**DESIGNAÇÃO COMO OPERADOR**
**- Data Processing Agreement -**
*(Art. 28 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016)*

**CONSIDERANDO QUE**

**a.** Entre o CLIENTE e o FORNECEDOR indicado no contrato ao qual o presente documento se refere (doravante FORNECEDOR) está em vigor um contrato de prestação de serviços de informática e/ou de serviços a eles relacionados (doravante SERVIÇO e/ou SERVIÇOS), do qual a presente designação é parte integrante;

**b.** no presente contrato, as partes concordam em designar
- pelo termo "GDPR" o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e
- pelo termo "Legislação de Proteção de Dados" as disposições do GDPR, bem como todas as demais disposições das leis da União ou das leis dos Estados-Membros relativas à proteção dos dados pessoais e à sua livre circulação.

**c.** na prestação do SERVIÇO, o Controlador dos dados pessoais, nos termos e para os efeitos do art. 4°, item 1, n° 7, do GDPR, é o CLIENTE, a quem incumbe a prática de todos os atos previstos na Legislação de Proteção de Dados para o tratamento dos dados pessoais, ou seja, a política de privacidade, a coleta do consentimento, a adoção de todas as medidas de autorização, de designação e de conservação e de outra natureza, inclusive para implementar o sistema de segurança, incluindo as respectivas medidas;

Isto posto, entre as Partes,

**FICA CONVENCIONADO E ESTIPULADO**

o disposto a seguir.

**1. Designação como Operador**

**1.1** Para as tarefas que, com base no contrato relativo ao SERVIÇO, são confiadas ao FORNECEDOR, este é designado Operador, nos termos do art. 4°, item 1, n° 8), e do art. 28 do GDPR.

**1.2** O Operador declara estar em condições de oferecer garantias suficientes de implementação de medidas técnicas e organizacionais adequadas, de modo que o tratamento atenda aos requisitos do GDPR e assegure a proteção dos direitos dos titulares dos dados.

**2. Objeto do DPA**

**2.1** A presente designação tem por objeto definir as formas e as condições contratuais segundo as quais o Operador se compromete a realizar, por conta do Controlador, as operações de tratamento dos dados pessoais, conforme definidos no contrato e especificadas no anexo técnico "Registro do tratamento do serviço", disponibilizado mediante solicitação do Controlador.

**2.2** No âmbito de suas relações contratuais, as partes se comprometem a respeitar a regulamentação em vigor aplicável ao tratamento de dados pessoais e, em particular, o GDPR e a Legislação de Proteção de Dados.

**3. Duração do DPA**

A presente designação terá a duração do contrato a que se refere.

**4. Descrição das atividades do Operador**

**4.1** O Operador está autorizado a tratar, por conta do Controlador, os dados pessoais necessários para prestar o SERVIÇO conforme previsto no contrato. Para os dados que o Controlador já forneceu e que vier a fornecer, este garante dispor de uma base legal adequada nos termos do art. 6° do GDPR, como o contrato com o hóspede, as obrigações legais em matéria de segurança pública, estatística e fiscal e, quando necessário, o consentimento.

O Controlador garante ao Operador que dispõe legitimamente de todas as informações que confiar ao Operador para tratamento, assegurando também que essas informações não violam de forma alguma direitos de terceiros.

O Controlador mantém a titularidade das informações que forem comunicadas ao Operador para o SERVIÇO, assume expressamente a mais ampla responsabilidade quanto ao conteúdo dos respectivos dados pessoais e isenta o Operador de qualquer obrigação e/ou ônus de verificação e/ou de controle, direto e indireto, a esse respeito.

**4.2** A natureza das operações realizadas sobre os dados é a prestação do SERVIÇO e/ou dos SERVIÇOS indicados no contrato, razão pela qual o Controlador declara confiar ao Operador o respectivo tratamento dos dados.

**4.3** A finalidade do tratamento, a natureza e o tipo dos dados tratados e as categorias de titulares dos dados são os especificados no "Registro do tratamento do serviço".

**4.4** No âmbito de sua competência, o Operador, ao tratar os dados para a prestação do SERVIÇO, realizará o tratamento em observância do art. 5° do GDPR, relativo aos "Princípios relativos ao tratamento de dados pessoais".

**4.5** Para a execução do encargo objeto do presente contrato, o Controlador disponibiliza ao Operador as informações necessárias à execução das atividades relativas ao SERVIÇO, inclusive as destinadas ao uso adequado do sistema de informação.

**4.6** O Operador, nos termos do art. 28, item 3, alínea b), do GDPR, identifica e designa por escrito as suas pessoas autorizadas, definindo com precisão o âmbito de tratamento permitido. O Operador declara estar ciente de que as suas pessoas autorizadas atuam sob a sua autoridade.

**5. Obrigações do Operador**

O Operador, no exercício de suas funções, se compromete a cumprir e observar as seguintes obrigações.

**5.1** <u>Observância das instruções dadas pelo Controlador</u>

a. O Operador deverá tratar os dados somente para as finalidades acima especificadas e para a execução das prestações contratuais.

b. O Operador deverá tratar os dados em conformidade com o previsto no "Registro do tratamento do serviço", e o Controlador considera adequadas as medidas de segurança nele previstas.

