaster Recovery Plan which shall set out: measures to minimize interruptions to the normal functioning of the system; limit the extent of any damage and disasters; enable a smooth transition of Personal Data from one computer system to another; if necessary, provide for alternative means of operating a computer system; educate, exercise and familiarize personnel with emergency procedures; provide for fast and smooth system recovery, and minimize the economic effects of any disaster event.

b. a Contingency Plan which must address the following possible dangers to the system and appropriate criteria to determine when the Plan should be triggered: the critical functions and systems, the strategy for protecting the system and priorities in the event the Plan is activated; an inventory of relevant staff members to be called upon during an emergency, as well as telephone numbers of other relevant parties; a set of procedures for calculating the damage incurred; realistic time management plans to enable the recovery of the system; clearly allocated staff duties; possible use of alarms and special devices (e.g., air filters, noise filters); in the event of a fire, special equipment should be available (e.g., fire extinguisher, water pumps, etc.); devices or methods for determining temperature, humidity and other environmental factors (e.g., air conditioning, thermometers, etc.); special security software to detect breaches of security; special generators for dealing with power cuts; retention of copies of software or materials in other protected buildings to avoid inadvertent loss.

8. The security document shall be available to staff who have access to Personal Data and the Information Systems, and must cover the following aspects as a minimum:

a. The scope, with a detailed specification of protected resources;
b. The measures, standards, procedures, code of conduct rules and norms to guarantee security, including for the control, inspection and supervision of the Information Systems;
c. The functions and obligations of staff;
d. The structure of files containing Personal Data and a description of the Information Systems on which they are Processed;
e. The purposes for which the Information Systems may be used;
f. The procedures for reporting, managing and responding to incidents;
g. The procedures for making back-up copies and recovering data including the person who undertook the process, the data restored and, as appropriate, which data had to be input manually in the recovery process.

9. The security document and any related records and documentation shall be retained for a minimum period of 5 years from the end of the Processing.

Third Party Management

10.Contracts and Agreements - There is a Contract or Agreement with the vendor of the system - There is a sub processor agreement or a Data Processing Agreement with the vendor of the system.

Rights of the data subjects

11.Right to information - The system allows responding to the exercise of the right to information required in the processing of personal data – Data Subjects are informed about the personal data processed and the purposes through written information (e.g. forms, contracts, website, privacy policy, etc.) or recorded oral information (e.g. recorded telephone call, etc.)

12.Right of Access (Also known as a Subject Access Request) - The system allows responding to the exercise of the right of access. Data Subjects have the Right to obtain:

a. Confirmation that their data is being processed
b. Access to their personal data and
c. Other supplementary information

13.Right to rectification - The system makes it possible to respond to the exercise of the right of rectification. Data Subjects are entitled to have their personal data rectified if it is inaccurate or incomplete. If the information in question has been disclosed to a third party the Data is also entitled to be informed of the third parties to whom the data has been disclosed, where appropriate.

14.Right to erasure of data - The system allows to respond to the exercise of the erasure right. "This Right is also known as the ‘Right to be Forgotten’. It enables Data Subjects to request the deletion or removal of personal data where there is no compelling reason for its continued processing by the Data Controller.

15.Right to restriction of processing - The system allows for a response to the exercise of the right to limit treatment. When this Right is exercised you are permitted to store the personal data but not further process it. Restricted information about the individual may be retained to ensure that the restriction is respected in the future.

16.Right to data portability - The system allows to answer the exercise of the portability right. This Right allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows the individual to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way in a common data format, for example, Excel or CSV file;

17.Right to object - The system allows to respond to the exercise of the right of opposition. "Individuals have the Right to object to:

a. Processing based on legitimate interest or performance of a task in the public interest/exercise of official authority (including profiling)
b. Direct marketing (including profiling)
c. Processing for the purposes of scientific/historical research and statistics"; and

18.Right not to be subject to a decision based solely on automated processing, including profiling - - The system allows to respond to the exercise of the right of not to be subject to a decision based solely on automated processing, including profiling - "This Right provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention."

Personal Data Processing

19.Consents - The system allows the collection and disclosure of the consent of the Data Subjects (e.g., customer authorizations for marketing communications). Data Subjects must give their consent for the processing of their data, for certain purposes (eg customer authorizations for marketing communications). It is necessary that the systems through which the consent is collected allow the disclosure / registration of their obtaining, for example through registries, traceability logs, etc.

