

## Regulations for Provision of Prepaid Services by ComVision Sp. z o.o. of 21 May 2018

### Table of Contents:

Section I General Provisions

Section II Types and Scope of Services to be Provided Under the Regulations

Section III Conditions for Entering Into, Performing and Terminating the Agreements

Section IV Liability

Section V Complaint Procedure

Section VI Final Provisions

### Section I General Provisions

- 1.1. On the basis of Art. 8 item 1 point 1 of the Act of 18<sup>th</sup> July 2002 – concerning providing the services by electronic way (Journal of Laws No 144, item 1204, with later amendments), ComVision Sp. z o.o., with the registered office in Poland, Gliwice 44-100, Toszecka str. 101, taxpayer's identification number (NIP): 969-156-67-36, company registration number (REGON): 241520885, registered under the National Court Register (NCR) number: 0000350201 by Regional Court in Gliwice, 10th Economic Department of the NCR, with the share capital of PLN 100,000.00, establishes the following Regulations for the provision of services by electronic way.
- 1.2. The Regulations constitute the template of the agreement within the meaning of Art. 384 of the Civil Code and they are made available free of charge to the Service Recipient before entering into an agreement for providing the Service by electronic way in a manner that makes it possible to store and recover the same in an ordinary course of action, with the use of the website on the Internet under URL address [www.smsapi.com](http://www.smsapi.com).
- 1.3. The Regulations specify the principles and technical conditions for entering into and performing by ComVision Sp. z o.o. the agreements, whose subject matter is the use by Service Recipients of the electronically made available service system for automatic sending and receiving messages, under the name SMSAPI service, especially through the website available on the Internet under URL address [www.smsapi.com](http://www.smsapi.com).
- 1.4. Wherever the word "agreement" appears in the Regulations, it means the agreement indicated in point 4.2 of the Regulations.
- 1.5. Service Recipients are obliged to get acquainted with the content of the Regulations and its attachments which are its integral part and to follow their provisions, which shall be confirmed by the Service Recipients through the declaration to be submitted during the registration of the Account in the SMSAPI Service.
2. For the purposes of the Regulations as well as the agreements for the performance thereof, the following definitions are established:
  - a. **Account** – the profile of the Service Recipient created by the SMSAPI service system that includes the identification data provided by the Service Recipient. The Account has a unique Login (user name) and the password.

- b. **Telecommunication Law** - the Act of 16st July 2004 – *Telecommunication Law* (Journal of Laws No 171, item 1800 of 2004 with later amendments).
- c. **Act on the Provision of Services by Electronic Way** - *Act on the Provision of Services by Electronic Way of 18<sup>th</sup> July 2002* (Journal of Laws No 144, item 1204 with later amendments).
- d. **"Data Protection Legislation"** shall mean the EU General Data Protection Regulation 2016/679 ("**GDPR**") upon entering into force, and national provisions on protection of privacy in the country in which the Controller is established, as amended, replaced or superseded from time to time, including laws implementing or supplementing the GDPR.
- e. **"Personal Data"** means any information relating to an identified or identifiable natural person (the "**Data Subject**").
- f. **SMSAPI Service** – a system for automatic sending and receiving messages that is made available by electronic way, with the use of a website available on the Internet under URL address [www.smsapi.com](http://www.smsapi.com).
- g. **Teleinformation System** - a set of computer devices cooperating with each other and the software, which makes it possible to process and store, as well as send and receive the data through the telecommunication nets with the use of a final device appropriate for a given type of the net within the meaning of the Telecommunication Law.
- h. **Provision of the Service by Electronic Way** – providing the service without simultaneous presence of both parties (from the distance), through the transfer of data on the individual request of the Service Recipient, sent and received with the use of devices for electronic processing, including the digital compression and storage of the data, which is sent, received and transmitted with the use of telecommunication net within the meaning of the Act *Telecommunication Law*.
- i. **Means of Electronic Communication** – technical solutions, including the teleinformation devices and the software tools cooperating with them, which make it possible to communicate from the distance with the use of data transmission between the teleinformation systems, especially the electronic mail.
- j. **Service Provider** - ComVision Sp. z o.o., with the registered office in Gliwice Poland, ul. Toszecka 101 , 44-100 Gliwice Poland, taxpayer's identification number (NIP) 9691566736 , company registration number (REGON) 241520885.
- k. **Service Recipient** or **User** – an entity that uses the services provided by the Service Provider and has an active account in SMSAPI service.
- l. **Technical Specification** – the collection of information about the Service Provider's teleinformation system and the technical requirements necessary for the cooperation with this system, which constitutes the appendix to the Regulations, is available at <https://docs.smsapi.com/> .
- m. **Message** – a message in textual or binary form (SMS/MMS/VMS/WAPPUSH/Vcard/other).
- n. **Special Characters** – the characters not included on the following list:  
@ £ \$ ¥ è é ù ì ò ç ø å ä \_ ^ { } \ [ ~ ] | Æ æ ß É ! " # ¤ % & ' ( ) \*  
+ , - . / : ; < = > ? 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P  
Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z Ä Ö

