APPOINTMENT AS DATA PROCESSOR
- Data Processing Agreement -
(Art. 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016)

WHEREAS

a. A contract is in place between the CUSTOMER and the SUPPLIER indicated in the contract to which this document refers (hereinafter SUPPLIER) for the provision of IT services and/or services connected with them (hereinafter SERVICE and/or SERVICES), of which this document forms an integral part;

b. in this contract the parties agree to define
- as "GDPR" 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
- as "Privacy Legislation" the provisions of the GDPR as well as all the other provisions of Union law or of Member State law relating to the protection of personal data and to their free movement.

c. in the performance of the SERVICE, the Controller of the personal data, pursuant to and for the purposes of Article 4(1), point 7, of the GDPR, is the CUSTOMER, which is responsible for carrying out all the acts required by the Privacy Legislation for the processing of personal data, that is to say the privacy notice, the collection of consent and the adoption of all authorisation, appointment, retention and other measures, also in order to set up the security system, including the related measures;

In view of the above, between the Parties,

IT IS AGREED AND STIPULATED

as set out below.

1. Appointment as Data Processor

1.1 For the tasks that, on the basis of the contract for the SERVICE, are entrusted to the SUPPLIER, the latter is appointed as Processor pursuant to Article 4(1), point 8), and Article 28 GDPR.

1.2 The Processor states that it is able to provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing meets the requirements of the GDPR and ensures the protection of the rights of data subjects.

2. Subject matter of the DPA

2.1 The purpose of this appointment is to define the contractual terms and conditions under which the Processor undertakes to carry out, on behalf of the Controller, the personal data processing operations as defined in the contract and specified in the technical annex "Service Processing Record", made available at the request of the Controller.

2.2 Within the framework of their contractual relations, the parties undertake to comply with the regulations in force applicable to the processing of personal data and, in particular, the GDPR and the Privacy Legislation.

3. Term of the DPA

This appointment shall have the same term as the contract to which it refers.

4. Description of the services of the Processor

4.1 The Processor is authorised to process, on behalf of the Controller, the personal data necessary to provide the SERVICE as provided for in the contract. For the data that the Controller has already provided and will provide, the Controller warrants that it has a suitable legal basis pursuant to Article 6 GDPR, such as the contract with the guest, the legal obligations relating to public security, statistics and tax and, where necessary, consent.

The Controller warrants to the Processor that it lawfully holds all the information that it will entrust to the Processor for processing, and also gives assurance that such information does not in any way infringe the rights of third parties.

The Controller retains ownership of the information that will be communicated to the Processor for the SERVICE and expressly assumes the fullest responsibility for the content of the related personal data and indemnifies and holds the Processor harmless from any obligation and/or burden of direct and indirect verification and/or control in this regard.

4.2 The nature of the operations carried out on the data is the provision of the SERVICE and/or SERVICES indicated in the contract, for which the Controller declares that it entrusts the related data processing to the Processor.

4.3 The purpose of the processing, the nature and type of the data processed and the categories of data subjects are those specified in the "Service Processing Record".

4.4 Within its area of responsibility, the Processor, when processing the data for the provision of the SERVICE, shall carry out the processing in compliance with Article 5 GDPR on the "Principles relating to processing of personal data".

4.5 For the performance of the assignment covered by this contract, the Controller makes available to the Processor the information necessary to carry out the activities for the SERVICE, including information aimed at the appropriate use of the information system.

4.6 Pursuant to Article 28(3)(b) GDPR, the Processor identifies and appoints in writing its own authorised persons, precisely defining the permitted scope of processing. The Processor declares that it is aware that its authorised persons act under its authority.

5. Obligations of the Processor

In the performance of its functions, the Processor undertakes to fulfil and observe the following obligations.

5.1 <u>Compliance with the instructions given by the Controller</u>

a. The Processor shall process the data only for the purposes specified above and for the performance of the contractual services.

b. The Processor shall process the data in accordance with the provisions of the "Service Processing Record", and the Controller considers the security measures provided for therein to be adequate.

5.2 <u>Ensuring confidentiality</u>

a. The Processor guarantees that the confidentiality of the personal data processed under this appointment is observed.

b. The Processor guarantees that the persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and that they receive and are given the necessary training on the processing of personal data.