**5.2** <u>Garantir a confidencialidade</u>

a. O Operador garante a observância da confidencialidade dos dados pessoais tratados no âmbito da presente designação.

b. O Operador garante que as pessoas autorizadas a tratar os dados pessoais se comprometeram com a confidencialidade ou estão sujeitas a uma obrigação legal adequada de confidencialidade e que recebem o treinamento necessário em matéria de tratamento de dados pessoais.

**5.3** <u>Adoção das medidas de segurança do tratamento</u>

a. O Operador deve realizar o tratamento dos dados pessoais com as medidas exigidas nos termos do art. 32 do GDPR. As medidas de segurança adotadas são as declaradas no "Registro do tratamento do serviço". O Controlador toma ciência de que, em alguns casos, o Operador realizará o tratamento por meio das ferramentas preparadas e configuradas pelo próprio Controlador e, portanto, o Operador só deverá adotar todas as precauções necessárias quando o tratamento for realizado fora do controle da ferramenta definida e configurada pelo Controlador.

b. Se o Operador tiver aderido a um código de conduta ou apresentado uma certificação, deve operar com as medidas de segurança previstas no código de conduta ou nos protocolos da certificação. Nesse caso, o Controlador aceitará a certificação

como prova de que o Operador adotou medidas adequadas em relação ao tratamento realizado, renunciando à realização de atividades de auditoria nos sistemas e nos procedimentos do FORNECEDOR.

c. O Operador, nos casos previstos no art. 37 do GDPR, atua com o apoio do seu Encarregado de Proteção de Dados (DPO): se tiver sido designado, os respectivos dados de contato estão indicados no "Registro do tratamento do serviço".

d. Em conformidade com o art. 30 do GDPR, o Operador (e, quando aplicável, o seu representante, se não se enquadrar nos casos de isenção previstos no parágrafo 5 desse artigo) deve manter um registro de todas as categorias de atividades de tratamento realizadas por conta do Controlador, contendo o indicado no item 2 do referido artigo.

e. Os registros indicados são mantidos por escrito, inclusive em formato eletrônico, e serão disponibilizados ao Controlador mediante solicitação deste.

**5.4** Designação de Suboperadores

a. Nos termos do art. 28, item 2, do GDPR, com a presente designação, o Controlador concede ao Operador autorização expressa, por escrito e geral para a escolha de outros terceiros que desempenhem, por conta do próprio Operador, a função de Suboperadores. Em razão dessa autorização, o Operador se compromete a comunicar ao Controlador a lista de todos os eventuais terceiros escolhidos na qualidade de Suboperadores. Caso ocorram, ao longo do tempo, alterações, inclusões ou substituições dos Suboperadores inicialmente comunicados, essas novas designações deverão ser comunicadas ao Controlador, que terá 15 dias contados do recebimento da comunicação para apresentar eventuais oposições, expondo os motivos que as fundamentam. Caso não seja possível chegar a uma solução de comum acordo, o Cliente/Controlador poderá rescindir o contrato relativo ao Serviço utilizado, nos termos nele previstos. O Operador declara e garante que os Suboperadores apresentam garantias suficientes de implementação de medidas técnicas e organizacionais adequadas para garantir o cumprimento das disposições da Legislação de Proteção de Dados em vigor e se compromete a vincular contratualmente os suboperadores ao cumprimento das mesmas obrigações em matéria de proteção de dados pessoais assumidas pelo Operador perante o CLIENTE.

b. Caso o Suboperador deixe de cumprir as suas obrigações em matéria de proteção de dados, o Operador continua integralmente responsável, perante o Controlador, pelo cumprimento das obrigações do Suboperador.

c. Esclarece-se que, em todos os casos em que o SERVIÇO não for prestado diretamente ao CLIENTE, mas aos clientes finais deste, o FORNECEDOR atua como Suboperador e deverá tratar os dados nas mesmas condições estabelecidas no presente ato de designação para o Operador.

**5.5** Assistência ao Controlador para o exercício dos direitos dos titulares dos dados

a. Na medida do possível, o Operador – levando em conta a natureza do tratamento – deve prestar assistência ao Controlador para permitir que este atenda aos pedidos de exercício dos direitos do titular dos dados previstos no Capítulo III do GDPR.

O Operador, na medida em que isso for possível, prestará assistência ao Controlador por meio de medidas técnicas e organizacionais adequadas.

b. Quanto ao direito de informação dos titulares dos dados, cabe ao Controlador fornecer as informações previstas nos arts. 13 e 14 do GDPR aos titulares dos dados envolvidos nas operações de tratamento, no momento da coleta dos dados.

Caso receba diretamente pedidos de um titular dos dados relativos ao tratamento de dados pessoais realizado por conta do CLIENTE, o Operador desse tratamento orienta o titular dos dados a se dirigir ao CLIENTE, na qualidade de Controlador, e comunica prontamente a este último o pedido recebido do titular dos dados, no prazo de 10 dias úteis contados do seu recebimento.