Ñ Ü § ¿ a – z ä ö ñ ü à o and “space” and “enter”, where the characters ^ { } [ ] ~ \ | € as well as “enter” are counted as 2 characters.

- o. **SMS Message:** Text or binary message with as defined in GSM 03.38 Specification. Number of characters and parts as specified:
    - a. Number of characters for a one-part SMS message:
      - a. Without special characters: maximum 160
      - b. With special characters: maximum 70
    - b. Formulae for the calculation of the number of parts for a SMS message consisting of a higher number of characters than that provided in points 2.o.a.a and 2.o.a.b:
      - a. Without special characters:  $N^* = \text{number of characters} / 153$
      - b. With special characters:  $M^* = \text{number of characters} / 67$
- \* N and M are the number of parts; the result (N and M) needs to be rounded up to the nearest integer.
- o. **HLR Number Check:** a one-time check of the GSM number.
  - p. **Push (Message) Notification:** are messages or information sent to applications on platforms such as iOS, Android, Windows and others. Push notifications are sent through services such as the Apple Push Notification Service (APNS), Google Cloud Messaging (GCM), Windows Push Notification Services (WNS) or similar.

## Section II Types and Scope of Services to be Provided Under the Regulations

- 3.1. The Regulations cover the services provided by the Service Provider by electronic mail, which make the system for the automatic sending and receiving of the messages available to the Service Recipients through the use of the website on the Internet under URL address [www.smsapi.com](http://www.smsapi.com).
- 3.2. The access defined in point 3.1 above is provided with the use of an Account assigned to a given User.
- 3.3. In the case of lack of separate agreement, the User is not entitled to make the Account access data in the form of user login and password available to the third parties.
- 3.4. In the case of lack of separate agreement between the parties, the User is obliged to use the Account in an active way at least once during the period of 6 months. In the case the Service Provider identifies the lack of activity on the Account for the period longer than 6 months, the Account can be removed by the Service Provider.

## Section III Conditions for Entering Into, Performing and Terminating the Agreements

- 4.1. The basis for User’s use of the services covered by the Regulations is the agreement entered into between the parties.
- 4.2. The agreement as specified in point 4.1 is entered into by registration of the Account in SMSAPI service by the Service Recipient. Within 7 days from the registration date, the Service Provider is entitled to reject such agreement, which is tantamount to the termination of the agreement along with the return of the equivalent of the points as specified in point 5.2, which have not been utilized by the Service Recipient until such termination.

- 4.3. Through the registration of the Account, the User entitles the Service Provider to send to its address, e-mail address or telephone number indicated during the registration, all information connected with the agreement or the performance thereof, as well as with functioning of the SMSAPI service. Until indicating the new contact data, the contact data presented during the registration is regarded as applicable for mutual contacts.
- 5.1. For the services provided, the Service Provider acquires the right to remuneration.
- 5.2. The User purchases the Points in the SMSAPI Service. One Point has a value of EUR 1.00 net (in words: one Euro). The Points are automatically settled basing on the price list value for the messages sent by the Service Recipient with the use of the SMSAPI service and the additional services available in the SMSAPI service and they cannot be used in any other way. The Points are subject neither to exchange nor return.
- 5.3. The value of the message as referred to in point 5.2 above depends on the type of the message and the operator to which it is directed. Detailed data on the number of Points assigned to a given type of message and other services are each time published on the Service Provider's website [www.smsapi.com](http://www.smsapi.com).
- 5.4. The Service Provider is entitled to change the number of the Points assigned to a given type of message or other services within the SMSAPI service, and is obliged to inform the Users about such change on the website [www.smsapi.com](http://www.smsapi.com) and with the use of electronic mail. The above-mentioned changes shall not require the termination of the agreement for their effectiveness.
- 5.5. The Points as referred to in point 5.2 are obtained by the Users with the use of SMSAPI service.
- 5.6. The payments for the purchased Points can be made with the use of electronic service for on-line electronic payments or by the payment into the SMSAPI service account after having previously generated a pro-forma invoice. The sale and at the same time the activation of the purchased number of Points depend on the payment of the entire amount due dictated by the price. Each purchase shall be confirmed by a VAT invoice to be delivered to the electronic mail of the User.
- 6.1. The agreements are entered into for an unspecified period of time.
- 6.2. Each party can terminate the agreement with two-week notice. Before the end of such notice, the User should utilize the points in its possession. The Service Provider does not return the equivalent of Points not utilized by the User before the end of the notice.
- 6.3. The Service Provider may terminate the agreement without the notice as referred to above in the following cases:
  - a. In the case of appearing or revealing the technical, economic or legal reasons making it impossible or making it significantly difficult to continue the performance of the agreement in compliance with its provisions, including the case of prices being considerably increased by the operators as compared to its previous rates, whose services the Service Provider uses in performing the agreement.
  - b. Identified breach of the provisions of point 3.4, 3.5 or 7.1 of the Regulations by the Service Recipient.

