ADDSECURES WAY OF PROCESSING PERSONAL DATA

For the processing of personal data that AddSecure performs on behalf of its customers, AddSecure becomes a Personal Data Processor. If you are a contact person for one of AddSecure's customers, your personal data is your employer's responsibility. AddSecure is responsible for ensuring that your personal data is adequately protected when processed by us. The obligations that AddSecure has as a Personal Data Processor are regulated in the main customer agreement and in AddSecure's general personal data agreement which is provided as an appendix to the main agreement, except in cases where the customer has chosen to sign a separate personal data agreement. AddSecure's Privacy Policy and General Personal Data Agreement is accessible on AddSecure's website.

ADDSECURE AS PERSONAL DATA PROCESSOR

As part of AddSecure's offering, various web-based services are included, such as AddView, SafeView, SecureApps, Telecall and various Partner portals, hereinafter referred to as "**the Service**". AddSecure acts as Personal Data Processor for the Service and is therefore responsible for the technical and organizational security measures needed to make sure that the storage of and access to the personal data is conducted in a safe way with regard to recent developments, implementation costs, type of processing, scope, context and purpose, and also risks of varying probability and seriousness, concerning people's rights and freedoms.

The customer is responsible for the processing of personal data and therefore acts as personal data controller for the Service, i.e. the customer that is registered as an invoice recipient for the Service. AddSecure processes personal data on behalf of the customer.

THIS NEEDS TO BE CONSIDERED AS A PERSONAL DATA CONTROLLER

The Personal Data Controller's responsibility is regulated in the General Data Protection Regulation (GDPR). As a Personal Data Controller, your company (as an AddSecure customer) needs to control what type of data you process, what purpose you have for processing the data, how long the data can be stored and on what legal basis you process the data. You may also need to obtain the consent of the registered persons. More information about the responsibility of the personal data controller can be found on the web: https://gdpr-info.eu/.

GENERAL PERSONAL DATA PROCESSOR AGREEMENT

1. Parties

AddSecure Group (”**AddSecure**”) consist of the companies:

- AddSecure AB (Sweden) SE5565272001
- AddSecure AG (Switzerland), CH02030377837
- AddSecure AS (Norway) NO976145178
- AddSecure Ltd (England), GB03593453
- AddSecure Oy (Finland), FI28410722
- AddSecure Smart Grids AB (Sweden), SE5590442314
- Contal Security AB (Sweden), SE5564684123

Between the Customer (in the Main agreement) referred to below as the **“Personal Data Controller”** and **AddSecure** referred to below as **“Personal Data Processor”** the following Personal Data Processor Agreement is concluded as a part of the Main Agreement.

2. PURPOSE

2.1

The purpose of this Personal Data Processor Agreement is to ensure that the Personal Data Processor’s processing of personal data on behalf of the Personal Data Controller, only occur in accordance with this Personal Data Processor Agreement and otherwise in accordance with the requirements stated in Article 28 of General Data Protection Regulation (GDPR) (EU) 2016/679

2.2

The subject of personal data processing in accordance with this Personal Data Processor Agreement is personal data related to systems and services that fall within the scope of the Main Agreement.

Processing will occur during the Main Agreement’s validity period and it may consist of various forms of action having to do with personal data, such as data collection, registration, organisation, structuring, storing, processing, alteration, preparation, reading, use, issuance, dissemination or other forms of processing, adjustment or consolidation, limitation, deletion or destruction.

Processing relates to all types of personal data that the Personal Data Processor has access to in order to fulfil the obligations stated in the Main Agreement.

3. DEFINITIONS

This Personal Data Processor Agreement shall be interpreted in accordance with – and contain the definitions stated in – Article 4 of the General Data Protection Regulation (GDPR).

4. PERSONAL DATA CONTROLLER

The Personal Data Controller is responsible for ensuring compliance with the General Data Protection Regulation (GDPR), regarding processing of personal data and use of assistants. The Personal Data Controller is entitled to control how the Personal Data Processor processes personal data and shall therefore provide the documented instructions required for the Personal Data Processor's processing of data.

5. RESPONSIBILITIES OF THE PERSONAL DATA PROCESSOR

The Personal Data Processor undertakes to only process personal data concerning contractual personal data in accordance with the documented instructions from the Personal Data Controller and in accordance with this Personal Data Processor Agreement and the Main Agreement.

5.1

The Personal Data Processor undertakes to comply with applicable law when processing personal data, particularly Article 4 of the General Data Protection Regulation (GDPR). In addition the Personal Data Processor must comply with regulations, statements and recommendations on permitted processing of personal data issued by the relevant EU body.

5.2

The Personal Data Processor certifies that the necessary technical and organisational safeguards have been taken with respect to the personal data, such that the processing meets the requirements of the General Data Protection Regulation (GDPR) and protects the rights of the registered individuals.

5.3

The Personal Data Processor must, in accordance with the Personal Data Controller's instructions, correct, delete or hand over inaccurate, incomplete or outdated personal data without undue delay.