**5.6** Assistência ao Controlador para garantir o cumprimento das obrigações previstas nos artigos 32 a 36 do GDPR

a. O Operador, levando em conta a natureza do tratamento e as informações à sua disposição, deve prestar assistência ao Controlador para garantir o cumprimento das obrigações previstas nos arts. 32 a 36 do GDPR, a saber:

- o artigo 32. Segurança do tratamento;
- o artigo 33. Notificação de uma violação de dados pessoais à autoridade de controle;
- o artigo 34. Comunicação de uma violação de dados pessoais ao titular dos dados;
- o artigo 35. Avaliação de impacto sobre a proteção de dados;
- o artigo 36. Consulta prévia.

b. Assistência para a Segurança do tratamento – O Operador tem a obrigação de prestar assistência ao Controlador na implementação da segurança do tratamento, em conformidade com o art. 32 do GDPR.

O Operador, mediante solicitação do Controlador, apresentará relatório sobre as medidas de segurança adotadas, inclusive por meio de eventuais questionários e listas de verificação, após avaliação prévia no nível de projeto, se necessária.

c. Medidas de segurança específicas do Operador já em vigor – O Controlador toma ciência de que, para o SERVIÇO, o Operador mantém medidas de segurança adequadas em observância do GDPR.

*Administradores de sistema*. Em relação às atividades realizadas pelo Operador referentes à conservação dos dados pessoais e às atividades de administração de sistemas destinadas à manutenção da rede e à atualização dos respectivos bancos de dados e sistemas operacionais, os profissionais do Operador terão a função de Administradores de sistema.

As obrigações previstas pelo Garante per la privacy (autoridade italiana de proteção de dados) na decisão de 27 de novembro de 2008 serão cumpridas pelo Operador; em particular, caberá ao Operador avaliar as características subjetivas dos administradores de sistema, realizar as designações individuais, verificar as atividades por eles realizadas e providenciar o registro dos respectivos acessos. Em relação ao previsto na referida decisão, o Operador se obriga a comunicar ao Controlador a lista atualizada dos Administradores de sistema; a comunicação desses dados poderá ser feita em formato eletrônico ou em papel, e o Controlador considera cumprida essa obrigação também com a simples disponibilização da lista atualizada dos nomes dos referidos Administradores de sistema, mediante solicitação do Controlador.

**5.7** Assistência relativa à obrigação de Notificação de uma violação de dados pessoais à autoridade de controle

O Operador tem a obrigação de prestar assistência ao Controlador no cumprimento das suas obrigações de notificação de uma violação de dados pessoais à autoridade de controle, em conformidade com o art. 33 do GDPR. O Operador notifica o Controlador de qualquer violação de dados pessoais no prazo máximo de 48 horas após ter tomado conhecimento dela. Essa notificação é acompanhada das informações expressamente indicadas no item 3 do art. 33, úteis para permitir que o Controlador, se necessário, notifique essa violação à autoridade de controle competente.

Com efeito, cabe exclusivamente ao Cliente, quando Controlador, determinar se o incidente pode ser classificado como Data Breach e se o risco para os titulares dos dados é tal que exija a notificação à Autoridade de controle e a comunicação aos titulares dos dados afetados, nos termos dos referidos artigos 33 e 34 do Regulamento.

O Operador assegura o cumprimento das obrigações do presente artigo também pelos Suboperadores que utiliza para a prestação do SERVIÇO ao CLIENTE/Controlador, obrigando-os a comunicar ao Operador, de forma tempestiva e sem demora injustificada, eventuais incidentes de segurança, assim que deles tiverem conhecimento, na forma e nos prazos previstos nos respectivos acordos.

**5.8** Assistência relativa à obrigação de comunicação de uma violação de dados pessoais ao titular dos dados

O Operador tem a obrigação de prestar assistência ao Controlador no cumprimento das obrigações de comunicação de uma violação de dados pessoais ao titular dos dados, em conformidade com o art. 34 do GDPR; essa comunicação deverá, em todo caso, ser sempre feita pelo Controlador.

**5.9** Assistência do Operador no cumprimento da obrigação do Controlador relativa à avaliação de impacto sobre a proteção de dados

O Operador prestará assistência ao Controlador no cumprimento das obrigações de análise de riscos e de avaliação de impacto sobre a proteção de dados, em conformidade com o art. 35 do GDPR, fornecendo todas as informações úteis em seu poder por meio do "Registro do tratamento do serviço".

**5.10** Assistência do Operador no cumprimento da obrigação do Controlador relativa à consulta prévia

O Operador presta assistência ao Controlador na consulta prévia à autoridade de controle, prevista no art. 36 do GDPR, fornecendo ao Controlador todas as informações úteis em seu poder por meio do "Registro do tratamento do serviço".

**5.11** Assistência do Operador em caso de inspeções/pedidos por parte da autoridade competente.

O Operador presta assistência ao Controlador e colabora com ele em caso de inspeções/pedidos por parte da autoridade pública que possam de algum modo lhe dizer respeito.

Em caso de inspeções junto ao Operador que digam respeito ao Controlador, o Controlador será imediatamente informado, sempre que isso for possível tendo em vista os pressupostos da investigação judicial realizada.