- c. Identified User's provision of false personal data.
- 6.4. Termination of the agreement by the Service Recipient without the period of notice in the situations indicated in point 6.3.b and c of the Regulations is tantamount to losing by the Service Recipient all the unused points with no right to any settlement from the Service Provider.
- 6.5. In the case of lack of separate provision of the agreement the Service Provider shall be obliged to provide the services for the Service Recipient from the date of entering into the agreement.
- 7.1. The Service Recipient is obliged to abstain from abusing the electronic communication means in particular through:
  - a. Indicating false or misleading denoting of the sender;
  - b. Sending the messages to the recipients, who have not given the consent required by legal regulations;
  - c. Sending to 1 telephone number more than 20 messages within the subsequent 60 seconds.
  - d. Using SMSAPI service for sending spam:
    - a. Sending Messages that contain unrequested commercial information, within the meaning of the Electronic Services Act of 18 July 2002
    - b. Sending Messages the subject of which are games of chance and betting, within the meaning of the Gambling Game Act of 19 November 2009
  - e. Delivering by or to the teleinformation systems the information that:
    - a. Causes interferences in the operation of or overloads the teleinformation systems of the Service Provider or other entities that take direct or indirect part in providing services by electronic way
    - b. Infringes the rights and interests of the Service Provider, third parties, and commonly accepted social norms, as well as information not in compliance with the commonly accepted legal regulations applicable in the place of sending or in the place to which the message is sent
  - f. Advertising or promoting services using the numbers for calling and sending SMS/MMS messages, which are connected with collecting increased charges or subscription of payable service, in particular Premium SMS.
- 7.2. Should the Service Recipient breach the point 7.1 of the Regulations, the Service Provider shall be regardless of other rights to which it is entitled on the basis of the Act, agreement or the Regulations, entitled to refrain from providing the Service for the Service Recipient, without having to terminate the agreement.
- 7.3. As of the day of the cessation of the legal relation under the agreement between the parties, the Service Recipient is obliged to stop using SMSAPI service.
- 7.4. The Service Provider has a right to control fulfillment of the specified obligation by the Service Recipient and to remove the account of the Service Recipient;
- 7.5. The Service Recipient is the only person responsible for the form and the content of messages being sent with the use of SMSAPI service.

- 8.1. The Service Provider reserves the right to conduct teleinformation system related maintenance works, which may cause difficulties or make it impossible for the Service Recipients to use the services. The dates for and expected durations of such maintenance works will be published on the website or sent by e-mail before the beginning of said works.
- 8.2. In the special cases having the influence on the safety and stability of teleinformation system, the Service Provider has a right to temporarily stop or limit the provision of the services, without prior notification and to conduct the maintenance works aiming at recovering the safety and stability of teleinformation system.
- 8.3. Difficulties or lack of possibility to use the services because of the reasons indicated in point 8.1 and 8.2 of the Regulations shall not justify any claims against the Service Provider.
- 8.4. The Service Provider spares no effort so that the message was sent correctly, but he does not guarantee to deliver every message.
- 9.1. The Service Provider ensures the confidentiality of the content of the messages sent through SMSAPI service, as well as of the information on the entity through and to which the messages are sent, unless such information is in the public domain as a matter of principle or its disclosure is necessary for the correct provision of the services. The Information as referred to above may be revealed only in the cases specified in legal regulations.
- 9.2. The Service Provider takes the matters of protection and security of Personal Data seriously and will process such information in accordance with applicable Data Protection Legislation and the Agreement. In order to provide the Services, Service Provider may process Personal Data about Users and others who access the Services. Service Provider may disclose Personal Data to third parties as set out in the Agreement.
- 9.3. The way of dealing with Personal data, scope and responsibilities of the Service Provider in the processing of personal data are described in Annex 1 to these Regulations, which constitutes the Data Processing Agreement for entrusting the processing of personal data between the Service Provider and the Service Recipient which constitutes a documented processing order in accordance with art. 28 paragraph 3.a) of GDPR.

