DATA PROTECTION AND PROCESSING OF PERSONAL DATA

1 DEFINITIONS

The concepts used in this Appendix have the same meaning as those used in the EU's General Data Protection Regulation (2016/679, '**GDPR**'). Such concepts include especially the following: controller, processor, personal data, data subject, processing, and personal data breach.

2 PURPOSE AND NATURE OF THE PROCESSING OF PERSONAL DATA

In this Appendix, NextUp and the Customer agree on the conditions and procedures under which NextUp processes personal data on behalf of the Customer (i.e. the data controller).

NextUp will process personal data exclusively for the purposes of implementing the Services agreed with the Customer, unless, and to the extent, the legislation governing NextUp otherwise requires.

NextUp does not have the right to process personal data for purposes other than those referred to above, or for the benefit of any party other than the Customer or a party specified by the Customer.

NextUp will notify the Customer immediately if it considers that the written guidelines issued by the Customer regarding the processing violate the GDPR or other mandatory provisions governing NextUp. In addition to the conditions set out in this Appendix, NextUp ('the processor') and the Customer ('the controller') are also required comply with the mandatory data protection legislation valid at any given time.

3 PERSONAL DATA AND CATEGORIES OF DATA SUBJECTS UNDERGOING PROCESSING

NextUp may only process personal data imported to the NextUp system by the Customer where this is necessary for the provision of the Services.

The Customer is responsible for obtaining all the authorisations and consents for NextUp required from the data subjects, as well as for drawing up the required data file descriptions and implementing the measures necessary to implement the tasks and Services agreed between NextUp and the Customer and to process the related personal data of the Customer. The Customer is liable for ensuring that all data stored in the NextUp system is timely and appropriate. Consequently, the Customer is responsible for any required rectification, updates, erasure or other alteration of the personal data. NextUp erases all logging data from its systems that is older than 90 days.

4 DATA SECURITY

The Customer is responsible for the data protection and data security concerning its own computers, data systems, local area networks, and other similar data communications devices or systems. The Customer is also liable for any sanctions arising from violations concerning these, as well as for any damage caused to NextUp or third parties from viruses or other types of malware introduced to the NextUp service network by the Customer.

NextUp observes at least the minimum data security requirements and practices that can be expected of diligent and professional operators in the industry. NextUp implements the appropriate technical and organisational measures required in the GDPR to prevent any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

NextUp plans the measures taking into account the applicable technology, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks related to the processing.

NextUp takes reasonable measures to prevent the access of viruses or other harmful or damaging programmes or codes into the Customer's data systems.

NextUp has implemented the following data security measures: training of staff on the processing of personal data, restricting access to data, password protection, backup files, and firewalls.

On request, NextUp can provide the Customer with a separate report of its data security policies.

5 TRANSMISSION OF DATA AND SUBCONTRACTING

NextUp will not transfer any personal data of the Customer outside the EU or the EEA, unless the Customer has provided its explicit written approval for the measure in advance.

NextUp has the right to use the services of teleoperators and communications partners in the transmission of SMS messages over mobile networks.

When using services of another data processor, NextUp commits to agree with the service provider that the processing will be carried out in compliance with the same data protection conditions as specified in this Appendix.

6 CONFIDENTIALITY

All personal data processed by NextUp on behalf of the Customer is considered confidential data. NextUp keeps the data secret, refrains from disclosing or divulging it to a third party and uses the data exclusively for the purposes agreed. NextUp discloses or divulges personal data only to employees or other parties (including possible subcontractors) who need to be aware of the data for the fulfilment of the purpose of the Agreement or who are obligated under a service, employment or other contract or the law to keep the data confidential. The non-disclosure obligation remains in force after the expiry of the Agreement.

7 PERSONAL DATA BREACHES

NextUp will document and investigate all security breaches or incidents observed or suspected in its activities and report any personal data breaches to the Customer concerning the processing it has become aware of without any undue delay so that the Customer has the opportunity to comply with the notification obligations set out to data controllers in the GDPR. NextUp will provide the Customer with sufficient details about a personal data breach. NextUp also agrees to provide reasonable assistance to the Customer so that the Customer can fulfil its obligations under the GDPR. Furthermore, NextUp commits to taking necessary, reasonable, further measures to mitigate harmful impacts of personal data breaches and to avoid any future breaches.

8 DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

If NextUp discovers that the planned processing would result in a high risk to the rights and freedoms of natural persons, it will inform the Customer of the matter and, where necessary, assist the Customer in the implementation of a data protection impact assessment. Furthermore, NextUp commits to assisting the Customer in prior consultations, insofar as this is possible, if the Customer is required to consult a supervisory authority prior to the processing of personal data.

9 RESPONDING TO REQUESTS FROM DATA SUBJECTS

NextUp commits to assisting the Customer by taking appropriate technical and organisational measures, insofar as this is possible and without any undue delay, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights laid down in the GDPR. These rights include, for example, the right of access by the data subject, the right to rectification, the right to prohibit processing, the right to erasure ('the right to be forgotten'), the right to the restriction of processing, and right to have one's personal data transmitted to another system. Where such requests are presented directly to NextUp, NextUp will notify the Customer of the requests immediately.

In such cases, NextUp must also consider its real capabilities on a case-by-case basis to respond to the request presented by a data subject.

10 ACCOUNTABILITY AND AUDITS

NextUp makes available all the information necessary to the Customer to demonstrate compliance with the obligations agreed in the General Terms and Conditions and laid down in the mandatory data protection legislation, insofar as NextUp has access to such information.

NextUp also allows for and reasonably contributes to audits, including inspections, carried out on NextUp premises, systems, processes and documentation by the Customer or another auditor mandated by the Customer, where the Customer considers such an audit necessary. Audits must be carried out during the normal business hours and so that they cause minimum disturbance to NextUp's business operations. The Customer is responsible for any costs arising from audits. The Customer must notify NextUp of such audits at least thirty (30) days in advance. The auditor may not be NextUp's competitor.

11 ERASURE OF DATA

After the end of the provision of the Services, NextUp commits to destroying all personal and other data stored by the Customer in the Services and any related logging data within ninety (90) days of the termination of the Services, as well as any existing copies, unless NextUp is obligated to retain the personal data pursuant to applicable law or unless NextUp has another justifiable reason to retain such data under the GDPR.