5.3 <u>Adoption of the security measures for the processing</u>

a. The Processor must process the personal data with the measures required pursuant to Article 32 GDPR in place. The security measures adopted are those declared in the "Service Processing Record". The Controller acknowledges that in some cases the Processor will carry out the processing through the tools set up and configured by the Controller itself and, therefore, will have to take every necessary precaution only where the processing is carried out outside the control of the tool set up and configured by the Controller.

b. If the Processor has adhered to a code of conduct, or has presented a certification, it must operate applying the security measures provided for by the code of conduct or by the protocols referred to in the certification. In this case the Controller shall

accept the certification as proof that the Processor has adopted adequate measures in relation to the processing carried out, thereby waiving the carrying out of audit activities on the systems and procedures of the SUPPLIER.

c. In the cases covered by Article 37 of the GDPR, the Processor operates with the assistance of its own Data Protection Officer (RPD or DPO): if one has been designated, the contact details are indicated in the "Service Processing Record".

d. In accordance with Article 30 GDPR, the Processor (and, where applicable, its representative, unless it falls within the cases of exemption referred to in paragraph 5 of that Article) must maintain a record of all categories of processing activities carried out on behalf of the Controller, containing the information indicated in paragraph 2 of that Article.

e. The records referred to are kept in writing, including in electronic form, and shall be made available to the Controller at its request.

5.4 Appointment of Sub-processors

a. Pursuant to Article 28(2) GDPR, by this appointment the Controller gives the Processor express general written authorisation to identify other parties that perform, on behalf of the Processor, the role of Sub-processors. In return for this authorisation, the Processor undertakes to communicate to the Controller the list of all the parties, if any, identified as Sub-processors. If, over time, there are changes, additions or replacements of the Sub-processors initially communicated, such new appointments must be communicated to the Controller, which shall have 15 days from receipt of the communication to raise any objections, stating the reasons supporting its objection. Where it is not possible to reach an agreed solution, the Customer/Controller may withdraw from the contract relating to the Service used, under the terms provided for therein. The Processor represents and warrants that the Sub-processors provide sufficient guarantees to implement technical and organisational measures suitable for ensuring compliance with the provisions of the Privacy Legislation in force and undertakes to bind the further processors by contract to comply with the same personal data protection obligations assumed by the Processor towards the CUSTOMER.

b. Where the Sub-processor fails to fulfil its data protection obligations, the Processor remains fully liable to the Controller for the performance of the Sub-processor's obligations.

c. It is specified that, in all cases in which the SERVICE is not provided directly to the CUSTOMER but to the CUSTOMER's end customers, the SUPPLIER acts as a further Processor and shall be required to process the data under the same conditions laid down in this deed of appointment for the Processor.

5.5 Assistance to the Controller for the exercise of data subjects' rights

a. As far as possible, the Processor – taking into account the nature of the processing – must assist the Controller in order to enable it to respond to requests for the exercise of the data subject's rights laid down in Chapter III GDPR.
The Processor shall, insofar as this is possible, assist the Controller by appropriate technical and organisational measures.

b. With regard to the data subjects' right to information, it is for the Controller to provide the information referred to in Articles 13 and 14 GDPR to the data subjects for the processing operations, at the time the data are collected.
Where it directly receives requests from a data subject concerning the processing of personal data carried out on behalf of the CUSTOMER, the Processor for that processing invites the data subject to contact the CUSTOMER, as Controller, and promptly notifies the CUSTOMER of the request received from the data subject, within 10 working days of receiving it.

5.6 Assistance to the Controller in ensuring compliance with the obligations under Articles 32 to 36 of the GDPR

a. Taking into account the nature of the processing and the information available to it, the Processor must assist the Controller in ensuring compliance with the obligations under Articles 32 to 36 of the GDPR, namely:
- Article 32. Security of processing;
- Article 33. Notification of a personal data breach to the supervisory authority;
- Article 34. Communication of a personal data breach to the data subject;
- Article 35. Data protection impact assessment;
- Article 36. Prior consultation.

b. Assistance for the Security of processing – The Processor is obliged to assist the Controller in implementing the security of processing, in accordance with Article 32 GDPR.
At the request of the Controller, the Processor shall report on the security measures adopted, including by means of any questionnaires and checklists, subject, if necessary, to an assessment at project level.

c. Particular security measures of the Processor already in place – The Controller acknowledges that, for the SERVICE, the Processor has adequate security measures in place in compliance with the GDPR.
System Administrators. In relation to the activities carried out by the Processor concerning the storage of personal data and the system activities aimed at maintaining the network and updating the related databases and operating systems, the Processor's operators shall have the function of System Administrators.
The requirements laid down by the Garante per la privacy (Italian Data Protection Authority) in its decision of 27 November 2008 shall be managed by the Processor; in particular, it shall be the Processor that assesses the subjective characteristics of the system administrators, makes the individual designations, checks the activities they carry out and arranges for the logging of their accesses. In relation to the provisions of that decision, the Processor undertakes to communicate to the Controller the updated list of System Administrators; such data may be communicated in electronic or paper form, and the Controller considers this requirement to be fulfilled also by simply making the updated list of the names of those System Administrators available at the request of the Controller.