#### **Section IV Liability**

- 10.1. The Service Provider shall not be liable for the breaks in the provision of the services that result from failures or incorrect functioning of the teleinformation systems, unless they are caused by circumstances attributable to the Service Provider, as well as the legal obstacles.
- 10.2. The Service Provider shall not be liable for the lack of possibility to access the services that results from incorrect registration by the Service Recipient.
- 11.1. In the case of damage, the Service Provider has a right to claim for the supplementary compensation.
- 11.2. The provision of point 11.1 shall not deprive the Service Provider of the possibility to demand repairing the damage in compliance with the general principles of Polish Civil Code.

- 11.3. The total and maximum liability in each twelve (12) month period of either party towards the other party under any provision of the Data Processing Agreement or any transaction contemplated by the Data Processing Agreement shall in no event exceed an amount equal to the total amounts paid for the Services under the Agreement in the twelve (12) months preceding the event that incurs liability
- 11.4. The Service Provider shall be liable for actual damage incurred by the Service Recipient or third parties as a result of the data processing being not in compliance with the provisions of this section. The liability as referred to in this point results from the provisions of the Personal Data Protection Act and relevant regulations of Polish Civil Code.

## **Section V Complaint Procedure**

- 12.1. Complaints can be submitted due to the failure to provide, correctly provide, or correctly settle the services.
- 12.2. The complaint shall be submitted through electronic mail to the e-mail address: [support@smsapi.com](mailto:support@smsapi.com).  
The User is obliged to provide in its complaint the data allowing for identification of the message sent.
- 12.3. The complaint can be filed within 7 days from the date of sending the message to which such complaint applies.
- 12.4. The complaint about the failure to provide or failure to correctly provide the service must in particular include the subject matter of and the circumstances that justify such claim, as well as a precise description of Service Recipient's claim;
- 12.5. The Service Provider shall consider the complaint within 14 days from the complaint submission date. If the complaint cannot be considered during the above period of time, the Service Provider shall during said period inform in writing the complaint submitter about the reasons for such delay and the expected timeframe of complaint consideration.
- 12.6. A breach of the complaint procedure justifies the complaint rejection.

## **Section VI Final Provisions**

13. The Service Recipient agrees to place his name and / or his logo on the Service Provider's website. The Service User authorizes the user to place his name and / or his logo in internal materials used for the needs of the Service Provider.
14. This Agreement does not authorize the Service Provider to use, in any other manner than the one resulting from this Agreement, trademarks, advertising slogans, trade names or other intellectual property rights to which the Service Recipient is entitled.
15. All declarations of the parties which are connected with the agreement entered into by and between them shall be sent to the User's address or e-mail address as indicated during the account registration. The User is obliged to immediately inform the Service Provider about the change of its mailing data. Until the moment of receipt by the party of the information about the change of mailing data of its contracting

party, the declaration sent to the current address shall be regarded effectively delivered regardless of whether it has been received or not.

16. Except as stated in the agreement or the Regulations, Polish laws, in particular the regulations of the Civil Code, the Electronic Services, the Telecommunication Law, and the Data Protection Legislation shall apply.
17. The Service Provider reserves the right to introduce changes to the Regulations.
18. The Service Provider reserves the right to monitor, store and archive the content of SMS messages sent, and the IP addresses of the computers from which the messages are sent. The data are stored in order to prove sending of the messages in the case of stating the infringement of the Regulations, and also in order to transfer all the documents to relevant penal prosecution agencies in the event of illegal use of SMSAPI service.
19. The User gives consent to process its personal data for the purposes connected with the provision of the services.
20. The User is entitled to have insight into and correct its personal data and to demand that the Service Provider stop processing the same.
21. The User gives consent to place the name and the logo of his company on the website, in offers and promotional materials of service SMSAPI, unless the User shall inform SMSAPI service about other decision.
22. The common court having jurisdiction over the registered office of the Service Provider is the competent body for settling disputes arising from the agreement or the Regulations.
23. Attachments to these Regulations (contracts), and in particular Annex No. 1 - Contract for entrusting the processing of personal data and Annex No. 2 - Security, constitute its integral part.

