Data Processing Agreement

Access Control Cloud Applications

INTRODUCTION

You are a customer that concluded a contract with the Spanish company Salto Systems, S.L. for the rendering of the SaaS services named “Salto KS Keys as a Service” through the “Salto KS Keys as a Service” platform (respectively, “KS Services” and the “Platform”), subject to the General Terms & Conditions of the services “Salto KS Key as a Service” which are applicable from time to time (the “General Conditions”).

In addition, Salto Systems, S.L. and/or the subsidiary of Salto Systems, S.L. corresponding to the geographical area where the customer is located may need to render technical support services related to such KS Services and/or to the associated locking hardware (the “Technical Support Services”). The KS Services and the Technical Support Services shall hereinafter jointly be referred to as the “Services”.

In order to render the Services to you, Salto Systems, S.L. and occasionally the subsidiary of Salto Systems, S.L. corresponding to the geographical area where you are located, need to access and process personal data on your behalf. Salto Systems, S.L. and the corresponding subsidiary of Salto Systems, S.L. acts each as a data processor of such personal data and you act as the data controller of such personal data.

Therefore, Salto Systems, S.L. and the corresponding subsidiary of Salto Systems, S.L., located inside the European Economic Area (hereinafter “EEA”) ARE OBLIGED under the European General Data Protection Regulation (the “ GDPR”) TO CONCLUDE A DATA PROCESSING AGREEMENT with the customer.

Accordingly, this Data Processing Agreement (the “DPA”) is formalized between (a) the customer subscribing the services KS Services (the “Customer” or the “Data Controller”), (b) Salto Systems, S.L. (“Salto HQ”) and, (c) the subsidiary of Salto HQ corresponding to the geographical area where the Customer is located (whose concrete data and identity can be consulted at https://www.saltosystems.com/en/quick-links/salto-systems-offices/) (the “Salto’s Subsidiary”). Salto HQ and Salto’s Subsidiary shall also jointly and indistinctly be referred to as “Salto” or the “Data Processor”.

If you are a natural person acting in the course of a purely personal or household activity, the content of the DPA applicable to you is the content of section A. In the remaining cases, the content of the DPA applicable to you shall be the one set forth in section B.

The parties acknowledge that non-European legislation may also apply to the processing of the personal data. Except to the extent specifically indicated in this DPA, the content of this DPA shall apply regardless of the data protection legislation which is applicable to the processing of data.

By accepting the General Conditions, the parties hereby enter into this DPA as required by the applicable legislation, which the Client hereby accepts and agrees.

SECTION A: APPLICABLE TO NATURAL PERSONS ACTING IN THE COURSE OF A PURELY PERSONAL OR HOUSEHOLD ACTIVITY

This DPA shall enter into force on the date of its acceptance by the Customer and shall remain in force until the KS Services

have been definitely terminated. For the purposes of this DPA, the KS Services shall be deemed definitely terminated on the earlier of the following dates:

- Once the term of the KS Services has been terminated in accordance with the General Conditions which may apply from time to time (i.e. when the Customer does not renew the KS Services) and the Customer has expressly notified in writing to Salto its intention not to further renew the KS Services in the future anymore, or;
- Once the term of the KS Services has been terminated in accordance with the General Conditions which may apply from time to time (i.e. when the Customer does not renew the KS Services), and a period of 6 months has elapsed without the Customer having renewed the term of the KS Services.

This DPA contains a detailed description of the services provided. The data processing activities that Salto will carry out will only be those strictly necessary to provide the Services hired by the Customer.

Salto may only process personal data in order to provide the Services hired by the Customer. In this sense, Salto shall comply with the obligations established in article 28 of the General Data Protection Regulation (GDPR). Specifically, and without prejudice to the other obligations imposed by the GDPR, Salto, as Data Processor, must comply with the following obligations:

- Use the personal data matter of the processing for the sole purpose of providing the Platform, KS Services, and Technical Support Services and in accordance with the Customer's instructions.
- Not communicate the personal data to third parties, unless the Customer has granted his express authorization.
- Maintain the secrecy regarding the Personal Data to which Salto accessed for the provision of Services, even after the expiry of the term of this DPA.
- Notify the Customer without undue delay since Salto is aware of a personal data breach, through the email address indicated by the Customer at the Platform, together with all the relevant information for the documentation and communication of the incident.
- Process personal data implementing the appropriate security measures in compliance with article 32 GDPR, as well as to observe and adopt the technical and organizational security measures that are necessary in order to ensure the confidentiality, secrecy and integrity of the personal data to which it has access.
- Upon the definite termination of the KS Services, Salto shall destroy the Personal Data, and, if applicable, any copies, documents or supporting materials containing such Personal Data. In any case, Salto may store a copy of Personal Data blocked during the prescription periods of liabilities arising from the execution of the agreed Services. In this case, Salto warrants it will not process such data unless Salto is required to make data available to Public Administration, Judges and Courts during the referred prescription periods.