6. SECURITY MEASURES

The Personal Data Processor must take and maintain appropriate technical and organisational security measures to protect the personal data.

6.1

The Personal Data Processor's security measures must provide the level of protection specified in applicable law and, upon its entry into force, the General Data Protection Regulation and which otherwise is applicable given the technical possibilities, cost of implementation, specific risks of processing and the extent to which the processed personal data is, or is likely perceived as being, sensitive.

6.2

The Personal Data Processor is responsible for ensuring that their own operations are run in a way that otherwise ensures adequate information security.

6.3

The Personal Data Processor must ensure that employees, consultants and others for whom the Personal Data Processor is responsible, and who process or have access to personal data, are bound by an appropriate confidentiality agreement and are informed on how personal data processing must be done in accordance with instructions from the Personal Data Controller.

6.4

The Personal Data Processor's technical and organisational security measures must take into account the latest technological developments, implementation costs, and the nature, scope, context and purpose of the personal data processing, including risks to natural persons' rights and freedoms of varying severity and probability, to ensure that there is a suitable security level in relation to the risk.

6.5

The Personal Data Processor's implementation of security measures shall, where appropriate, include pseudonymization and encryption of personal data, the ability to continuously ensure confidentiality, integrity, availability and resilience of processing systems and services ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident and a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

6.6

When assessing the appropriate level of security, special consideration shall be given to the risk of unintentional or unlawful destruction, loss, alteration or unauthorised disclosure or access to the personal data.

7. INCIDENTS

The Personal Data Processor shall, upon discovery of a known or suspected security incident, such as unauthorised access, destruction, alteration or other unlawful interference with the personal data, immediately investigate the incident, take appropriate measures to remedy the situation and prevent its reoccurrence, along with informing the Personal Data Controller by providing an Incident Report, unless the Personal Data Processor can demonstrate that there is no risk that the rights and freedoms of the data subjects are violated as a consequence of the personal data incident.

7.1

An Incident Report shall, include a description of the nature of the incident, categories of and the approximate number of registered individuals affected and the categories of and the approximate number of personal data items affected, description of the likely consequences stemming from the

incident and an action plan for appropriate measures to mitigate the potential adverse effects. Furthermore, the Incident Report must contain contact information for the Data Protection Officer or other contact points for obtaining further information about the incident.

8. SUBCONTRACTORS (ASSISTANTS TO THE PERSONAL DATA PROCESSOR)

The Personal Data Processor is entitled to subcontract processing of personal data to sub-processors within and outside of the EU/EEA. The Personal Data Controller hereby approves that processing of personal data may be carried out by sub-processors usually used in the business to perform all or part of the processing of personal data without prior written consent of the Personal Data Controller. The Personal Data Processor must ensure that sub-processors are bound by written agreements that they provide at least the same level of data protection as the obligations under this Personal Data Processor Agreement. If any sub-processor fails to fulfil the obligations in accordance with above, the Personal Data Processor is responsible for the non-performance of such sub-processors obligations.

The Personal Data Processor will inform the Personal Data Controller of any intentions to replace or hire a new sub-processor, with exception for sub-processors usually used in the business. The information will include an indication of the name of the sub-processor and the geographic location of the processing of personal data. The Personal Data Controller has the right to submit a written objection to the replacement or hiring of such new sub-processor within fourteen days from receipt of notice. Should the Personal Data Processor despite the Personal Data Controller's objection still wish to replace or hire a new sub-processor, the Personal Data Controller is entitled to terminate the Agreement in accordance with section 12.

9. TRANSPARENCY

In order to ensure maintenance of an appropriate level of security and compliance with this Personal Data Processor Agreement, the Personal Data Controller is entitled to the requisite transparency into those parts of the Personal Data Processor's organisation and systems used for personal data processing.

10. LIABILITY FOR DAMAGE

If the Personal Data Processor's processing of personal data or failure to process personal data, in breach of this personal data agreement or the instructions issued by the Personal Data Controller, results in damages to the Personal Data Controller, such damages shall be reimbursed by the Personal Data Processor.

11. TRANSFER OF THE AGREEMENT

Transfer of this Personal Data Processor Agreement may only occur in conjunction with a transfer of the Main Agreement.

12. DURATION OF THE AGREEMENT

This agreement is valid as of the conclusion date of the Main Agreement and as long as the Personal Data Processor stores or in any other way processes personal data on behalf of the Personal Data Controller.

12.1

Upon termination of the Personal Data Processor Agreement, the Personal Data Processor shall, in accordance with the Personal Data Controller's instructions, delete or return all data containing personal details, on all media used to store the personal data, and afterwards, delete any copies.

13. DISPUTES AND APPLICABLE LAW

The country where the Personal Data Controller is situated is the applicable country law to this agreement.

Any dispute stemming from this Personal Data Processor Agreement shall be settled in accordance with the terms on dispute resolution that are specified in the Main Agreement.