#### **Annex No. 1 – Data Processing Agreement**



The agreement is concluded between the below mentioned parties, hereinafter referred to separately as **Processor** and **Controller** and jointly by the Parties:

The Service Provider is also referred to as the **Personal Data Processor ("Processor")** and the Service Recipient, also referred to as the **Data Controller ("Controller")**:

## 1 INTRODUCTION

This Appendix sets out the main principles for processing of Personal Data under and constitutes an integral part of the existing agreement for Services between the parties (the "Agreement").

This agreement document constitutes the data processing agreement between the parties and is in the following referred to as the "Processing Agreement".

## 2 MAIN PRINCIPLES OF PROCESSING OF PERSONAL DATA

### 2.1 Protection of personal data

The Processor takes the matters of protection and security of Personal Data seriously and will process such information in accordance with applicable Data Protection Legislation and the Agreement. In order to provide the Services, Processor may process Personal Data about Users and others who access the Services. Processor may disclose Personal Data to third parties as set out in the Agreement.

### 2.2 Privacy notice

Please refer to the privacy notice for more information about how Personal Data will be processed in relation to the Services. The privacy notice is available here: <https://www.smsapi.com/privacy>.

## 3 PURPOSE OF THE PROCESSING AGREEMENT

The purpose of the Processing Agreement is to regulate rights and obligations pursuant to applicable Data Protection Legislation relating to Processor's processing of Personal Data on behalf of the Controller.

**"Data Protection Legislation"** shall mean the EU General Data Protection Regulation 2016/679 ("GDPR") upon entering into force, and national provisions on protection of privacy in the country in which the Controller is established, as amended, replaced or superseded from time to time, including laws implementing or supplementing the GDPR.

**"Personal Data"** means any information relating to an identified or identifiable natural person (the "Data Subject").

The Processing Agreement shall ensure that Personal Data is processed in accordance with Data Protection Legislation and is not used unlawfully or comes into the possession of any unauthorized party.

## 4 SCOPE OF PROCESSING

### 4.1 General

The Controller determines the purposes and means of the processing of Personal Data.

The Processor, its Sub-processors, and other persons acting under the authority of the Processor who has access to the Personal Data shall process the Personal Data only on behalf of the Controller and in compliance with the Agreement and the Controller's documented instructions, and in accordance with the Processing Agreement, unless otherwise stipulated in applicable statutory laws.

The Processor shall immediately inform the Controller if, in the Processor's opinion, an instruction infringes the Data Protection Legislation.

### 4.2 The scope of the processing

The Processing Agreement concerns the Processor's processing of Personal Data on behalf of the Controller in connection with the provision of the Services as further described in the Agreement.

#### 4.3 The purpose of the processing

The nature and the purpose of the processing, including operations and basic processing activities, are to provide the Services as further described in the Agreement.

#### 4.4 Categories of Personal Data and Data Subjects

The processing involves processing of Personal Data related to Controller's end-users, customers or employees, depending of the Controller's use of the Services.

The Processing relates to the following categories of Personal Data, subject to the Controller's concrete use of the Services:

- Basic Personal Data (such as name), contact details (such as email, phone number etc).
- Special categories of Personal Data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or health data.
- Location data, such as GPS, Wi-Fi location data and location data derived from Processor's network (that is not traffic data as defined below).
- Traffic data: personal data processed in relation to the conveyance of communication on an electronic communications network or billing thereof.
- Data related to content of communication, such as e-mails, voice mails, SMS/MMS, browsing data etc.

### 5 OBLIGATIONS OF THE CONTROLLER

The Controller warrants that the Personal Data is processed for legitimate and objective purposes and that the Processor is not processing more Personal Data than required for fulfilling such purposes.

The Controller is responsible for ensuring that a valid legal basis for processing exists at the time of transferring the Personal Data to the Processor, including that any consent is given explicitly, voluntarily, unambiguously and on an informed basis. Upon the Processor's request, the Controller undertakes, in writing, to account for and/or provide documentation of the basis for processing.

In addition, the Controller warrants that the Data Subjects to which the personal data pertains have been provided with sufficient information on the processing of their Personal Data.