The Customer grants general authorization to Salto to engage other Data Processors for the processing of the Personal Data.

Moreover, it also grants general authorization in order for such sub-processors to also subcontract to other sub-processors.

The Customer declares that he/she is of legal age and that has been duly authorized to upload the personal data of the data subject to the Platform (including, among others, any specific consent regarding children's personal data) and to grant access to Salto to such personal data for their processing in accordance with the provisions of this DPA.

Salto expressly confirms that it has appointed a Data Protection Officer. For this purpose, if the Customer wishes to contact him/her, you can do so through the following email address: privacy@saltosystems.com

Any communication to be sent to the Customer within the framework of this DPA shall be sent by email to the email address of the owner of the system indicated in the Platform, through the Platform, through the Salto KS's mobile app or by letter with acknowledgement of receipt to the address of the system's owner indicated in the Platform.

In order to allow Salto to render the Platform and the KS Services, as well as the Technical Support Services, the Customer accepts and guarantees to provide Salto with the necessary data so that it can provide the Services. Each of the parties to this DPA will be liable for the direct damages that may arise from the breach of the obligations assumed under it, and must assume, in this case, the compensation for the damages that such failure could cause to the other Party. The total maximum liability of either party towards the other under this DPA will be limited to the maximum liability per event agreed in the General Conditions which may apply from time to time.

The parties of this DPA mutually agree that any differences or disagreements which may arise with regard to the interpretation and/or performance of the DPA shall be resolved by the Courts of the jurisdiction in which Salto HQ has its registered office pursuant to Spanish law and expressly waive any other jurisdiction which may correspond to them.

SECTION B: APPLICABLE TO LEGAL ENTITIES AND NATURAL PERSONS NOT ACTING IN THE COURSE OF A PURELY PERSONAL OR HOUSEHOLD ACTIVITY

1. Subject matter of DPA

1.1. The subject matter of this DPA is the data processing carried out by Salto HQ and by Salto's Subsidiary, as Data Processors, on behalf of the Data Controller, in compliance with its instructions throughout the main contractual relationship that binds the parties, in accordance with the obligations provided for in Articles 28 and 29 GDPR and the applicable data protection local law.

1.2. Personal Data. For the performance of the Services, the Data Controller shall make available to the Data Processor the personal data concerning the following categories and data subjects name and surname, e-mail, mobile telephone number, country, user picture (optional), address (optional) and language (optional) of the users created by the system owner (hereinafter the "Personal Data").

1.3. Data Processing. The data processing will consist of:
a. the hosting and the access by Salto HQ to the Personal Data uploaded to the Platform by the Customer and to the database containing such Personal Data, in order to provide the KS Services, maintain the Platform and render the Technical Support Services ("Processing 1").
b. the access to all or part of the database containing the Personal Data by Salto's Subsidiary in order to render, upon the Customer's request, the Technical Support Services (the "Processing 2").

1.4. Duration. This DPA shall enter into force on the date of its acceptance by the Customer and shall remain in force until the KS Services have been definitely terminated. For the purposes of this DPA, the KS Services shall be deemed definitely terminated on the earlier of the following dates:
a. Once the term of the KS Services has been terminated in accordance with the General Conditions which may apply from time to time (i.e. when the Data Controller does not renew the KS Services) and the Data Controller has expressly notified in writing to the Data Processor its intention not to further renew the KS Services in the future
anymore or;
b. Once the term of the KS Services has been terminated in accordance with the General Conditions which may apply from

time to time (i.e. when the Data Controller does not renew the KS Services), and a period of 6 months has elapsed without the Data Controller having renewed the term of the KS Services. The parties agree that on the termination of the Technical Support Services and on the definite termination of the KS Services, the provisions of clause 2.5 shall apply with respect to the destruction of the Personal Data.