5.7 Assistance with the obligation of Notification of a personal data breach to the supervisory authority
The Processor is obliged to assist the Controller in fulfilling its obligations to notify a personal data breach to the supervisory authority, in accordance with Article 33 GDPR. The Processor notifies the Controller of any personal data breach within a maximum of 48 hours after becoming aware of it. This notification is accompanied by the information expressly indicated in paragraph 3 of Article 33, which is useful to enable the Controller, if necessary, to notify this breach to the competent supervisory authority.
It is, in fact, the sole responsibility of the Customer, where it is the Controller, to determine whether the incident can be classified as a Data Breach and whether the risk to data subjects is such as to require notification to the Supervisory Authority and communication to the data subjects concerned pursuant to the aforementioned Articles 33 and 34 of the Regulation.
The Processor ensures that the obligations of this Article are also complied with by the Sub-processors it uses for the purposes of providing the SERVICE to the CUSTOMER/Controller, binding them to report any security incidents to the Processor promptly and without undue delay, as soon as they become aware of them, in the manner and within the time limits laid down in the respective agreements.

5.8 Assistance with the obligation to communicate a personal data breach to the data subject
The Processor is obliged to assist the Controller in fulfilling the obligations to communicate a personal data breach to the data subject, in accordance with Article 34 GDPR; such communication must in any case always be made by the Controller.

5.9 Assistance by the Processor in the fulfilment of the Controller's obligation to carry out the data protection impact assessment
The Processor shall assist the Controller in fulfilling the obligations relating to risk analysis and data protection impact assessment, in accordance with Article 35 GDPR, by providing all useful information in its possession through the "Service Processing Record".

5.10 Assistance by the Processor in the fulfilment of the Controller's obligation of prior consultation
The Processor assists the Controller in the prior consultation of the supervisory authority provided for in Article 36 of the GDPR, by providing the Controller with all useful information in its possession through the "Service Processing Record".

5.11 Assistance by the Processor in the event of inspections/requests by the competent authority.
The Processor assists and cooperates with the Controller in the event of inspections/requests by a public authority that may in any way concern it.
In the event of inspections at the Processor's premises that concern the Controller, the Controller shall be informed immediately, where this is possible in view of the circumstances of the judicial investigation being conducted.

5.12 Data retention periods: deletion or return of all personal data at the end of the assignment
After the end of the provision of services relating to processing, the Processor shall, at the choice of the Controller, return or delete all the personal data and delete existing copies.
The data held by the Processor shall be returned to the Controller, at its request, by means of the export functions of the platform, in commonly used structured formats, before the end of the contract; and/or deleted within the time limits defined in the "Service Processing Record".
Any further backup copies of the data may be kept, for the additional period indicated in the "Service Processing Record", exclusively for security purposes and not intended for communication or dissemination.
By way of derogation from the preceding points, the Processor shall retain the data in cases where Union or Member State law requires their retention, for the periods imposed by such legislation or by such measures.

5.13 Making available to the Controller all the information necessary to demonstrate compliance with the obligations
The Processor shall make available to the Controller all the information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and must allow for and contribute to audits, including inspections, conducted by the Controller or by another party mandated by the Controller – under the terms and in the manner more fully defined in Article 8 below – or by the authorities.

5.14 Case in which an instruction to the Processor is considered to infringe the GDPR
If, in its opinion, the Processor considers that an instruction of the Controller infringes the GDPR or other national or Union data protection provisions, it shall immediately inform the Controller.

5.15 Compliance with the principles of "privacy by design" and "privacy by default"
In performing the assignment, the Processor shall operate in compliance with the principles of data protection from the design stage (privacy by design) and of data protection by default. The SERVICES are provided in a standard form, the same for all customers, and are designed according to these principles.

6. Obligations of the Controller

6.1 The Controller must:

- provide the Processor with the data referred to in Article 4 of these clauses;
- document in writing all instructions concerning the processing of the data by the Processor;
- oversee, in advance and throughout the duration of the processing, the Processor's compliance with the obligations laid down in the European data protection regulation;
- supervise the processing, carrying out audits and inspections.