Any instructions regarding the processing of Personal Data carried out under this Processing Agreement shall primarily be submitted to the Processor. In case the Controller instructs a Sub-processor appointed in accordance with section 11 directly, the Controller shall immediately inform the Processor hereof. The Processor shall not in any way be liable for any processing carried out by the Sub-processor as a result of instructions received directly from the Controller, and such instructions result in a breach of this Data Processing Agreement, the Agreement or Data Protection Legislation.

### 6 CONFIDENTIALITY

The Processor, its Sub-processors, and other persons acting under the authority of the Processor who has access to the Personal Data are subject to a duty of confidentiality and shall observe professional secrecy in regard to the processing of Personal Data and security documentation pursuant to applicable Data Protection Legislation. The Processor is responsible for ensuring that any Sub-processor, or other persons acting under its authority, is subject to such duty of confidentiality.

The Controller is subject to a duty of confidentiality regarding any documentation and information, received by the Processor, related to the Processor's and its Sub-processors' implemented technical and organisational security measures, or information which the Processor otherwise wants to keep confidential.

The confidentiality obligations also apply after the termination of the Processing Agreement.

### 7 ACCESS TO PERSONAL DATA AND FULFILMENT OF DATA SUBJECTS' RIGHTS

Unless otherwise agreed or pursuant to applicable statutory laws, the Controller is entitled to request access to Personal Data being processed by the Processor on behalf of the Controller.

If the Processor, or Sub-processor, receives a request from a Data Subject relating to processing of Personal Data, the Processor shall send such request to the Controller, for the Controller's further handling thereof, unless otherwise stipulated in statutory law or the Controller's instructions.

The Processor shall assist the Controller for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights stipulated in Data Protection Legislation, including the Data Subject's right to (i) access to its Personal Data, (ii) rectification of its inaccurate Personal Data; (iii) erasure of its Personal Data; (iv) restriction of, or objection to, processing of its Personal Data; and (v) the right to receive its Personal Data in a structured, commonly used and machine-readable format (data portability). The Processor shall be compensated for such assistance at the Processor's then current rates, unless otherwise agreed.

## **8 OTHER ASSISTANCE TO THE CONTROLLER**

If the Processor, or a Sub-processor, receives a request for access or information from the relevant supervisory authority relating to the registered Personal Data or processing activities subject to this Processing Agreement, the Processor shall notify the Controller, for the Controller's further processing thereof, unless the Processor is entitled to handle such request itself.

If the Controller is obliged to perform an impact assessment and/or consult the supervisory authority in connection with the processing of Personal Data under this Processing Agreement, the Processor shall provide assistance to the Controller. The Controller shall bear any costs accrued by the Processor related to such assistance.

## **9 NOTIFICATION OF PERSONAL DATA BREACH**

The Processor shall notify the Controller without undue delay after becoming aware of a breach related to the processing of Personal Data ("Personal Data Breach"). The Controller is responsible for notifying the Personal Data Breach to the relevant supervisory authority.

The notification to the Controller shall as a minimum describe (i) 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 Personal Data records concerned; (ii) the likely consequences of the Personal Data Breach; (iii) the measures taken or proposed to be taken by the Processor to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

In the event the Controller is obliged to communicate a Personal Data Breach to the Data Subjects, the Processor shall assist the Controller, including the provision, if available, of necessary contact information to the affected Data Subjects. The Controller shall bear any costs related to such communication to the Data Subject. The Processor shall nevertheless bear such costs if the Personal Data Breach is caused by circumstances for which the Processor is responsible.

Country") may only occur in case of approval from the Controller, as described in section 12 below, and is subject to EUs standard contractual clauses between the Controller and the relevant company at the location, or other legal basis for such Transfer.

## **10 USE OF SUB-PROCESSORS**

The Controller agrees that LINK may appoint another processor ("Sub-processor") to assist in providing the services and processing Personal Data under the Agreement, provided that LINK ensures that;

i) the data protection obligations as set out in this Processing Agreement and in Data Protection Legislation are imposed upon any Sub-processors by a written agreement; and that

ii) any Sub-processor provides sufficient guarantees to implement appropriate technical and organisational measures to comply with Data Protection Legislation and this Processing Agreement, and provide the Controller and relevant supervisory authorities with access and information necessary to verify such compliance.

LINK shall remain fully liable to the Controller for the performance of any Sub-processor.