2. Obligations of the Data Processor

2.1. General Obligations. Each Data Processor is obliged to:

2.1.1. Use the Personal Data subject matter of the processing, as well as such data that may be collected by the Data Processor, only when necessary for the performance of the Services and in accordance with the provisions of the General Conditions that may apply from time to time. In any case, Personal Data may not be used by the Data Processor for its own purposes.

2.1.2. Promptly notify the Data Controller when the Data Processor or its staff finds that the GDPR or other applicable data protection local laws are being infringed.

2.1.3. Process Personal Data in accordance with the Data Controller's instructions, which must be transferred in writing to the following email address: privacy@saltosystems.com.
In those cases in which the Data Processor considers that an instruction of the Data Controller breaches any legal provision in terms of data protection of the EEA or of any of the EEA Member States, it must inform the Data Controller in writing immediately. In the event that a proven breach has occurred, the Data Processor may suspend the execution of that instruction, until the admissibility of said instruction has been clarified.

2.1.4. Ensure that anyone acting on their behalf or on behalf of the Data Controller and having access to the Personal Data, only processes such data according to the instructions of the Data Controller, unless it must do so in compliance with any legal provision of the EEA of any of the Member States of the EEA or of any other applicable legislation.

2.1.5. Implement the technical and organizational security measures in accordance with article 32 GDPR, for which purposes the Data Processor undertakes to assess potential risks arising from the data processing activities that it carries out, taking into account the means that are used to provide the services (technology, resources, etc.) and other circumstances which may have a security impact.

2.1.6. Assist the Data Controller in ensuring compliance with obligations regarding security of processing, notifications of personal data breaches to the corresponding supervisory authority and to the affected data subjects, data protection impact assessment and prior consultations pursuant to articles 32 to 36 GDPR or applicable local data protection regulation, taking into account the nature of processing and the information available to the Data Processor.
Notifications to be made to the Customer under this DPA will be made to the email address of the system owner registered at the Platform. Customer is solely responsible for ensuring that such email address is current and valid.

2.1.7. When necessary, maintain a record of processing activities on behalf of the Data Controller in accordance with article 30 GDPR.

2.1.8. Provide the Data Controller with all the necessary information to demonstrate compliance with its obligations. The parties shall agree among themselves the terms under which the Data Processor certifies compliance with its legal

obligations.
Upon the Data Controller's request, the Data Processor will provide the Data Controller with adequate evidence of the implementation of technical and organizational measures in accordance with this DPA, the instructions received, as well as the legal provisions on protection of the EEA or from any of the EEA Member States.

2.1.9. Allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

2.1.10. Maintain the secrecy regarding the Personal Data to which the Data Processor accessed for the provision of Services, even after the expiry of the term of this DPA. The Data Processor undertakes to keep the strictest secrecy and confidentiality with respect to the data, documents and information received or which the Data Processor became aware of as a result of the rendering of the Services, and to protect them against any unauthorized use or unauthorized third parties' inspection.
The Data Processor will immediately inform the Data Controller in writing in case an unauthorized third party has gained access to or has inspected the respective confidential data, documents and information as well as results of work performed within the Services. In such case, the Data Processor will also communicate the name of such third party to the Data Controller.

2.1.11. Ensure that access to Personal Data shall be only authorized to staff or collaborators who committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and which by virtue of the nature of their working duties, are strictly necessary for the provision of the Services.
The Data Processor warrants that authorized staff are duly trained regarding personal data protection and have agreed, expressly and in writing, to comply with the security measures appropriate to the type and purposes of the data processing activities, about which they shall be informed.

2.1.12. For rendering the Services, Salto may engage some third party service providers located outside the EEA who shall process the Personal Data. In that case, Salto shall require that providers comply with the measures designed to protect the Personal Data established in a binding contract, except in cases where the European Commission has determined that the country where the recipient is located provides an adequate level of protection.

2.2. Outsourcing

2.2.1. The Data Controller grants general authorization to Data Processor to engage other data processors for the processing of the Personal Data. Moreover, it also grants general authorization in order for such sub-data processors to also subcontract to other sub-data processors.The Sub-data processor(s) currently engaged in the processing of Personal Data are included in the Appendix 1. When the Data Processor engages other companies, the Data Processor shall inform the Data Controller being deemed automatically included in such Appendix as of such notification, without the need of updating such Appendix.

2.2.2. When the Data Processor engages another Data Processor for carrying out specific processing activities on behalf of the Data Controller, the Data Processor is obliged to sign a Sub-data processing agreement subject to the terms foreseen in this DPA.