**5.12** Prazos de conservação dos dados: eliminação ou devolução de todos os dados pessoais ao término do encargo

Após o término da prestação dos serviços relacionados ao tratamento, o Operador, a critério do Controlador, deverá devolver ou eliminar todos os dados pessoais e eliminar as cópias existentes.

Os dados em poder do Operador deverão ser devolvidos ao Controlador, mediante solicitação deste, por meio das funções de exportação da plataforma, em formatos estruturados de uso comum, antes do encerramento; e/ou eliminados nos prazos definidos no "Registro do tratamento do serviço".

Eventuais cópias adicionais de backup dos mesmos dados poderão ser conservadas, pelo período adicional indicado no "Registro do tratamento do serviço", para fins exclusivamente de segurança e não de comunicação ou difusão.

Em derrogação ao indicado nos itens anteriores, o Operador deverá conservar os dados nos casos em que o direito da União ou dos Estados-Membros preveja a sua conservação, nos termos impostos por essa legislação ou por essas determinações.

**5.13** Disponibilização ao Controlador de todas as informações necessárias para demonstrar o cumprimento das obrigações

O Operador disponibilizará ao Controlador todas as informações necessárias para demonstrar o cumprimento das obrigações previstas no art. 28 do GDPR e deve permitir e contribuir para as auditorias, inclusive as inspeções, realizadas pelo Controlador ou por outro auditor por ele designado – nos termos e na forma mais bem definidos no art. 8° abaixo – ou pelas autoridades.

**5.14** Caso em que uma instrução dada ao Operador seja considerada contrária ao GDPR

Caso o Operador, em sua opinião, considere que uma instrução do Controlador viola o GDPR ou outras disposições, nacionais ou da União, relativas à proteção de dados, deverá informar imediatamente o Controlador.

**5.15** Observância dos princípios de "privacy by design" e de "privacy by default"

O Operador, no desempenho do encargo, deverá atuar em observância dos princípios de proteção de dados desde a concepção (privacy by design) e de proteção de dados por padrão. Os SERVIÇOS são prestados de forma padronizada, igual para todos os clientes, e são concebidos de acordo com esses princípios.

**6. Obrigações do Controlador**

**6.1** O Controlador deve:

- fornecer ao Operador os dados previstos no art. 4° das presentes cláusulas;
- documentar por escrito todas as instruções relativas ao tratamento dos dados pelo Operador;
- zelar, previamente e durante todo o tratamento, pelo cumprimento, por parte do Operador, das obrigações previstas no regulamento europeu de proteção de dados;
- supervisionar o tratamento, realizando auditorias e inspeções.

**7. Locais onde os dados estão e estarão armazenados**

**7.1** Os dados serão tratados pelo Operador nos locais indicados no "Registro do tratamento do serviço". Caso o tratamento venha a ser realizado em países fora da UE, o Operador disponibilizará ao Controlador as garantias adotadas em função do local onde o tratamento for realizado.

**7.2** Se o Operador for obrigado a realizar uma transferência de dados para um país terceiro ou uma organização internacional, por força do direito da União ou do direito do Estado-Membro ao qual está sujeito, deve informar o Controlador sobre essa obrigação legal antes da transferência, a fim de obter autorização, salvo se a lei proibir essa informação por motivos relevantes de interesse público.

**8. Controles**

**8.1** O Controlador se reserva o direito de, inclusive por meio de verificações periódicas, fiscalizar a pontual observância das disposições legais sobre o tratamento dos dados e o cumprimento das suas instruções indicadas no presente documento. O Operador deverá permitir que o Controlador realize, com sua plena colaboração, verificações periódicas quanto à adequação das medidas de segurança adotadas e ao cumprimento da Legislação de Proteção de Dados e das disposições do próprio Controlador.

**8.2** Qualquer atividade de auditoria por parte do Controlador deverá ser acordada com o Operador, com aviso prévio de pelo menos 10 dias úteis. Caso essas atividades impliquem ônus e despesas não previstos no presente contrato, todas as solicitações do Controlador deverão ter a forma de execução acordada e ser gerenciadas no nível de projeto, com a definição de uma avaliação, inclusive econômica, para sua realização (sejam elas atividades de penetration test, vulnerability assessment ou outras).

**8.3** Qualquer informação compartilhada em cumprimento das obrigações do Operador ou do Controlador é classificada como confidencial e, portanto, não poderá ser divulgada, comunicada ou publicada na internet sem autorização prévia por escrito da outra parte. Cada pessoa autorizada que tratar a informação terá assinado um acordo de confidencialidade que preverá a proibição de comunicação a pessoas não autorizadas, mesmo após o término da relação de trabalho e até que as informações se tornem de domínio público por causas que não lhes sejam imputáveis. Qualquer violação da confidencialidade dessas informações será punida nos termos da lei e do contrato.