7. Places where the data are and will be kept

7.1 The data shall be processed by the Processor in the places indicated in the "Service Processing Record". Should the processing be carried out in non-EU countries, the Processor shall make available to the Controller the safeguards adopted according to the place where the processing will be carried out.

7.2 If the Processor is required to transfer the data to a third country or an international organisation under Union law or the law of the Member State to which it is subject, it must inform the Controller of that legal requirement before the transfer in order to obtain authorisation, unless the law prohibits such information on important grounds of public interest.

8. Checks

8.1 The Controller reserves the right, including through periodic checks, to monitor strict compliance with the legal provisions on the processing of the data and compliance with its own instructions set out in this document. The Processor shall allow the Controller, giving it full cooperation, to carry out periodic checks on the adequacy of the security measures adopted and on compliance with the Privacy Legislation and with the instructions of the Controller itself.

8.2 Any audit activity by the Controller must be agreed with the Processor, with at least 10 working days' notice. Where such activities entail charges and expenses not provided for in this contract, all requests of the Controller must be agreed as regards the manner of their execution and managed at project level, with the definition of an assessment, including of the costs, for their implementation (whether they are penetration tests, vulnerability assessments or other activities).

8.3 All information shared in fulfilment of the obligations of the Processor or of the Controller is classified as confidential and therefore may not be disseminated, communicated or published online without the prior written authorisation of the other party. Each authorised person who processes the information shall have signed a confidentiality agreement that prohibits communication to unauthorised parties even after the end of the employment relationship and until the information becomes public knowledge for reasons not attributable to them. Any breach of the confidentiality of such information shall be punished under the terms of the law and of the contract.

Octorate S.r.l.
Via Filippo Caruso 23, 00173 Roma · C.F. e P. IVA 13493861002 · octorate.com

Courtesy translation of the Italian original. In the event of any differences, the Italian text prevails.

Author	Privacy Office, Zucchetti Spa
Approval	Fabrizio Scuppa, legal representative of Octorate S.r.l.

Version Revision

Version	Author	DPO consultation	Date of issue	Reason for revision
0	Privacy Office		12/11/2026	First issue

OCTORATE

PROCESSOR					
Company name	Octorate Srl				
VAT number	13493861002				
Address	Via Filippo Caruso 23				
City	Roma	**Post code**	00173	**Prov.**	RM
Legal Representative	Fabrizio Scuppa				

PERSONS AUTHORISED TO PROCESS THE DATA
Octorate staff responsible for customer support, onboarding and training, developers and system engineers, authorised and instructed to carry out the processing, with access limited to their duties. For OctoAgent, the development team (4 people) and the support team (3 people) of iManager S.r.l., a Sub-processor indicated among the recipients.

CONTACT DETAILS			
Processor	Octorate Srl	legal@octorate.com	06 4542 0568
Representative of the processor	N/A		
Data Protection Officer (DPO)	Octorate's DPO	dpo@octorate.com	

DESCRIPTION
System for managing bookings, rates and availability, distribution on the connected channels, website and booking engine, communications with guests, compliance obligations towards the Polizia di Stato (Italian State Police), ISTAT (Italian National Institute of Statistics) and the Agenzia delle Entrate (Italian Revenue Agency), payment integrations, day-to-day operations of the property and, where active, automated management of conversations with OctoAgent.

PURPOSE OF THE PROCESSING
Provision of the Octorate Services on behalf of the Customer, that is to say management of bookings, rates

and availability, distribution on the connected channels, website and booking engine, communications with guests, compliance obligations towards the Polizia di Stato, ISTAT and the Agenzia delle Entrate, payment integrations, day-to-day operations of the property and, where active, automated management of conversations with OctoAgent, with the support and maintenance of the Services.
Nature of the processing. Collection, recording, organisation, structuring, storage, consultation, processing, retrieval, disclosure by transmission to the recipients indicated by the Customer, deletion. For OctoAgent, also automated processing by means of artificial intelligence models to generate replies, translations, summaries, transcripts, classifications and alerts.
Duration and frequency. For the entire duration of the contractual relationship, on a continuous basis. The retention periods by category are indicated in the time limits for data deletion.

CATEGORY OF DATA SUBJECTS

Guests and persons making bookings, including accompanying persons and guests who are minors within the limits of legal requirements. Persons who contact the property for information or quotes. Users of the Customer's account, that is to say owner, staff and collaborators. Owners of the units managed, for property managers who use the owners' portal. Suppliers and partners of the Customer that may be registered on the platform.

