Data Processing Agreement

Catalogic Software, Inc. ("Catalogic") may process personal data in the course of providing its CloudCasa Cloud Services ("Cloud Services" or "the Cloud Services"). This Data Processing Agreement (the "DPA") incorporates the Standard Contractual Clauses Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors and forms part of the Master Service Agreement and all Annexes, Supplements, Exhibits or sub-agreements (collectively defined as "Agreement") between Catalogic and Customer for the purchase of Cloud Services. Any terms not defined have the same definition ascribed to them in the Master Service Agreement, Terms of Service or Standard Contractual Clauses. This DPA has been executed by Catalogic as the data processor. To execute this DPA, Customer should complete Customer's information and return the fully executed DPA to info@catalogicsoftware.com. *Acceptance of this DPA is effective upon Catalogic's email receipt of the signed DPA.*

Revised September, 2023

CLARIFICATION REGARDING FOOTNOTES

In certain instances, footnotes included in the Standard Contracting Clauses ("Clauses") have been omitted to facilitate ease of reading and formatting for posting this DPA on Catalogic's CloudCasa website. These footnotes address specific questions regarding the application of the Clauses under circumstances not relevant to Catalogic Software, Inc. For the purposes of removing any doubt, the omission of any footnote is acknowledged parenthetically [Footnote X omitted] and the Parties (as defined in Annex I) agree that for the purposes of satisfying the requirement in Clause 2(a) that the Standard Contracting Clauses not be changed, such footnote of the Standard Contracting Clauses is incorporated as if set forth in full herein in its entirety. The Standard Contracting Clauses use Modules depending upon the designation of the Parties as processor, controller, or both. The numbering of the footnotes omitted reflects the numbering of the footnotes as they appear in the Clauses and Modules applicable to this Data Processing Agreement.

SECTION I – INTRODUCTION

Clause 1 – Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to

ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2 – Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3 – Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4- Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 – Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and

signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6 – Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7 – Obligations of the Parties

7.1. **Instructions**

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. **Purpose limitation**

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. **Duration of the processing of personal data**

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. **Security of processing**

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised

disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. **Sensitive data**

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. **Documentation and compliance**

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. **Use of sub-processors** (a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The

processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby – in the event the processor has factually disappeared, ceased to exist in law or has become insolvent – the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. **International transfers**

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8 – Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9 – Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 **Data breach concerning data processed by the controller**

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data

breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 **Data breach concerning data processed by the processor**

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10 – Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

> (1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
>
> (2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
>
> (3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I – List of Parties

Primary Controller(s):
Customer and its affiliates:
Name: …
Address: …
Contact person's name, position
contact details: …
Data Protection Officer….

_____(Date)_____

_____
Name and Title of signing individual

Limited Controller – Limited to the collection of minimal staff contact information necessary for Catalogic to render technical support or managing Customer's use of Cloud Services, including data privacy requirements.

Catalogic Systems, Inc.
140 E. Ridgewood Ave.
Suite 415, South Tower, Office 416
Paramus, NJ 07652
Contact Person: Sathya Sankaran, COO
info@catalogicsoftware.com
Telephone: +1 201-249-8980

_____(Date)_____
Sathya Sankaran, Chief Operating Officer

Processor(s):
140 E. Ridgewood Ave.
Suite 415, South Tower, Office 416
Paramus, NJ 07652
Contact Person: Sathya Sankaran, COO
info@catalogicsoftware.com
Telephone: +1 201-249-8980

_____(Date)_____
Sathya Sankaran, Chief Operating Officer

ANNEX II - Description of the processing

Categories of data subjects whose personal data is processed

- Categories of data subjects whose personal data is processed is determined by the controller and may vary depending upon the exact use and configuration of the Cloud Services elected by Customer
- Customer's staff, in the limited capacity as noted below

Categories of personal data processed

- Customer Data subject to backup – due to the nature of Cloud Services and encryption used, the specific types of Personal Data cannot be conclusively established and may vary depending on the exact use and configuration of the Cloud Services elected by Customer.
- CloudCasa login ID
- Credentials such as passwords, password hints, and similar security information used for authentication
- Service usage information (metrics/logs)
- Host names and IP addresses
- File names and file paths
- Data about customer systems including, but not limited to, cluster, database, and cloud account names
- Interactions with Catalogic, if any, e.g., inquiries or complaints, support tickets
- For the purpose of removing any doubt, Catalogic may be required to process minimal personal data of Customer's staff in order to comply with its obligations under the Agreement, including without limitation, obligations regarding data privacy protection, technical support and the managing and use of the Cloud Services. In such limited instances only, Catalogic would be Controller, and possibly processor, of said personal data of Customer's staff, which may be further processed by sub-processors. Such data may include:
    - First and last name
    - CloudCasa login ID
    - Basic contact information (email, phone, fax, and postal address)
    - Company and/or employer
    - Title and/or position
    - Logs related to use of Cloud Services
    - Data types related to any technical support sought
- CloudCasa is designed for use by entities, institutions, and similarly situated legal organizations; however, it is theoretically possible that an individual natural person would choose to purchase Cloud Services. For the purposes of removing any doubt, when Catalogic acts as Controller in the unlikely instance in which a natural person purchases Cloud Services individually, the categories of personal data processed may include:

- First and last name
- CloudCasa login ID
- Basic contact information (email, phone, fax, and postal address)
- Billing related information

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Not Applicable. However, due to the nature of the Cloud Services, the exact types of personal data cannot be conclusively established and may vary depending on the exact use and configuration of the Cloud Services elected by Customer. No sensitive data is required in order to use the Cloud Services.