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

*Tradução de cortesia do original em italiano. Em caso de divergência, prevalece o texto em italiano.*

| | |
|---|---|
| Autor | Departamento de Privacidade da Zucchetti Spa |
| Aprovação | Fabrizio Scuppa, representante legal da Octorate S.r.l. |

**Versão Revisão**

| Versão | Autor | Consulta ao DPO | Data de emissão | Motivo da revisão |
|---|---|---|---|---|
| 0 | Departamento de Privacidade | | 12/11/2026 | Primeira emissão |

# OCTORATE

| OPERADOR | | | | | |
|---|---|---|---|---|---|
| **Razão social** | Octorate Srl | | | | |
| **N° de IVA** | 13493861002 | | | | |
| **Endereço** | Via Filippo Caruso 23 | | | | |
| **Cidade** | Roma | **CEP** | 00173 | **Prov.** | RM |
| **Representante legal** | Fabrizio Scuppa | | | | |

| PESSOAS AUTORIZADAS A TRATAR OS DADOS |
|---|
| Funcionários da Octorate responsáveis pelo suporte ao cliente, pelo onboarding e pelo treinamento, desenvolvedores e administradores de sistemas, autorizados e instruídos para o tratamento, com acessos limitados às suas funções. Para o OctoAgent, a equipe de desenvolvimento (4 pessoas) e a equipe de suporte (3 pessoas) da iManager S.r.l., Suboperador indicado entre os destinatários. |

| DADOS DE CONTATO | | | |
|---|---|---|---|
| **Operador** | Octorate Srl | legal@octorate.com | 06 4542 0568 |
| **Representante do operador** | N.A. | | |
| **Encarregado de Proteção de Dados (DPO)** | DPO da Octorate | dpo@octorate.com | |

| DESCRIÇÃO |
|---|
| Sistema de gestão das reservas, das tarifas e da disponibilidade, distribuição nos canais conectados, site e booking engine, comunicações com os hóspedes, cumprimento de obrigações perante a Polizia di Stato (polícia italiana), o ISTAT (instituto italiano de estatística) e a Agenzia delle Entrate (autoridade fiscal italiana), integrações de pagamento, operação diária do estabelecimento e, quando ativado, gestão automatizada das conversas com o OctoAgent. |

| FINALIDADE DO TRATAMENTO |
|---|
| Prestação dos Serviços Octorate por conta do Cliente, ou seja, gestão das reservas, das tarifas e da dis poni- |

bilidade, distribuição nos canais conectados, site e booking engine, comunicações com os hóspedes, cumprimento de obrigações perante a Polizia di Stato, o ISTAT e a Agenzia delle Entrate, integrações de pagamento, operação diária do estabelecimento e, quando ativado, gestão automatizada das conversas com o OctoAgent, com o suporte e a manutenção dos Serviços.
**Natureza do tratamento.** Coleta, registro, organização, estruturação, conservação, consulta, processamento, extração, comunicação por transmissão aos destinatários indicados pelo Cliente, eliminação. Para o OctoAgent, também processamento automatizado por meio de modelos de inteligência artificial para gerar respostas, traduções, resumos, transcrições, classificações e alertas.
**Duração e frequência.** Durante toda a vigência da relação contratual, de forma contínua. Os prazos de conservação por categoria estão indicados na seção sobre os prazos para a eliminação dos dados.

## CATEGORIA DE TITULARES DOS DADOS

Hóspedes e pessoas que fazem reservas, incluindo acompanhantes e hóspedes menores de idade, dentro dos limites das obrigações legais. Pessoas que entram em contato com o estabelecimento para pedir informações ou orçamentos. Usuários da conta do Cliente, ou seja, o titular do negócio, a equipe e os colaboradores. Proprietários das unidades administradas, no caso dos property managers que utilizam o portal de proprietários. Fornecedores e parceiros do Cliente eventualmente cadastrados na plataforma.

## CATEGORIAS DE DADOS PESSOAIS

Dados de reserva e de estadia. Nome e sobrenome, contatos, idioma, nacionalidade, datas de chegada e de partida, unidade e tipo, número e composição dos hóspedes, valores, canal de origem, preferências e observações inseridas pelo Cliente ou pelo hóspede.
Dados para o cumprimento de obrigações legais. Para as fichas de hóspedes Alloggiati, dados cadastrais, local e data de nascimento, cidadania, tipo, número e local de emissão do documento de identidade. Para o ISTAT, dados estatísticos sobre os fluxos. Para os documentos fiscais, dados fiscais dos hóspedes, código fiscal e nº de IVA.
Dados de pagamento. Dados do cartão de crédito coletados como garantia da reserva, armazenados de forma criptografada segundo os padrões PCI-DSS e que não podem ser descriptografados diretamente pela Octorate, resultados das transações comunicados pelos gateways e pelas instituições de pagamento.
Comunicações. Conteúdo e anexos das mensagens trocadas com os hóspedes por e-mail, mensagens dos portais OTA, WhatsApp, SMS e chat do site. Com o OctoAgent, também as imagens enviadas pelos hóspedes, os resumos, as transcrições e as gravações de áudio das chamadas quando o módulo de voz está ativo, as linhas de raciocínio do agente e as lições aprovadas pelo Cliente.
Check-in online com o OctoAgent. Imagem do documento de identidade enviada pelo hóspede para o check-in, da qual o OctoAgent extrai os dados cadastrais. A fotografia do documento é ocultada antes do envio ao modelo de inteligência artificial.
Site e booking engine. Dados dos visitantes e das pessoas que fazem reservas no site e no booking engine do Cliente, de acordo com a política de privacidade e a política de cookies do Cliente.