2.2.3. The sub-data processor is considered as a data processor and shall not process Personal Data except on instructions from the Data Controller and the Clauses of this DPA. The Data Processor should regulate the new contractual relationship so that the same data protection obligations (instructions, security measures, duties, etc.) and the same formal requirements regarding data processing and rights and freedoms of data subjects are fulfilled by the sub-data processor.

2.3. Exercise of rights

2.3.1. If the data subjects exercise towards the Data Processor the rights of access, rectification, erasure, not to be the subject to a decision based solely on automated processing, restriction of the processing, objection and data portability, the Data Processor shall notify the Data Controller such circumstance by electronic mail to the address included in the Platform. The Data Processor shall assist the Data Controller by appropriate technical and organizational measures, insofar as this is possible, taking into account the nature of the processing, for the fulfillment of the Data Controller's obligation to respond to requests for exercising the data subject's rights granted in Chapter III of the GDPR or applicable local data protection regulation.

2.3.2. In particular, the Platform may include an option for data subjects to delete their account of the Platform. In such cases, the Data Controller shall be notified, by email or by a notification sent to its Platform account, about data subject's request and the date after which such user profile and related data will be unalterably deleted from the Platform or anonymised. The Data Controller shall be entitled to download the data from the Platform before the aforementioned date in order to comply with Data Controller's data retention periods.

2.4. Security Measures

2.4.1. In accordance with the data processing activities identified and, in accordance with the risk analysis carried out by the Data Processor, the Data Processor undertakes to implement the appropriate security measures in compliance with article 32 GDPR.

2.4.2. The Parties may decide to specify the security measures implemented and agreed by the parties in an Appendix to this DPA.

2.5. Termination of Services

2.5.1. *With respect to the Processing 1*: Upon the definite termination of the KS Services (subject to the provisions of clause 1.4 of this DPA), the Data Processor shall destroy the Personal Data, and, if applicable, any copies, documents or supporting materials containing such Personal Data. Accordingly, upon termination of the term of the KS Services in accordance with the General Conditions which may apply from time to time (i.e. when the Data Controller does not renew the KS Services), if not expressly indicated otherwise in writing by the Data Controller, the Data Processor shall maintain the database and the Personal Data contained therein during a period of 6 months with the aim to facilitate the Customer re-activation of the KS Services.
Once such 6 months have elapsed without the Data Controller having reactivated the KS Service or if earlier expressly required in writing by the Data Controller, the KS Services shall be deemed definitely terminated and, thus, the Data Processor shall destroy the Personal Data, and, if applicable, any copies, documents or supporting materials containing such Personal Data.
In any case, the Data Processor may store a copy of Personal Data blocked during the prescription periods of liabilities arising from the execution of the agreed Services. In this case, the Data Processor warrants it will not process it unless the Data Processor is required to make data available to Public Administration, Judges and Courts during the referred prescription periods.

2.5.2. *With respect to the Processing 2*: Upon performance of each of the concrete Technical Support Services (i.e. upon solving the concrete incidence with respect which the Technical Support Services were required to be rendered), Salto shall, without undue delay (which shall not exceed from three (3) calendar days), destroy the Personal Data or any password given to access to such Personal Data, and, if applicable, any copies, documents or supporting materials containing such Personal

Data.

2.6. Personal Data Breach

2.6.1. In case of personal data breach, the Data Processor shall notify the Data Controller without undue delay after becoming aware of a personal data breach, and through the email address indicated by the Data Controller at the Platform, together with all the relevant information for the documentation and communication of the incident.

2.7. Data Protection Officer

2.7.1. The Data Processor expressly confirms that it has appointed a Data Protection Officer. For this purpose, if the Customer wishes to contact him/her, you can do so through the following email address: privacy@saltosystems.com

2.7.2. The Data Processor's Data Protection Officer has to ensure without any restrictions that all relevant EEA or EEA Member State data protection provisions are complied with at the Data Processor and performed in relation to the contractual relationship between the Data Processor and the Data Controller.

2.7.3. In case the Data Protection Officer should detect any irregularities in that connection at the Data Processor, he/she has to inform the Data Controller in writing without undue delay. In such case, the Data Processor's Data Protection Officer shall be expressly exempted from the obligation to observe secrecy towards the Data Controller.