## **11 PROCEDURE FOR USE OF SUB-PROCESSORS**

Processor shall maintain an up-to-date list of the names and contact details of any Sub-processors and locations used by such Sub-processors for processing of Personal Data on the Controller's behalf at <https://www.linkmobility.com/list/>. Processor shall update the list to reflect any addition or replacement of Sub-processors and notify the Controller at least 3 months prior to the date on which such Sub-processor shall commence processing of Personal Data. Any objection to such changes must be provided to Processor within 3 weeks of receipt of such notification or publication on the website. In case of an objection from Controller as to the supplementing or change of a Sub-processor, Processor may terminate the Agreement and this Processing Agreement with 1 months notice.

By entering into this Processing Agreement, the Controller grants Processor authority to enter into EUs standard contractual clauses on behalf of Controller or to secure other legal basis for Transfer to Third Countries for any Sub-processor approved in accordance with the procedure stipulated above. Upon request, Processor shall provide the Controller with a copy of such EUs standard contractual clauses or description of such other legal basis for Transfer.

Processor shall provide reasonable assistance and documentation to be used in Controller's independent risk assessment in relation to use of Sub-processors or Transfer of Personal Data to a Third Country.

## **12 AUDITS**

Processor shall provide the Controller with documentation of implemented technical and organisational measures to ensure an appropriate level of security, and other information necessary to demonstrate the Processor's compliance with its obligations under the Processing Agreement and relevant Data Protection Legislation.

Controller and the supervisory authority under the relevant Data Protection Legislation shall be entitled to conduct audits, including on-premises inspections and evaluations of Personal Data being processed, the systems and equipment used for this purpose, implemented technical and organisational measures, including security policies and similar, and Sub-processors. Controller shall not be given access to information concerning Processor's other customers and information subject to confidentiality obligations.

Controller is entitled to conduct such audits once a year. If Controller appoints an external auditor to perform the audits, such external auditor shall be bound by a duty of confidentiality.

Controller shall bear any costs related to audits initiated by Controller or accrued in relation to audits of Controller, including compensation to Processor for reasonable time spent by it and its employees complying with on premises audits. Processor shall nevertheless bear such costs if an audit reveals non-compliance with the Processing Agreement or Data Protection Legislation.

## **13 TERM AND TERMINATION**

The Processing Agreement is valid for as long as the Processor processes Personal Data on behalf of the Controller.

In the event of the Processor's breach of the Processing Agreement or non-compliance of the Data Protection Legislation, the Controller may (i) instruct the Processor to stop further processing of Personal Data with immediate effect; and/or (ii) terminate the Processing Agreement with immediate effect.

## **14 EFFECTS OF TERMINATION**

The Processor shall, upon the termination of the Processing Agreement and at the choice of the Controller, delete or return all the Personal Data to the Controller, including back-up copies, unless otherwise stipulated in applicable statutory law.

The Processor shall document in writing to the Controller that deletion has taken place in accordance with the Processing Agreement and as instructed by the Controller.

## **15 LIMITATION OF LIABILITY**

Neither party shall be liable to the other party for any incidental, special, consequential, or indirect damages of any kind (including without limitation damages for interruption of business, loss of data, loss of profits or the like) regardless of the form of action, whether in contract, tort (including without limitation negligence), strict product liability, or other, even if advised of the possibility of such damages (jointly "Indirect Damages").

Neither party shall be liable to the other party for:

- a) errors or delays that are outside the defaulting party's reasonable control, including general internet or line delays, power failure or faults on any machines; or
- b) errors caused by the other party's systems or actions, negligence or omissions, which shall be the sole responsibility of that party.

The total and maximum liability in each twelve (12) month period of either party towards the other party under any provision of the Data Processing Agreement or any transaction contemplated by the Data Processing Agreement shall in no event exceed an amount equal to the total amounts paid for the Services under the Agreement in the twelve (12) months preceding the event that incurs liability.

The above limitations shall not apply to damages attributable to fraud, gross negligence or intentional misconduct.

## **16 NOTICES AND AMENDMENTS**

All notices relating to the Processing Agreement shall be submitted in writing to the email address stated on the first page of the Processing Agreement.

In case changes in Data Protection Legislation, a judgement or opinion from another authoritative source causes another interpretation of Data Protection Legislation, or changes to the Services require changes to this Processing Agreement, the parties shall in good faith cooperate to update the Processing Agreement accordingly.

Any modification or amendment of this Processing Agreement shall be effective only if agreed in writing and signed by both parties.

## **17 GOVERNING LAW AND LEGAL VENUE**

Governing law, dispute resolution method and legal venue of the Agreement shall apply accordingly.