Usuários da conta. Nome, e-mail, função, credenciais, logs de acesso e de atividade, necessários ao funcionamento e à segurança da plataforma.
Categorias especiais de dados. Não previstas pelos Serviços. As informações comunicadas espontaneamente pelos hóspedes, por exemplo necessidades de saúde, alimentares ou religiosas, são tratadas sob a responsabilidade do Cliente.

## NENHUM USO PARA FINALIDADES PRÓPRIAS

A Octorate não utiliza os Dados do Cliente para finalidades próprias. A Octorate pode processar dados de forma agregada e anônima, que não permitem identificar nem o Cliente nem os titulares dos dados, para fins estatísticos, de segurança e de melhoria dos Serviços.

## CATEGORIA DE DESTINATÁRIOS AOS QUAIS OS DADOS PODERÃO SER COMUNICADOS

Lista dos Suboperadores autorizados de forma geral pelo Cliente, com o país e as garantias para a transferência dos dados de cada fornecedor. Os portais OTA, os órgãos públicos, os gateways e as instituições de pagamento não são Suboperadores e recebem os dados conforme indicado entre as entidades que recebem os dados como controladores autônomos.

- Aruba S.p.A. (Itália). Hosting, banco de dados, armazenamento e backup da plataforma Octorate (PMS, Channel Manager, Booking Engine). Garantia de transferência intra-EEE.
- Complior AB (antiga 24 Solutions) (Suécia). Ambiente certificado PCI DSS conectado à plataforma para os dados dos cartões de crédito. Garantia de transferência intra-EEE.
- iManager S.r.l., Via del Muro Linari 31, 00173 Roma, código fiscal e n° de IVA 16082961000 (Itália). Desenvolvimento, gestão e hosting da aplicação da plataforma OctoAgent. Garantia de transferência intra-EEE.
- Google Cloud (Google Cloud EMEA Limited) (Irlanda, data center de Milão). Hosting do OctoAgent. Garantia de transferência intra-EEE, cláusulas contratuais padrão para eventuais acessos a partir de países terceiros.
- MongoDB Atlas (MongoDB Limited) (Irlanda, data centers de Milão e Frankfurt). Banco de dados do OctoAgent e backup. Garantia de transferência intra-EEE, cláusulas contratuais padrão para eventuais acessos a partir de países terceiros.
- OpenAI (OpenAI Ireland Limited, parte contratante para o EEE) (Irlanda, tratamento também nos Estados Unidos). Modelos de inteligência artificial do OctoAgent, geração de respostas, resumos, transcrições, extração dos dados dos documentos, por meio da conta da iManager. Modelos de inteligência artificial das outras funções da plataforma Octorate, por meio da conta da Octorate. Garantia de transferência Cláusulas contratuais padrão incluídas no DPA da OpenAI, que não tem a certificação DPF.
- Openapi S.r.l. (Openapi.com) (Itália). Envio de SMS aos hóspedes pelo OctoAgent. Garantia de transferência intra-EEE.
- Better Stack (UE). Monitoramento da disponibilidade e alarmes do OctoAgent, região de dados UE, somente se dados pessoais trafegarem pelos logs. Garantia de transferência intra-EEE.

- Microsoft Clarity (Microsoft) (Irlanda, EUA). Análise do uso do console do OctoAgent pelos usuários dos estabelecimentos, com mascaramento ativado. Garantia de transferência Adequação (DPF) ou cláusulas contratuais padrão.
- Meta (WhatsApp Business Platform) (Irlanda, EUA). Mensagens de WhatsApp entre estabelecimentos e hóspedes. Garantia de transferência Adequação (DPF) ou cláusulas contratuais padrão.
- Mailchimp Transactional (Mandrill, The Rocket Science Group LLC) e SparkPost (Bird) (EUA, UE). Serviços de envio de e-mail autorizados para o domínio octorate.com, para os e-mails que não saem dos servidores de e-mail da Octorate. O OctoAgent não os utiliza. Garantia de transferência Adequação (DPF) ou cláusulas contratuais padrão.
- Mailgun (Mailgun Technologies, Inc., grupo Sinch) (EUA, UE). Serviço de envio dos e-mails dos Serviços. Garantia de transferência Cláusulas contratuais padrão.
- Intercom (Intercom R&D Unlimited Company) (Irlanda, EUA). Chat de suporte da plataforma Octorate, somente se por ele trafegarem dados dos hóspedes. O OctoAgent não o utiliza. Garantia de transferência Adequação (DPF).

O serviço de telefonia do módulo de voz do OctoAgent é prestado pela Vonage com um contrato em nome do Cliente, ativado por indicação da Octorate, razão pela qual a Vonage não é Suboperador da Octorate. As alterações desta lista são comunicadas ao Cliente. A versão atualizada está disponível mediante solicitação para legal@octorate.com.