CATEGORIES OF PERSONAL DATA

Booking and stay data. First name and surname, contact details, language, nationality, arrival and departure dates, unit and type, number and composition of guests, amounts, source channel, preferences and notes entered by the Customer or by the guest.
Data for legal requirements. For the Alloggiati guest registration forms, personal details, place and date of birth, citizenship, type, number and place of issue of the identity document. For ISTAT, statistical data on flows. For tax documents, guests' tax data, tax code and VAT number.
Payment data. Credit card details acquired as a guarantee for the booking, stored in encrypted form in accordance with the PCI-DSS standards and not directly decryptable by Octorate, transaction outcomes communicated by the gateways and payment institutions.
Communications. Content and attachments of the messages exchanged with guests by email, OTA portal messaging, WhatsApp, text message and website chat. With OctoAgent, also the images sent by guests, the summaries, transcripts and audio recordings of calls when the voice module is active, the agent's reasoning lines and the lessons approved by the Customer.
Online check-in with OctoAgent. Image of the identity document sent by the guest for check-in, from which OctoAgent extracts the personal details. The photograph on the document is obscured before it is sent to the artificial intelligence model.
Website and booking engine. Data of visitors and of persons making bookings on the Customer's website and booking engine, in accordance with the Customer's privacy notice and cookie policy.
Account users. Name, email, role, credentials, access and activity logs, necessary for the operation and

security of the platform.
Special categories of data. Not envisaged by the Services. Information communicated spontaneously by guests, for example health, dietary or religious needs, is processed under the responsibility of the Customer.

NO USE FOR OWN PURPOSES

Octorate does not use the Customer Data for its own purposes. Octorate may process data in aggregated and anonymous form, which do not allow either the Customer or the data subjects to be identified, for statistical and security purposes and to improve the Services.

CATEGORY OF RECIPIENTS TO WHOM THE DATA MAY BE DISCLOSED

List of the Sub-processors authorised by the Customer under a general authorisation, with the country and the data transfer safeguards of each provider. OTA portals, public bodies, gateways and payment institutions are not Sub-processors and receive the data as indicated under the parties that receive the data as independent controllers.

- Aruba S.p.A. (Italy). Hosting, database, storage and backup of the Octorate platform (PMS, Channel Manager, Booking Engine). Transfer safeguard intra-EEA.
- Complior AB (formerly 24 Solutions) (Sweden). PCI DSS certified environment connected to the platform for credit card data. Transfer safeguard intra-EEA.
- iManager S.r.l., Via del Muro Linari 31, 00173 Roma, tax code and VAT no. 16082961000 (Italy). Development, management and application hosting of the OctoAgent platform. Transfer safeguard intra-EEA.
- Google Cloud (Google Cloud EMEA Limited) (Ireland, Milan data centre). Hosting of OctoAgent. Transfer safeguard intra-EEA, standard contractual clauses for any access from third countries.
- MongoDB Atlas (MongoDB Limited) (Ireland, Milan and Frankfurt data centres). OctoAgent database and backups. Transfer safeguard intra-EEA, standard contractual clauses for any access from third countries.
- OpenAI (OpenAI Ireland Limited, contracting entity for the EEA) (Ireland, processing also in the United States). Artificial intelligence models of OctoAgent, generation of replies, summaries, transcripts, extraction of data from documents, through iManager's account. Artificial intelligence models of the other functions of the Octorate platform, through Octorate's account. Transfer safeguard Standard contractual clauses included in the DPA of OpenAI, which does not hold DPF certification.
- Openapi S.r.l. (Openapi.com) (Italy). Sending of text messages to guests by OctoAgent. Transfer safeguard intra-EEA.
- Better Stack (EU). Availability monitoring and alarms for OctoAgent, EU data region, only if personal data pass through the logs. Transfer safeguard intra-EEA.
- Microsoft Clarity (Microsoft) (Ireland, USA). Analysis of the use of the OctoAgent console by the properties' users, with masking enabled. Transfer safeguard Adequacy (DPF) or standard contractual clauses.
- Meta (WhatsApp Business Platform) (Ireland, USA). WhatsApp messaging between properties and guests. Transfer safeguard Adequacy (DPF) or standard contractual clauses.
- Mailchimp Transactional (Mandrill, The Rocket Science Group LLC) and SparkPost (Bird) (USA, EU).

Email sending services authorised for the octorate.com domain, for emails that are not sent from Octorate's mail servers. OctoAgent does not use them. Transfer safeguard Adequacy (DPF) or standard contractual clauses.

- Mailgun (Mailgun Technologies, Inc., Sinch group) (USA, EU). Sending service for the emails of the Services. Transfer safeguard Standard contractual clauses.
- Intercom (Intercom R&D Unlimited Company) (Ireland, USA). Support chat of the Octorate platform, only if guests' data pass through it. OctoAgent does not use it. Transfer safeguard Adequacy (DPF).