## **Annex No. 2 – SECURITY**

### **1 Requirement of information security**

The Processor, which according to the Agreement processes Personal Data on behalf of the Controller, shall implement appropriate technical and organisational measures as stipulated in Data Protection Legislation and/or measures imposed by relevant supervisory authority pursuant to Data Protection Legislation or other applicable statutory law to ensure an appropriate level of security.

The Processor shall assess the appropriate level of security and take into account the risks related to the processing in relation to the Services, including risk for accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Person Data transmitted, stored or otherwise processed.

All transmissions of Personal Data between the Processor and the Controller or between the Processor and any third party shall be done at a sufficient security level, or otherwise as agreed between the Parties. This Appendix contains a general description of technical and organisational measures that shall be implemented by the Processor to ensure an appropriate level of security.

To the extent the Processor has access to such information, the Processor shall provide the Controller with general descriptions of its Sub-processors' technical and organisational measures implemented to ensure an appropriate level of security.

### **2 Technical and organisational measures**

#### **2.1 Physical access control**

Processor will take proportionate measures to prevent unauthorised physical access to Processor's premises and facilities holding Personal Data. Measures shall include:

- Procedural and/or physical access control systems
- Door locking or other electronic access control measures
- Alarm system, video/CCTV monitor or other surveillance facilities
- Logging of facility entries/exits
- ID, key or other access requirements

#### **2.2 Access control to systems**

Processor will take proportionate measures to prevent unauthorised access to systems holding Personal Data. Measures shall include:

- Password procedures (including e.g. requirements to length or special characters, forced change of password on frequent basis etc.)
- Access to systems subject to approval from HR management or IT system administrators
- No access to systems for guest users or anonymous accounts
- Central management of system access
- Routines of manual lock when workstations are left unattended, and automatic lock within maximum 5 minutes
- Restrictions on use of removable media, such as memory sticks, CD/DVD disks or portable hard drives, and requirements of encryption

#### **2.3 Access control to data**

Processor will take proportionate measures to prevent authorised users from accessing data beyond their authorised access rights, and to prevent the unauthorised access to or removal, modification or disclosure of Personal Data. Measures shall include:

- Differentiated access rights, defined according to duties
- Automated log of user access via IT systems

#### **2.4 Data entry control**

Processor will take proportionate measures to check and establish whether and by whom Personal Data has been supplied in the systems, modified or removed. Measures shall include:

- Differentiated access rights based on duties
- Automated log of user access, and frequent review of security logs to uncover and follow-up on any potential incidents
- Ensure that it is possible to verify and establish to which bodies Personal Data have been or may be transmitted or made available using data communication equipment

- Ensure that it is possible to verify and establish which Personal Data have been entered into data-processing systems, altered or deleted, and when and by whom the Personal Data have been input, altered or deleted

#### 2.5 Disclosure control

Processor will take proportionate measures to prevent unauthorised access, alteration or removal of Personal Data during transfer of the Personal Data. Measures shall include:

- Use of state of the art encryption on all electronic transfer of Personal Data
- Encryption using a VPN or HTTPS for remote access, transport and communication of Personal Data
- Audit trail of all data transfers
- Compulsory use of wholly-owned private networks for Personal Data transfers

#### 2.6 Availability control

Processor will take proportionate measures to ensure that Personal Data are protected from accidental destruction or loss. Measures shall include:

- Frequent back-up of Personal Data
- Remote storage
- Use of anti-virus/firewall protection
- Monitoring of systems in order to detect virus etc.
- Ensure stored Personal Data cannot be corrupted by means of malfunctioning of the system
- Ensure that installed systems may, in the case of interruption, be restored
- Uninterruptible power supply (UPS)
- Business Continuity procedures

#### 2.7 Separation control

Processor will take proportionate measures to ensure that Personal Data collected for different purposes are processed separately. Measures shall include:

- Restrictions on access to Personal Data stored for different purposes based on duties
- Segregation of business IT systems

#### 2.8 Job/subcontractor control

Processor shall implement measures to ensure that, in the case of commissioned processing of Personal Data, the Personal Data is processed strictly in accordance with the Controller's instructions. Measures shall include:

- Unambiguous wording of contractual instructions
- Monitoring of contract performance

#### 2.9 Training and awareness

Processor shall ensure that all employees are aware of routines on security and confidentiality, through:

- Unambiguous regulations in employment contracts on confidentiality, security and compliance with internal routines
- Internal routines and courses on requirements of processing of Personal Data to create awareness