## TRANSFERÊNCIA DE DADOS PARA O EXTERIOR

Os Dados do Cliente são armazenados em data centers situados na União Europeia, indicados nas medidas de segurança relativas ao data center.

A Octorate transfere Dados do Cliente para países terceiros, inclusive por meio de Suboperadores, somente em conformidade com o Capítulo V do GDPR, com base em uma decisão de adequação da Comissão Europeia, incluindo o marco EU-US Data Privacy Framework para os fornecedores certificados, ou nas cláusulas contratuais padrão adotadas pela Decisão de Execução (UE) 2021/914 da Comissão, complementadas pelas medidas suplementares eventualmente necessárias. As garantias aplicadas a cada Suboperador estão indicadas na lista dos destinatários. Para os modelos de inteligência artificial do OctoAgent e das outras funções da plataforma, os dados necessários à geração dos conteúdos são transmitidos à OpenAI, que também os trata nos Estados Unidos com base nas cláusulas contratuais padrão incluídas em seu acordo de tratamento de dados.

As transmissões para portais OTA, gateways de pagamento, softwares de terceiros conectados pelo Cliente via API, hóspedes e outros destinatários indicados pelo Cliente, inclusive situados em países terceiros, ocorrem por instrução do Cliente, que é responsável por elas.

## PRAZOS PARA A ELIMINAÇÃO DOS DADOS

Dados de reserva, de estadia e dados cadastrais dos hóspedes. Durante toda a vigência do contrato e até 30 dias após o encerramento, salvo instrução diversa do Cliente.

Mensagens e conversas com os hóspedes. Durante toda a vigência do contrato, salvo eliminação antecipada por instrução do Cliente.
Transcrições, resumos e gravações das chamadas, lições e linhas de raciocínio do OctoAgent. Durante toda a vigência do contrato, salvo eliminação antecipada por instrução do Cliente.
Dados enviados aos modelos de inteligência artificial (OpenAI). Não são armazenados pelo fornecedor para usos posteriores. A OpenAI os conserva por até 30 dias para o controle de abusos e depois os elimina.
Dados para fichas de hóspedes Alloggiati, ISTAT e documentos fiscais. Pelo tempo necessário à transmissão e ao cumprimento das obrigações de conservação previstas em lei.
Logs técnicos e de segurança. Para a plataforma Octorate, logs das requisições HTTP por 45 dias e logs dos acessos dos administradores de sistema por pelo menos 6 meses, salvo obrigações legais. Para o OctoAgent, logs de aplicação por 90 dias e logs de auditoria por 400 dias. Nos logs do OctoAgent não são registrados os conteúdos dos hóspedes, ou seja, mensagens, e-mails, telefone e documentos. Os logs técnicos das requisições, conservados por 400 dias para fins de segurança, contêm o endereço IP de quem se conecta. Somente a equipe de desenvolvimento da iManager tem acesso aos logs.
Backups. Sobrescrita automática segundo os ciclos indicados a seguir. Para o OctoAgent, backups diários conservados por 7 dias, semanais por 4 semanas e cópia diária em Frankfurt conservada por 90 dias. Para a plataforma Octorate, backups diários conservados por 30 dias.
Antes do encerramento, o Cliente pode exportar os Dados do Cliente por meio das funções de exportação da plataforma, em formatos estruturados de uso comum. Mediante solicitação por escrito recebida antes do encerramento, a Octorate presta assistência na devolução dos dados que não puderem ser exportados pelo próprio Cliente, pelos valores eventualmente acordados.
No prazo de 30 dias contados do encerramento, a Octorate elimina os Dados do Cliente e as cópias existentes, exceto os backups, que são sobrescritos de forma rotativa conforme indicado acima, e exceto os dados que a Octorate deva conservar por obrigações legais, entre eles os documentos fiscais e os logs exigidos pela legislação, que são conservados pelo prazo prescrito e depois eliminados. Os pedidos de eliminação recebidos durante a relação contratual são atendidos no prazo de 5 dias úteis, conforme previsto nos Termos e Condições. Mediante solicitação, a Octorate atesta por escrito que a eliminação foi realizada.

## ENTIDADES QUE RECEBEM OS DADOS COMO CONTROLADORES AUTÔNOMOS

Os portais OTA, os gateways e as instituições de pagamento, a Polizia di Stato, o ISTAT, a Agenzia delle Entrate e as demais entidades às quais os Serviços transmitem dados por instrução do Cliente tratam os dados como controladores autônomos ou de acordo com os respectivos acordos com o Cliente. A Octorate se limita à transmissão técnica e não responde pelo tratamento realizado por essas entidades. O mesmo vale para a Vonage, que presta o serviço de telefonia do módulo de voz do OctoAgent com um contrato em nome do Cliente.

## REGISTRO DAS ATIVIDADES DE TRATAMENTO

A Octorate mantém o registro das categorias de atividades de tratamento realizadas por conta dos clientes

nos termos do art. 30, parágrafo 2, do GDPR e o disponibiliza ao Cliente mediante solicitação para legal@octorate.com.

# DESCRIÇÃO GERAL DAS MEDIDAS DE SEGURANÇA TÉCNICAS E ORGANIZACIONAIS

## 1. MEDIDAS DE SEGURANÇA IMPLEMENTADAS NO SOFTWARE

Medidas de segurança adotadas na plataforma Octorate e no OctoAgent.