The telephone service of the OctoAgent voice module is provided by Vonage under a contract in the Customer's name, activated as indicated by Octorate, and therefore Vonage is not a Sub-processor of Octorate. Changes to this list are notified to the Customer. The updated version is available on request from legal@octorate.com.

TRANSFER OF DATA ABROAD

The Customer Data are stored in data centres located in the European Union, indicated in the security measures relating to the data centre.

Octorate transfers Customer Data to third countries, including through Sub-processors, only in compliance with Chapter V of the GDPR, on the basis of an adequacy decision of the European Commission, including the EU-US Data Privacy Framework for certified providers, or of the standard contractual clauses adopted by Commission Implementing Decision (EU) 2021/914, supplemented by any additional measures that may be necessary. The safeguards applied to each Sub-processor are indicated in the list of recipients. For the artificial intelligence models of OctoAgent and of the other functions of the platform, the data necessary to generate the content are transmitted to OpenAI, which also processes them in the United States on the basis of the standard contractual clauses included in its data processing agreement.

Transmissions to OTA portals, payment gateways, third-party software connected by the Customer via API, guests and other recipients indicated by the Customer, including those located in third countries, take place on the instructions of the Customer, which is responsible for them.

TIME LIMITS FOR DATA DELETION

Booking and stay data and guest profiles. For the entire duration of the contract and up to 30 days after the end of the contract, unless otherwise instructed by the Customer.

Messages and conversations with guests. For the entire duration of the contract, unless deleted earlier on the Customer's instructions.

Transcripts, summaries and recordings of calls, lessons and reasoning lines of OctoAgent. For the entire duration of the contract, unless deleted earlier on the Customer's instructions.

Data sent to the artificial intelligence models (OpenAI). Not stored by the provider for subsequent uses. OpenAI retains them for up to 30 days for abuse monitoring and then deletes them.

Data for Alloggiati guest registration forms, ISTAT and tax documents. For the time necessary for transmission and for the retention obligations laid down by law.

Technical and security logs. For the Octorate platform, HTTP request logs 45 days and system administrator access logs at least 6 months, subject to legal obligations. For OctoAgent, application logs 90 days and audit logs 400 days. Guests' content, that is to say messages, email, telephone and documents, is not recorded in the OctoAgent logs. The technical request logs, kept for 400 days for security, contain the IP address of the person connecting. Only the iManager development team has access to the logs.
Backups. Automatic overwriting according to the cycles indicated below. For OctoAgent, daily backups kept for 7 days, weekly backups for 4 weeks and a daily copy in Frankfurt kept for 90 days. For the Octorate platform, daily backups kept for 30 days.
Before the end of the contract, the Customer may export the Customer Data by means of the export functions of the platform, in commonly used structured formats. On written request received before the end of the contract, Octorate provides assistance for the return of data that cannot be exported independently, for any fees that may be agreed.
Within 30 days of the end of the contract, Octorate deletes the Customer Data and existing copies, except for backups, which are overwritten on a rotating basis as indicated above, and except for the data that Octorate must retain to comply with legal obligations, including tax documents and the logs required by legislation, which are retained for the prescribed period and then deleted. Deletion requests received during the relationship are carried out within 5 working days, as provided for in the Terms and Conditions. On request, Octorate certifies in writing that the deletion has taken place.

PARTIES THAT RECEIVE THE DATA AS INDEPENDENT CONTROLLERS

OTA portals, gateways and payment institutions, the Polizia di Stato, ISTAT, the Agenzia delle Entrate and the other parties to which the Services transmit data on the Customer's instructions process the data as independent controllers or in accordance with their respective agreements with the Customer. Octorate limits itself to the technical transmission and is not liable for the processing carried out by such parties. The same applies to Vonage, which provides the telephone service of the OctoAgent voice module under a contract in the Customer's name.

RECORD OF PROCESSING ACTIVITIES

Octorate maintains the record of the categories of processing activities carried out on behalf of customers pursuant to Article 30(2) of the GDPR and makes it available to the Customer on request to legal@octorate.com.

GENERAL DESCRIPTION OF THE TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

1. SECURITY MEASURES IMPLEMENTED IN THE SOFTWARE

Security measures adopted in the Octorate platform and in OctoAgent.

