SAFESTATE - DATA PROCESSING ADDENDUM

1. GENERAL

1.1. This Data Processing Addendum ("DPA") supplements the Safestate Terms of Service, as updated from time to time between Customer (controller) and Safestate (processor), or other agreement between Customer and Safestate governing Customer's use of the Services (the "Service agreement") when the GDPR applies to your use of the Safestate Services to process Customer Data. Controller and Processor are jointly referred to as "Parties".

2. INSTRUCTIONS FROM, AND CONTROL BY, THE CONTROLLER

2.1. The parties agree that this DPA and the Service agreement (including the provision of instructions via configuration tools made available by Safestate for the Services) constitute Customer's documented instructions regarding Safestate processing of Customer Data. Safestate will process Customer Data only in accordance with documented Instructions. Additional instructions outside the scope of the Instructions (if any) require prior written agreement between Safestate and Customer, including agreement on any additional fees payable by Customer to Safestate for carrying out such instructions. Further details regarding the processing of Personal Data are specified in Appendix A.

2.2. If the Processor deems the instructions insufficient for the fulfilment of this DPA, the Processor shall, without undue delay, inform the Controller thereof and fulfilment of the Service Agreement or this DPA may be affected by the lack of instructions while the Processor awaits further instructions from the Controller.

2.3. The Processor shall, at the request by the Controller, make available all information necessary to demonstrate compliance with Applicable law and this DPA. The Parties acknowledge that the Controller shall have the right to request an audit upon written notice provided at least sixty (60) days in advance to the Processor and verify that the Processor complies with this Agreement, through review of the Processor's policies, procedures, and documentation, solely as they relate to compliance with this Agreement once per year. Costs of such audit shall be borne by each Party for themselves. For any subsequent audit request amounting to more than once per year, the Controller shall have the right to, entirely at its own cost and upon at least 60 days in advance written notice to the Processor, conduct such review or appoint a third party to conduct the review. Such review:

2.3.1. Shall be conducted during Processor's regular business hours.
2.3.2. may only be conducted by a party approved by the Processor who is subject to a confidentiality agreement with Processor; and
2.3.3. must be performed in accordance with Processor's security requirements.

2.4. The Processor shall be obligated to, without any charge (other than for costs incurred as a result of assisting the foregoing review), give such assistance as is reasonably necessary to perform such review. If the Controller should find breaches or flaws of

importance to the Controller, the Controller shall have the right to terminate this DPA and the Service Agreement effective immediately. This right does not include on-site access to the Processor's offices or facilities, unless necessary.

3. NEW FEATURES AFFECTING THE SERVICE AGREEMENT

If the Processor's commitment in accordance with the Service agreement changes due to addition of new features, which may lead to new categories of processing or processing of new personal data types, the Controller shall immediately be informed about such changes and have the right to oppose such changes, where feasible. If opposition to such changes, in Processor's opinion, prevents effective provision of Processor's services, Processor may terminate the Service Agreement without penalty or liability.

4. PROHIBITION AGAINST TRANSFER TO THIRD COUNTRY

4.1. The Processor shall process Personal Data only within, and on devices physically located within, the EU/EEA, or such third country deemed to offer an adequate level of security by the European Commission, or by such DPA 2 suppliers that have entered into binding agreements that fully comply with the lawfulness of third country transfers.

4.2. Where the Processor transfers Personal Data outside the EU/EEA, the Processor shall ensure to enter the EU Standard Contractual Clauses where appropriate or undertake other appropriate safeguards to execute such a transfer in accordance with chapter V of the GDPR.

5. REQUESTS FROM AND CONTACTS WITH AUTHORITIES AND DATA SUBJECTS

5.1. In case a data subject, the Swedish Data Protection Authority or other authority/authorities which supersedes the Swedish Data Protection Authority or otherwise assumes the relevant responsibilities or any third-party requests information regarding the processing of Personal Data from the Processor, the Processor shall refer the request to the Controller. The Processor shall not be entitled to disclose any Personal Data or information regarding the processing of Personal Data unless otherwise explicitly instructed by the Controller.

5.2. The Processor shall, without delay, inform the Controller about any request or other contacts with the Swedish Data Protection Authority or any other data protection authority that affects the processing of Personal Data provided by the Controller to the Processor. The Processor has no right to represent or act on behalf of the Controller in relation to the data subject, the Swedish Data Protection Authority, another authority or any third party.

5.3. The Processor shall, dependent on the information available to the Processor, at Controller's sole cost, reasonably assist the Controller in presenting such information that has been requested by the Swedish Data Protection Authority, another authority, or the data subject.