20.Periods of conservation and erasure - The system allows to respect the established periods of conservation and erasure. The system allows deletion of personal data after the period of data storage (eg through alerts, automation, deletion routines or other mechanisms)

21.Anonimization / pseudononimization - The system allows to carry out the pseudo-anonymisation / anonymization of personal data. The system has mechanisms of pseudo-anonymization or anonymization that render the data unidentifiable (when necessary and applicable).

22.Other legal requirements required by Control Authorities (e.g. CNPD) - The system complies with other requirements required by Local Control Authorities resolutions. Applicable for example to services for business customers that are subject to specific Local Control Authorities deliberations and requirements (e.g. Video Surveillance; Biometrics; Occupational health and safety; Control attendance; Call recording; Wi-Fi; etc.)

Functions and Obligations of Staff

23.Only those employees who have demonstrated honesty, integrity and discretion should be Authorised Users or have access to premises where Information Systems or media

containing Personal Data are located. Staff should be bound by a duty of confidentiality in respect of any access to Personal Data.

24.The necessary measures shall be adopted to train and make staff familiar with these minimum security requirements, any relevant policies and applicable laws concerning the performance of their functions and duties in respect of the Processing of Personal Data and the consequences of any breach of these requirements.

25.The functions and obligations of staff having access to Personal Data and the Information Systems shall be clearly defined and documented.

26.Authorised Users shall be instructed to the effect that electronic equipment should not be left unattended and made accessible during Processing sessions.

27.Physical access to areas where any Personal Data are stored shall be restricted to Authorised Users.

28.The disciplinary measures for a breach of the security plan shall be clearly defined and documented and communicated to staff.

Technical Measures

Authorisation

29.Only those employees who have a legitimate operational need to access the Information Systems or carry out any Processing of Personal Data shall be authorised to do so (“Authorised Users”).

30.An authorisation system shall be used where different authorisation profiles are used for different purposes.

Identification

31.Every Authorised User must be issued with a personal and unique identification code for that purpose (“User ID”).

32.A User ID may not be assigned to another person, even at a subsequent time.

33.An up-to-date record shall be kept of Authorised Users, and the authorised access available to each, and identification and authentication procedures shall be established for all access to Information Systems or for carrying out any Processing of Personal Data.

Authentication

34.Authorised Users shall be allowed to Process Personal Data if they are provided with authentication credentials such as to successfully complete an authentication procedure relating either to a specific Processing operation or to a set of Processing operations.

35.Authentication must be based on a secret password associated with User ID, and which password shall only be known to the Authorised User; alternatively, authentication shall consist in an authentication device that shall be used and held exclusively by the person in charge of the Processing and may be associated with either an ID code or a password, or else in a biometric feature that relates to the person in charge of the Processing and may be associated with either an ID code or a password.

36.One or more authentication credentials shall be assigned to, or associated with, an Authorised User.

37.There must be a procedure that guarantees password confidentiality and integrity. Passwords must be stored in a way that makes them unintelligible while they remain valid. There must be a procedure for assigning, distributing and storing passwords.

38.Passwords shall consist of at least eight characters, or, if this is not technically permitted by the relevant Information Systems, a password shall consist of the maximum permitted number of characters. Passwords shall not contain any item that can be easily related to the Authorised User in charge of the Processing and must be changed at regular intervals, which intervals must be set out in the security document. Passwords shall be modified by the Authorised User to a secret value known only to the Authorised User when it is first used as well as at least every six months thereafter.

39.The instructions provided to Authorised Users shall lay down the obligation, as a condition of accessing the Information Systems, to take such precautions as may be necessary to ensure that the confidential component(s) in the credentials are kept secret and that the devices used and held exclusively by Authorised Users are kept with due care.

40.Authentication credentials shall be de-activated if they have not been used for at least six months, except for those that have been authorised exclusively for technical management and support purposes.

41.Authentication credentials shall be also de-activated if the Authorised User is disqualified or de-authorised from accessing the Information Systems or Processing Personal Data.

42.Where data and electronic equipment may only be accessed by using the confidential component(s) of the authentication credential, appropriate instructions shall be given in advance, in writing, to clearly specify the mechanisms by which the controller can ensure that data or electronic equipment are available in case the person in charge of the Processing is either absent or unavailable for a long time and it is indispensable to carry out certain activities without further delay exclusively for purposes related to system operationality and security. In this case, copies of the credentials shall be kept in such a way as to ensure their confidentiality by specifying, in writing, the entities in charge of keeping such credentials. Such entities shall have to inform the person in charge of the Processing, without delay, as to the activities carried out.