- *Management of access credentials*

• Personal credentials for each user, password strength rules, blocking of unauthorised access and logging of accesses.
• Two-factor authentication with OTP code for the Octorate platform and for access to OctoAgent with Octorate credentials.
• OctoAgent also provides internal access for the property's operational staff who do not have an Octorate user account, for example those who answer the telephone, maintenance and cleaning staff, without two-factor authentication and not intended for users with administrator powers. The extension of two-factor authentication to internal users is being assessed with the provider.

- *Minimisation*

• Roles and permissions configurable by the Customer, to limit access to the data to the duties of each user.
- Identification of those who have access to the system
• Technical logs that make it possible to reconstruct the activities carried out on the platform. For OctoAgent, application logs kept for 90 days, audit logs and technical request logs kept for 400 days, without guests' content. The technical logs contain the IP address of the person connecting and are accessible only to the iManager development team. For the Octorate platform, HTTP request logs kept for 45 days. System administrator accesses are recorded in a non-modifiable manner and the related logs are kept for at least 6 months, as required by the decision of the Garante (Italian Data Protection Authority) on system administrators.
• Access by support staff to the Customer's account in accordance with the measures for support services indicated below.

- *Encryption techniques*

• Data transmission with the TLS protocol on all the Services.
• Credit card data stored in encrypted form in accordance with the PCI DSS standard, not directly decryptable by Octorate.
• Encryption of data at rest in the databases of the Octorate platform and of OctoAgent.

- *Privacy by default*

• Services provided in a standard form, the same for all customers, and designed according to the principles of data protection by design and by default. Logical separation of the data of the different customers on the platform.

- Rights of data subjects

• The Customer may export the data from the platform in commonly used structured formats. Octorate assists the Customer in responding to data subjects' requests. Deletion requests received during the relationship are carried out within 5 working days.

2. PROCESSOR: SECURITY MEASURES IMPLEMENTED FOR SUPPORT SERVICES

Octorate provides support to Customers remotely, through the platform chat, email and telephone, with staff authorised and instructed to carry out the processing. Requests received by chat and email are tracked as tickets in Intercom, indicated among the recipients. When this is needed to resolve the request, support staff access the Customer's account from Octorate's internal panel, with personal credentials and without using the Customer's password. Octorate does not connect to the Customer's devices with remote control software.
Support staff process the Customer's data only to resolve the request. Files and exports for support purposes are received from the Customer as attachments in the platform chat and are used only for that request. They remain attached to the conversation in Intercom for the duration of the contract. They are deleted within the time limits indicated in this Record for the Customer Data, that is to say within 30 days of the end of the contract, subject to the retention obligations laid down by law, or earlier at the Customer's request.

3. PROCESSOR: SECURITY MEASURES RELATING TO THE DATA CENTRE

Octorate platform. Infrastructure at Aruba S.p.A. in data centres in Italy certified ISO/IEC 27001, 27017, 27018 and ANSI/TIA-942 Rating 4. Daily database backups kept for 30 days, with restore procedures.
Credit cards. Credit card data in a PCI DSS certified environment at Complior AB, Sweden.
OctoAgent. Since 20 October 2026, hosting on Google Cloud in Milan with a MongoDB Atlas database in Milan and a copy of the backups in Frankfurt, in place of Scaleway in Paris, where the data were deleted after the migration. Providers with ISO/IEC 27001 and SOC 2 certifications. Daily backups kept for 7 days, weekly backups for 4 weeks and a daily copy in Frankfurt kept for 90 days.
System emails. The platform's system emails are sent from Octorate's mail servers hosted by Aruba or from the email sending services indicated among the recipients.

4. NIS2 BASELINE SECURITY MEASURES

Octorate is part of the Zucchetti Group, an essential entity under the NIS2 Legislation, and applies the baseline security measures defined by the ACN (Italian National Cybersecurity Agency) according to the Group's model. The items below set out, for each area provided for by the model, the measures adopted by Octorate for the Services.

Reliability of providers. Octorate processes the Customer Data only with the Sub-processors indicated among the recipients, bound by agreements compliant with Article 28 and chosen from providers with recognised security certifications (ISO/IEC 27001, SOC 2, PCI DSS). Each new provider is assessed before use and notified to the Customer. Octorate takes part in the Zucchetti Group's provider qualification process through the group contact person.

Roles and responsibilities. Data Protection Officer reachable at dpo@octorate.com. Internal contact persons for security and incidents indicated in the incident management procedure. For the NIS2 obligations, Octorate refers to the NIS point of contact and to the CSIRT contact person designated by the Zucchetti Group for the hospitality sector, with the related deputy, indicated in the incident management procedure.