6. SECURITY

6.1. The Processor shall implement appropriate technical and organizational measures to protect the Personal Data in accordance with Article 32 of the European Data Protection Regulation ("GDPR") from unauthorized access, destruction, loss, or alteration. The measures shall be appropriate with respect to; (a) available technology, (b) costs, (c) specific risks associated with the processing, and (d) the sensitivity of the Personal Data. Notwithstanding the generality of the above, the Processor shall comply with those security measures set out in Appendix B.

6.2. Considering the nature of processing and insofar as this is possible, the Processor undertakes to assist the Controller with ensuring compliance with obligations such as security measures, breach notification, data protection impact assessments as well as prior consultation with the Supervisory Authorities where applicable.

6.3. The Processor shall Implement appropriate technical and practical measures to enable investigations of possible and suspected security breaches regarding Personal Data, such as unauthorized access, destruction, loss, or alteration.

6.4. The Processor warrants that all who have access to Personal Data are bound by confidentiality. For the avoidance of any doubt, such confidentiality shall apply also in contacts with authorities and data subjects.

6.5. The Processor shall notify the Controller without delay after becoming aware of a personal data breach. 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. The notification shall include, to the extent available to the Processor, at least the following: i. description of the nature of the personal data breach including categories and approximate number of data subjects concerned and approximate number of personal data records concerned. ii. a description of the likely consequences of the breach. iii. a description of the measures taken or planned to be taken to address the breach. DPA 3

6.6. If it is not possible to provide all the above information, the notification may be executed in phases without undue delay

7. SUB-PROCESSORS

7.1. The Processor shall have the right to use sub-contractors for the processing of Personal Data ("Subprocessors"), provided that the Sub-processors are bound by way of contract to at least the same commitments and obligations toward the Controller as the Processor, in accordance with this DPA. Subject to the limitations of liability contained in the Service Agreement, the Processor is fully liable toward the Controller for the Subprocessor's actions and any failure by the Sub-processor to adhere to its data protection obligations when processing Personal Data received by the Processor from the Controller.

7.2. Before appointing a Sub-processor, the Processor shall inform the Controller of such plans and which Subprocessor is considered. The Controller shall have the right to, if a reasonable basis exists, object to the engagement of a specific Sub-processor with regards to Personal Data it supplies to the Processor within 30 calendar days from being notified. If, within 30 calendar days of receipt of that notice, the Controller notifies Processor in writing of any objections (on reasonable grounds) to the proposed appointment, and that objection, in Processor's opinion, prevents effective provision of the Processor's services under the Service Agreement, either Party may determine terminate the Service Agreement without penalty or liability. The Processor shall use reasonable endeavours to address any objections of the Controller and take necessary, and reasonable, steps to meet such requirements.

7.3. The current list of existing and approved Sub-processors is enclosed in Appendix C together with information on the services they provide.

8. TERM AND TERMINATION

This DPA shall remain in force during the time the Processor is processing Personal Data for the Controller. The Controller and Processor agree that the Processor and any Sub-processors shall, following the termination of this DPA, either return all Personal Data, including copies, to the Controller, or erase the same in accordance with Section 9. The Processor commits to attest in writing that such return and/or erasure or anonymization has been completed.

9. ERASURE AND RETURNING OF PERSONAL DATA

9.1. Upon termination of this DPA, the Controller may request that Processor erase or return all Personal Data to Controller and ensure that all Sub-processors do the same.

9.2. If the Controller has neither requested to erase or return the Personal Data within 30 days from the termination of this DPA, the Processor shall be entitled to delete all the Personal Data it has processed on behalf of the Controller including all copies. In such event, the Processor will either completely delete the Personal Data from any medium where it is stored, in a way that it cannot be restored, or ensure that it is anonymized in such a way that it is not possible to connect to an individual or recreate.

10. LIMITATION OF LIABILITY
Subject to the Service Agreement, the Processor shall be liable for damages caused to the Controller following the Processor's processing of Personal Data in violation with the Controller's instructions, this DPA, the Service Agreement and Applicable law. The Processor shall not be liable for the Controllers legal expenses or costs related to conciliation agreements between the Controller and a third party. The liability is limited to claims affirmed by a relevant authority or a court of law. DPA 4

11. DATA PROTECTION REGULATIONS The processor agrees that it will make any necessary changes and amendments to this DPA for it to be compliant with Applicable law with regards to precedents, and new or updated guidelines or other practices from a relevant authority.

12. DISPUTE AND APPLICABLE LAW Any dispute, controversy or claim arising out of or in connection with this DPA, or the breach, termination, or invalidity thereof, shall be settled as stipulated in the Service Agreement.

13. MISCELLANEOUS

    13.1. If one or more provisions of this DPA is declared to be invalid or unenforceable, the remaining provisions will continue in full force and effect.

    13.2. This DPA supersedes all prior arrangements or undertakings between the Parties in relation to processing of personal data that are not consistent with this DPA.