

**Exhibit D – Model Contractual Clauses**

**Commission Decision C(2010)593  
Standard Contractual Clauses (processors)**

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: .....

Address: .....

Tel.: ..... ; fax: ..... ; e-mail: .....

Other information needed to identify the organisation:

.....  
(the data **exporter**)

And

Name of the data importing organisation: SOOMLA Inc.

Address: 260 MADISON AVE, SUITE 204 NEW YORK, NY 10016 United States

Tel.: +972527393089; fax: .....; e-mail: privacy@soom.la\_\_\_\_\_]

Other information needed to identify the organisation:

.....Not Applicable.....  
(the data **importer**)

Other information needed to identify the organisation:

.....Not Applicable.....  
(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

## Clause 1

### **Definitions**

For the purposes of the Clauses:

- (a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data<sup>1</sup>;
- (b) *'the data exporter'* means the controller who transfers the personal data;
- (c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

## Clause 2

### **Details of the transfer**

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

---

<sup>1</sup> Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

### *Clause 3*

#### ***Third-party beneficiary clause***

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

### *Clause 4*

#### ***Obligations of the data exporter***

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all

other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

#### *Clause 5*

#### ***Obligations of the data importer<sup>2</sup>***

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

---

<sup>2</sup> Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia*, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
  - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
  - (ii) any accidental or unauthorised access, and
  - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

## *Clause 6*

### ***Liability***

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

## *Clause 7*

### ***Mediation and jurisdiction***

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
  - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
  - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

*Clause 8*

***Cooperation with supervisory authorities***

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

*Clause 9*

***Governing Law***

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely.....

*Clause 10*

***Variation of the contract***

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

*Clause 11*

***Subprocessing***

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses<sup>3</sup>. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely .....  
.....  
.....
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

*Clause 12*

***Obligation after the termination of personal data processing services***

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the

---

<sup>3</sup> This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.



personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

**Additional commercial and clarifying provisions**

The parties agree that:

(a) The audits described in Clause 5(f), Clause 11 and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the provisions of Section 12 of the Data Protection Agreement executed by the parties.

(b) The copies of the Sub-processor agreements that must be sent by the Provider to the Client pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or provisions unrelated to the Standard Contractual Clauses or their equivalent, removed by the Provider beforehand; and, that such copies will be provided by Provider only upon reasonable request by Client.

(c) The certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Provider to the Client only upon Client's request.

(d) Section 15 of the Data Protection Agreement shall be deemed to apply to any violation of the Standard Contractual Clauses.

**On behalf of the data exporter:**

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature.....

(stamp of organisation)

**On behalf of the data importer:**

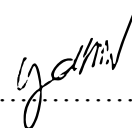
Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature.....



## **APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES**

This Appendix forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

### **Data exporter**

The data exporter is \_\_\_\_\_  
\_\_\_\_\_.

### **Data importer**

The data importer is a provider of a data analytics platform for mobile applications. In the provision of the services data importer stores and processes certain Personal Data belonging to the end users of the mobile applications.

### **Data subjects**

Data subjects include end users of mobile applications.

### **Categories of data**

The personal data transferred includes IP addresses, Advertising IDs (IDFA, GAID), customer provided ids, and ids provided by other processors of the Customer.

### **Processing operations**

The personal data transferred will be subject to the following basic processing activities:

- A. **Duration and Object of Data Processing.** The duration of data processing shall be for the term agreed between data exporter and the data importer. The objective of the data processing is the performance of the Services.
- B. **Scope and Purpose of Data Processing.** The scope and purpose of processing personal data is to facilitate provision of the Services.
- C. **Customer Data Access.** Customers can access, amend, delete or export data through their user interface. They can make such requests also by contacting [privacy@soomla.com](mailto:privacy@soomla.com).
- D. **Data Exporter's Instructions.** For the Services, Importer will only act upon data exporter's instructions.
- E. **Customer Data Deletion or Return.** Upon expiration or termination of data exporter's use of the Services, data importer will delete data exporter's customer data within sixty (60) days of the account termination unless otherwise required by law.

## **APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES**

### **SECURITY CONTROLS**

#### ORGANIZATION OF INFORMATION SECURITY

- Security Ownership. Soomla has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.
- Security Roles and Responsibilities. Soomla personnel with access to Client Personal Data are subject to confidentiality obligations.

#### PHYSICAL SECURITY

- Physical Access to Facilities. Soomla limits access to facilities where information systems that process Client Personal Data are located to identified authorized individuals.
- Video Surveillance. Soomla monitors its facilities with security cameras.
- Protection from Disruptions. Soomla uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.
- We use several services from AWS to regularly back up our data bases and prevent data loss.
- Component Disposal. Soomla uses industry standard processes to delete Client Personal Data when it is no longer needed.

#### COMMUNICATION AND OPERATION - Data Beyond Boundaries

- Soomla encrypts, or enables Client to encrypt, Client Personal Data that is transmitted over public networks.
- Soomla uses authentication mechanisms to ensure decryption is only possible by Client, Soomla or Soomla's sub processors
- Soomla restricts access to Client Personal Data in media leaving its facilities.

#### ACCESS CONTROL

Access Policy. Soomla maintains a record of security privileges of individuals having access to Client Personal Data.

Access Authorization

- Soomla maintains and updates a record of personnel authorized to access Soomla systems that contain Client Personal Data.
- Soomla deactivates authentication credentials for personnel that left the company, was fired or moved to a role that no longer requires access.
- Soomla identifies those personnel who may grant, alter or cancel authorized access to data and resources.
- Soomla ensures that where more than one individual has access to systems containing Client Personal Data, the individuals have separate identifiers/log-ins.

#### Least Privilege

- Technical support personnel are only permitted to have access to Client Personal Data only for customers where the situation requires it.
- Soomla restricts access to Client Personal Data to only those individuals who require such access to perform their job function.

#### Integrity and Confidentiality

- Soomla instructs Soomla personnel to disable administrative sessions when computers are otherwise left unattended.
- Soomla stores passwords in a way that makes them unintelligible while they are in force.

#### Authentication

- Soomla uses industry standard practices to identify and authenticate users who attempt to access information systems.
- Where authentication mechanisms are based on passwords, Soomla requires the password to be at least eight characters long.
- Soomla maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.
- Soomla uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

#### Network Design.

Soomla has controls to avoid individuals assuming access rights they have not been assigned to gain access to Client Personal Data they are not authorized to access.

We also regularly check the effectiveness of our network design to ensure the security of the data and assess potential risks