Nature of processing

Purpose(s) for which the personal data is processed on behalf of the controller

1. Providing data protection, backup/restore, disaster recovery, and data migration services as directed by the Customer;
2. Providing security-related infrastructure configuration scanning services as directed by the Customer;
3. Provisioning, configuration, and management of the Cloud Services;
4. Preventing, detecting, investigating, mitigating and repairing problems with the Cloud Services, including security incidents;
5. Preventing fraud;
6. Billing (CloudCasa is designed to service the needs of entities, institutions and similarly situated legal organizations; as such, processing of billing records typically does not require processing personal data of natural persons. For the purpose of removing any doubt, it is theoretically possible an individual could choose to use Cloud Services, in which case the minimum data necessary would be processed to effectuate billing for the Cloud Services.)

Duration of the processing

Duration of the processing shall be as defined by the controller in the License Contract or other proper and binding documentation.

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing:

The sub-processors will process data according to the Controller's instructions as communicated to the processor and as set forth in this Data Processing Agreement. As such, the nature and duration of the processing shall be the same for each category or type of data as that specified for processor, above.

The list of agreed upon processors, pursuant to the general authorization in Clause 7.7(a) is attached to each unique combined Data Processing Supplement as Exhibit A and is otherwise available at: https://cloudcasa.io/legal.

ANNEX III

Technical and organizational measures including technical and organizational measures to ensure the security of data

EXPLANATORY NOTE: The technical and organisational measures need to be described concretely and not in a generic manner.

Description of the technical and organisational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons. Examples of possible measures:

With a high value placed on data privacy and security, Catalogic has implemented and maintains a security program incorporating a combination of industry standards and best practices.

Depending on the exact use and configuration of the Cloud Services selected by Customer, aspects of the Cloud Services may be provided by Microsoft Azure, which has certain inherently associated technical and organizational measures. For Technical and Organizational Measures applicable to Microsoft Azure (sub-processor) please refer to the applicable terms and documentation in particular available here: https://www.microsoft.com/en-us/trust-center/privacy.

Measures of pseudonymisation and encryption of personal data

Catalogic has implemented suitable measures to prevent Personal Data from being read, copied, altered, or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished through:

- Use of adequate encryption and firewall technologies to protect the data as it travels through the network
- Sensitive Personal Data is encrypted during transmission using up-to-date versions of TLS or other security protocols using strong encryption algorithms and keys

- Protecting web-based access to management interfaces by employees using encryption (TLS) and access control

- Use of end-to-end encryption for any screen sharing for remote access, support, or real time communication

- Use of integrity checks to monitor the completeness and correctness of the transfer of data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Catalogic has implemented suitable measures to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services. This is accomplished by:

- Utilizing firewall, router, and VPN-based access controls to protect the private service networks and back-end-servers
- Continuously monitoring infrastructure security
- Regularly examining security risks
- Using role-based access control implemented in a manner consistent with the principle of least privilege
- Remote access to Catalogic's network infrastructure and cloud systems is secured using two-factor authentication tokens or multi-factor authentication
- Access to host servers, applications, databases, routers, switches, etc., is logged
- Access and account management requests must be submitted through internal approval systems
- Access must be approved by an appropriate approving authority
- Passwords must adhere to the Catalogic password policy, which includes minimum length requirements, enforced complexity, and set periodic resets
- Catalogic's intrusion detection systems include both network and host-based IDS
- Catalogic also uses commercial and custom tools to collect and examine its system and application logs for anomalies
- The Cloud Services are developed leveraging an architecture that ensures confidentiality, integrity, availability, and resilience

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

- Having implemented a business continuity and disaster recovery plan
- Utilizing redundant infrastructure that is implemented with high availability and disaster recovery in mind
- Situating data centers in secure co-location facilities that are ISP carrier neutral and provide physical security, redundant power, and infrastructure redundancy
- Utilizing cloud infrastructure with availability zone and region diversity
- Obtaining suitable service level agreements from CSPs/ISPs to ensure high levels of uptime
- Our service provider infrastructure is designed with rapid failover capability

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Persons entitled to use the systems are only able to access data within the scope and to the extent covered by their respective access permission (authorization). This is accomplished by:

- Employee policies and training
- Users have unique log in credentials
- Role based access control systems are used to restrict access to particular functions
- Activities on production systems are logged and monitored
- Access is controlled in compliance with the security principle of least privilege
- Internal segmentation and logical isolation of Catalogic's employees to enforce least privilege access policies
- Regular review of accounts and privileges (typically every 12 months depending on the particular system and sensitivity of data it provides access to)

Measures for ensuring physical security of locations at which personal data are processed

Web applications, communications, and database servers of Catalogic are located in secure data centers. Catalogic has implemented suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment. This is accomplished by:

- Establishing security areas
- Securing the data processing equipment and personal computers
- Establishing access authorizations for employees and third parties
- Restricting physical access to the servers by using electronically-locked doors and separate cages within facilities
- Data centers are protected by security alarm systems, and other appropriate security measures, such as user-related authentication procedures, including biometric authentication in some instances, and/or electronic access cards

Measures for ensuring accountability

Catalogic has implemented suitable measures to monitor, in accordance with applicable privacy laws, access restrictions of Catalogic's system administrators and to ensure that they act in accordance with instructions received. This is accomplished through:

- Individual appointment of system administrators;
- Maintaining records of system administrator's identification, access, and responsibilities
- Adoption of suitable measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for a reasonable period of time
- Audits of system administrators' activity

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller

Copies or summaries of Data Processing Agreements and, where applicable, Data Transfer Agreements, with sub-processors will be made available upon request.

Description of the specific technical and organizational measures to be taken by the processor to be able to provide assistance to the controller

CloudCasa's Shared Responsibility Model document highlights the technical aspects of Cloud Services that help the Customer/Controller fulfill its obligations.