3. Obligations of the Data Controller.

When the Data Controller is located in the EEA, the same accepts and guarantees to:

3.1. Provide the Data Processor with the necessary data so that it can provide the Services.

3.2. Comply with all the obligations set forth in the GDPR for the processing of the Personal Data and ensure, prior to and throughout the processing, full compliance with the GDPR by the Data Controller. Among others, the Data Controller hereby declares that prior to uploading any Personal Data to the Platform and/or to otherwise giving access to the Data Processor to any Personal Data, it will have fulfilled with any legal formalities and requirements and it will have obtained all the consents which are required under the applicable legislation for the collection of the Personal Data (including, among others, any specific consents required for processing of Children's Personal Data, if applicable) and for giving access to the Data Processor to such Personal Data and for the processing of such Personal Data by the Data Processor subject to the provisions of this DPA.

3.3. Supervise the processing of Personal Data.

When the Data controller is located outside the EEA, the same accepts and guarantees to:

3.4. Provide the Data Processor with the necessary data so that it can provide the Services.

3.5. Comply with all the obligations set forth in the applicable data protection legislation. Among others, the Data Controller hereby declares that prior to uploading any Personal Data to the Platform and/or to otherwise giving access to the Data Processor to any Personal Data, it will have fulfilled with any legal formalities and requirements and it will have obtained all the consents which are required under the applicable legislation for the collection of the Personal Data (including, among others, any specific consents required for processing of Children's Personal Data, if applicable), for giving access to the Data

Processor to such Personal Data and for the processing of such Personal Data by the Data Processor subject to the provisions of this DPA.

3.6. Supervise the processing of Personal Data.

4. Liability

Each of the parties to this DPA will be liable for the direct damages that may arise from the breach of the obligations assumed under it, and must assume, in this case, the compensation for the damages that such failure could cause to the other Party. The total maximum liability of either party towards the other under this DPA will be limited to the maximum liability per event agreed in the General Conditions which may apply from time to time.

5. Miscellaneous

5.1. Any alterations of and additions to this DPA must be accepted by the parties and made in writing to become effective.

5.2. This DPA is incorporated and supplements the General Conditions. Moreover, it partially amends and supersedes the provisions of the General Conditions which contravene or are in conflict with the content of this DPA (if any). For the avoidance of doubt, the remaining provisions of the General Conditions remain in effect.

5.3. Any communications to be sent between the Data Processor and the Data Controller within the framework of this DPA shall be made in accordance with the following rules:
a. If addressed to Salto HQ or to the Salto's Subsidiary: shall be sent by email to the email address privacy@saltosystems.com or by letter with acknowledgement of receipt to the following address:

SALTO SYSTEMS, S.L. (Att. Data Protection Officer)
Arkotz 9, Polígono Lanbarren
Oiartzun (Gipuzkoa-Spain)

b. If addressed to the Customer: shall be sent by email to the email address of the owner of the system indicated in the Platform, through the Platform, through the Salto KS's mobile app or by letter with acknowledgement of receipt to the address of the system's owner indicated in the Platform.
As an exception, any specific communication to be sent with respect to the rendering of the Technical Support Services may be made to the specific member of the staff solving the incidence.

6. Governing Law and Jurisdiction

6.1. The parties of this DPA mutually agree that any differences or disagreements which may arise with regard to the interpretation and/or performance of the DPA shall be resolved by the Courts of the jurisdiction in which Salto HQ has its registered office pursuant to Spanish law and expressly waive any other jurisdiction which may correspond to them.

APPENDIX 1: PERSONAL DATA SUB-PROCESSORS

In compliance with article 2.2.1 of the DPA herein, the Data Processor declares, and the Data Controller acknowledges and accepts, that at the date hereof the companies engaged in the processing of Personal Data on behalf of the Data Controller are the followings:

The Processing 1:

- Clay Solutions, B.V. (Salto Group company).
- Clay Solutions, B.V. subcontracts the hosting of the Platform to Microsoft Ireland Operations Limited and Qweb Internet Services B.V.
- Qweb Internet Services B.V. subcontracts the hosting of the Platform to Dataplace B.V.

The Processing 2:

- Salto HQ.
- Clay Solutions, B.V. (Salto Group company).

Disclaimer:

This is a downloadable version of the website content that we make available to you for informative purposes for an easier consultation and filling. However, SALTO assumes no responsibility for any errors or typos that the downloadable version may contain.

As SALTO reserves the right to modify this content from time to time, please check on the Legal section of our website to find the latest version of the legal documents and their updates.