Access Controls

43.Only Authorised Users shall have access to Personal Data, including when stored on any electronic or portable media or when transmitted. Authorised Users shall have authorised access only to those data and resources necessary for them to perform their duties.

44.A system for granting Authorised Users access to designated data and resources shall be used.

45.Authorisation profiles for each individual Authorised User or for homogeneous sets of Authorised Users shall be established and configured prior to the start of any Processing in such a way as to only enable access to data and resources that are necessary for Authorised Users to perform their duties.

46.It shall be regularly verified, at least at yearly intervals, that the prerequisites for retaining the relevant authorisation profiles still apply. This may also include the list of

Authorised Persons drawn up by homogeneous categories of task and corresponding authorisation profile.

47.Measures shall be put in place to prevent a user gaining unauthorised access to, or use of, the Information Systems . In particular, firewalls and intrusion detection systems reflecting the state of the art and industry best practice should be installed to protect the Information Systems from unauthorized access. Measures shall be put in place to identify when the Information Systems have been accessed or Personal Data has been Processed without authorization, or where there have been unsuccessful attempts at the same.

48.Operating system or database access controls must be correctly configured to ensure authorised access.

49.Only those staff authorised in the security document shall be authorised to grant, alter or cancel authorised access by users to the Information Systems

Management of Media

50.Information Systems and physical media storing Personal Data must be housed in a secure physical environment. Measures must be taken to prevent unauthorized physical access to premises housing Information Systems.

51.Organisational and technical instructions shall be issued with regard to keeping and using the removable media on which the data are stored in order to prevent unauthorised access and Processing.

52.Media containing Personal Data must permit the kind of information they contain to be identified, Inventoried (including the time of data entry; the Authorised User who entered the data and the person from whom the data was received; and the Personal Data entered) and stored at a physical location with physical access restricted to staff that are authorised in the security document to have such access.

53.When media are to be disposed of or reused, the necessary measures shall be taken to prevent any subsequent retrieval of the Personal Data and other information stored on them, or to otherwise make the information intelligible or be re-constructed by any technical means, before they are withdrawn from the inventory. All reusable media used for the

storage of Personal Data must be overwritten three times with randomised data prior to disposal or re-use.

54.The removal of media containing Personal Data from the designated premises must be specifically authorised by the controller.

55.Media containing Personal Data must be erased or rendered unreadable if it is no longer used or prior to disposal.

Distribution of Media and Transmission

56.Media containing Personal Data must only be available to Authorised Users.

57.Printing/copying Processes must be physically controlled by Authorised Users, to ensure that no prints or copies containing Personal Data remain left in the printers or copying machines.

58.Media containing Personal Data or printed copies of Personal Data must contain the classification mark “Confidential”.

59.Encryption (128-bit or stronger) or another equivalent form of protection must be used to protect Personal Data that is electronically transmitted over a public network or stored on a portable device, or where there is a requirement to store or Process Personal Data in a physically insecure environment.

60.Paper documents containing Personal Data must be transferred in a sealed container / envelope that indicates clearly that the document must be delivered by hand to an Authorised User.

61.When media containing Personal Data are to leave the designated premises as a result of maintenance operations, the necessary measures shall be taken to prevent any unauthorised retrieval of the Personal Data and other information stored on them.

62.A system for recording incoming and outgoing media must be set up which permits direct or indirect identification of the kind of media, the date and time, the sender/recipient, the number of media, the kind of information contained, how they are sent and the person responsible for receiving /sending them, who must be duly authorised.

63.Where Personal Data is transmitted or transferred over an electronic communications network, measures shall be put in place to control the flow of data and record the timing of the transmission or transfer, the Personal Data transmitted or transferred, the destination of any Personal Data transmitted or transferred , and details of the Authorised User conducting the transmission or transfer.

Preservation, Back-up copies and Recovery

64.Tools must be in place to prevent the unintended deterioration or destruction of Personal Data.

65.Procedures must be defined and laid down for making back-up copies and for recovering data. These procedures must guarantee that Personal Data files can be reconstructed in the state they were in at the time they were lost or destroyed.

66.Back-up copies must be made at least once a week, unless no data have been updated during that period.

Anti-Virus and Intrusion Detection

67.Anti-virus software and intrusion detection systems should be installed on the Information Systems to protect against attacks or other unauthorised acts in respect of Information Systems. Antivirus software and intrusion detection systems should be updated regularly in accordance with the state of the art and industry best practice for the Information Systems concerned (and at least every six months).