Reliability of human resources. Staff authorised to carry out the processing, instructed on the applicable Legislation and bound by confidentiality, with access limited to their duties and revoked when the relationship ends.

Compliance and audits. Information and checks available to the Customer on request. Infrastructure at providers that are certified and subject to third-party audits, in particular Aruba S.p.A. (ISO/IEC 27001, 27017, 27018 and ANSI/TIA-942 Rating 4), Complior AB (PCI DSS), Google Cloud and MongoDB (ISO/IEC 27001 and SOC 2).

Vulnerability management. Security updates and patches applied as a priority. For OctoAgent, vulnerability scan and review of the configuration of the new infrastructure by 30 November 2026, first external penetration test by 31 March 2027 and then once a year, with management of the findings and of the fixes. For the Octorate platform, vulnerability tests and penetration tests as part of the Zucchetti Group's programme, in which Octorate is included through the group contact person.

Business continuity and disaster recovery. Backups of the Octorate platform made daily and kept for 30 days, with restore procedures. For OctoAgent, daily backups kept for 7 days, weekly backups for 4 weeks and a daily copy in Frankfurt kept for 90 days. Data centres certified ANSI/TIA-942 Rating 4 for the Octorate platform. Continuous monitoring of the availability of the Services.

Identity and access management. Personal credentials, least privilege with roles and permissions configured by the Customer, password strength rules, blocking of unauthorised access, logging of accesses and review of user accounts. Two-factor authentication with OTP code for the Octorate platform and for access to OctoAgent with Octorate credentials. Internal access to OctoAgent for the property's operational staff with the limits indicated in the security measures implemented in the software. Technical and administrative access to the OctoAgent infrastructure through the cloud provider's console with two-factor authentication, on a private network not exposed to the internet, with the database access server switched on only when necessary. Administrative accesses and changes logged and monitored.

Physical security. Data stored exclusively in the data centres of the providers indicated in this Record, with the physical access control provided for by the providers' certifications.

Training and awareness. Staff training on personal data protection and IT security, with content differentiated for general staff, technical staff and management according to the Zucchetti Group's

programme, in which Octorate is included through the group contact person.
Data security. Transmission with the TLS protocol, encryption of data at rest in the databases of the Octorate platform and of OctoAgent, credit card data in a PCI DSS certified environment, logical separation of customers' data, backups stored in the European Union, secure deletion at the end of the contract.
Protection of networks and communications. Perimeter protection of the hosting providers, serverless OctoAgent infrastructure on a private network not exposed to the internet, application firewall on OctoAgent with logging of blocks, official communication channels with the Customer (account email and in-platform notices) also used for communications about incidents.
Event monitoring. For OctoAgent, checks every minute on the availability of the service from outside, application errors, response times, errors towards Octorate and towards the model providers, memory and work queues, application firewall blocks and administrative accesses and changes, with alarms to the technical team. Application logs kept for 90 days, audit logs and technical request logs for 400 days, without guests' content. The technical logs contain the IP address of the person connecting and are accessible only to the iManager development team. For the Octorate platform, HTTP request logs kept for 45 days and system administrator access logs, non-modifiable, kept for at least 6 months.
Incident management and reporting. Written procedure for detecting, assessing, containing and communicating incidents. The provider that operates OctoAgent informs Octorate within 12 hours of detecting an incident affecting the data or the service, even with partial information, with an update and analysis within 48 hours and a final report within 20 days, so that the Group can meet the time limits of 72 hours and one month towards CSIRT Italia. Octorate notifies the Customer of the breach within 48 hours of becoming aware of it and, for significant incidents under the NIS2 Legislation, activates the Zucchetti Group contact person for reporting to CSIRT Italia, with an early warning within 24 hours and a notification within 72 hours.
Secure development. Development according to security-by-design practices, security updates and patches, separate development and production environments and controlled releases.
Routine and evolutionary maintenance. Updates and new features released through a change management process and communicated to the Customer in accordance with the section Evolution and modification of the services of the Terms and Conditions. For OctoAgent, infrastructure migration completed on 20 October 2026, with review of the configuration by 30 November 2026.
Decommissioning. Deletion of the Customer Data within 30 days of the end of the contract and within 5 working days on request, as indicated in the time limits for data deletion, with overwriting of backups on a rotating basis. Secure disposal of media by the infrastructure providers in accordance with their respective certifications.
Subcontracting and supply chain. List of the Sub-processors among the recipients, with contractual obligations equivalent to those of the appointment as data processor, including the applicable NIS2 baseline security measures, and with the possibility for the Customer to object to changes within 15 days of the communication.