Software Updates

68.The software, firmware and hardware used in the Information Systems shall be reviewed regularly in order to detect vulnerabilities and flaws in the Information Systems and resolve such vulnerabilities and flaws. This review shall be carried out at least annually.

Record Keeping

Access Record

69.A history of Authorised Users' access to or disclosure of Personal Data shall be recorded on a secure audit trail.

Physical Access Record

70.Only those staff duly authorised in the security document may have physical access to the premises where Information Systems and media storing Personal Data are stored. A record of staff who access such premises shall be maintained, including name, date and time of access.

Record of Incidents

71.There shall be a procedure for reporting, responding to and managing security incidents such as data security breaches or attempts at unauthorised access. This shall include as a minimum:

a. A procedure for reporting such incidents/ breaches to appropriate management within the processor;

b. A clearly designated team for managing and co-ordinating the response to an incident led by the Security Officer;

c. A documented and tested process for managing the response to an incident including the requirement to keep appropriate issues and action logs to include the time at which the incident occurred, the person reporting the incident, to whom it was reported and the effects thereof;

d. The requirement on the processor to notify the controller immediately if it appears that Personal Data was involved in the incident or breach or may be impacted or affected in some way; and

e. The processor security/ incident management team should where appropriate work together with the controller's security representatives until the incident or breach has been satisfactorily resolved.

f. The system generates a log of access to personal data (logging) allowing the identification of the origin and the traceability of the accesses - The logs must comply with the security measures usually required by the Personal Data Local Control Authorities: digitally signed registers with timestamp, sequential id and a hash field applied to the previous elements (id, user, date, time and operation), clock synchronization to the timestamp , etc.

Medium Security Measures

Technical Measures

Identification and Authentication

72.Passwords shall be modified at least every three months.

73.The software, firmware and hardware used in the Information Systems shall be reviewed at least every six months in order to detect vulnerabilities and flaws in the Information Systems and resolve such vulnerabilities and flaws.

74.Mechanisms shall be set up that permit unequivocal, personalised identification of any user who attempts to access the information system and a check to establish whether each user is authorised.

75.Limits shall be placed on the scope for repeating attempts to gain unauthorised access to the Information System. After, at most, 6 failed attempts to authenticate, the associated User ID must be blocked.

Tests with Real Data

76.Testing prior to the implementation or modification of the Information Systems Processing Personal Data shall not use real or ‘live’ data unless such use is necessary and there is no reasonable alternative. Where real or ‘live’ data is used, it shall be limited to the extent necessary for the purposes of testing and the level of security corresponding to the type of Personal Data Processed must be guaranteed.

Audit

77.Regular audits of compliance with these minimum security requirements, at least at two yearly intervals, should be performed and delivered in the form of an audit report.

78.The audit report must provide an opinion on the extent to which the security measures and controls adopted comply with these minimum security requirements, identify any shortcomings and (if any) propose corrective or supplementary measures as necessary. It should also include the data, facts and observations on which the opinions reached and the recommendations proposed are based.

79.The audit report shall be analysed by the Security Officer who shall refer the conclusions to the controller and the Security Officer shall remain at the disposal of the controller.

High Security Measures

Organisational Measures

Incident Reporting

80.The procedure for reporting, managing and responding to incidents shall be tested at least once a year.

Technical Measures

Distribution of Media

81.Media containing Personal Data may only be distributed if the data have been encrypted to guarantee that that Personal Data and other information is not intelligible or may not be manipulated in transit.

Access Record

82.The minimum details to be recorded for every access to the Information Systems shall be the User ID, the date and the time of access, the file or data accessed, the kind of access and whether this was authorised or denied.

83.If access was authorised, it shall be necessary to retain the information which permits the record that was accessed to be identified.

84.The mechanisms permitting the data set out in detail in the preceding paragraphs to be recorded shall be under the direct control of the Security Officer and under no circumstances must it be permissible to deactivate these.

85.The minimum period for retaining the data recorded shall be two years.

86.The Security Officer shall periodically review the control information recorded, and shall draw up a report on the reviews carried out and any problems detected at least once a month.

Back-Up Copies and Recovery

87.A back-up copy and data recovery procedures must be kept at a different location from the site of the Information Systems Processing the Personal Data and these security requirements shall apply to such back-up copies.

Electronic Communications Networks

88.Personal Data may be distributed via electronic communications networks only if they have been encrypted, enciphered or another mechanism is used to guarantee that the information is not intelligible or is not manipulated by third parties.

Record Keeping

89.All findings from the tests by the Processor of the procedure for reporting, managing and responding to incidents shall be provided promptly to the controller for review.