*- Gestão das credenciais de acesso*

• Credenciais pessoais para cada usuário, regras sobre a força das senhas, bloqueio dos acessos não autorizados e registro dos acessos.
• Autenticação de dois fatores com código OTP para a plataforma Octorate e para o acesso ao OctoAgent com credenciais Octorate.
• O OctoAgent prevê também um acesso interno para a equipe operacional do estabelecimento que não tem conta de usuário Octorate, por exemplo quem atende o telefone, manutenção e limpeza, sem autenticação de dois fatores e não destinado a usuários com poderes de administrador. A extensão da autenticação de dois fatores aos usuários internos está em avaliação com o fornecedor.

*- Minimização*

• Perfis e permissões configuráveis pelo Cliente, para limitar o acesso aos dados às atribuições de cada usuário.
- Identificação de quem tem acesso ao sistema
• Logs técnicos que permitem reconstituir as atividades realizadas na plataforma. Para o OctoAgent, logs de aplicação conservados por 90 dias, logs de auditoria e logs técnicos das requisições conservados por 400 dias, sem os conteúdos dos hóspedes. Os logs técnicos contêm o endereço IP de quem se conecta e só podem ser acessados pela equipe de desenvolvimento da iManager. Para a plataforma Octorate, logs das requisições HTTP conservados por 45 dias. Os acessos dos administradores de sistema são registrados de forma inalterável e os respectivos logs são conservados por pelo menos 6 meses, conforme previsto na decisão do Garante (autoridade italiana de proteção de dados) sobre os administradores de sistema.
• Acessos da equipe de suporte à conta do Cliente de acordo com as medidas para os serviços de suporte indicadas mais adiante.

*- Técnicas de criptografia*

• Transmissão dos dados com protocolo TLS em todos os Serviços.
• Dados dos cartões de crédito armazenados de forma criptografada segundo o padrão PCI DSS, que não podem ser descriptografados diretamente pela Octorate.
• Criptografia dos dados em repouso nos bancos de dados da plataforma Octorate e do OctoAgent.

*- Privacy by default*

• Serviços prestados de forma padronizada, igual para todos os clientes, e concebidos de acordo com os princípios de proteção de dados desde a concepção e por padrão. Separação lógica dos dados dos diferentes clientes na plataforma.

*- Direitos dos titulares dos dados*

• O Cliente pode exportar os dados da plataforma em formatos estruturados de uso comum. A Octorate presta assistência ao Cliente para atender aos pedidos dos titulares dos dados. Os pedidos de eliminação recebidos durante a relação contratual são atendidos no prazo de 5 dias úteis.

## 2. OPERADOR: MEDIDAS DE SEGURANÇA IMPLEMENTADAS PARA OS SERVIÇOS DE SUPORTE

A Octorate presta suporte aos Clientes remotamente, pelo chat da plataforma, por e-mail e por telefone, com pessoal autorizado e instruído para o tratamento. Os pedidos recebidos por chat e por e-mail são registrados como tickets no Intercom, indicado entre os destinatários. Quando necessário para resolver o pedido, a equipe de suporte acessa a conta do Cliente pelo painel interno da Octorate, com credenciais pessoais e sem usar a senha do Cliente. A Octorate não se conecta aos dispositivos do Cliente com programas de acesso remoto.
A equipe de suporte trata os dados do Cliente somente para resolver o pedido. Os arquivos e as exportações para o suporte são recebidos do Cliente como anexos no chat da plataforma e são usados somente para aquele pedido. Permanecem anexados à conversa no Intercom durante a vigência do contrato. São eliminados nos prazos indicados neste Registro para os Dados do Cliente, ou seja, no prazo de 30 dias contados do encerramento, salvo as obrigações de conservação previstas em lei, ou antes, mediante solicitação do Cliente.

## 3. OPERADOR: MEDIDAS DE SEGURANÇA RELATIVAS AO DATA CENTER

**Plataforma Octorate.** Infraestrutura na Aruba S.p.A., em data centers na Itália certificados ISO/IEC 27001, 27017, 27018 e ANSI/TIA-942 Rating 4. Backups diários do banco de dados conservados por 30 dias, com procedimentos de restauração.
**Cartões de crédito.** Dados dos cartões de crédito em ambiente certificado PCI DSS na Complior AB, Suécia.
**OctoAgent.** Desde 20 de outubro de 2026, hosting no Google Cloud em Milão, com banco de dados MongoDB Atlas em Milão e cópia dos backups em Frankfurt, em substituição à Scaleway em Paris, onde os dados foram eliminados após a migração. Fornecedores com certificações ISO/IEC 27001 e SOC 2. Backups diários conservados por 7 dias, semanais por 4 semanas e cópia diária em Frankfurt conservada por 90 dias.
**E-mails do sistema.** Os e-mails do sistema da plataforma são enviados a partir dos servidores de e-mail da Octorate hospedados na Aruba ou pelos serviços de envio de e-mail indicados entre os destinatários.

## 4. MEDIDAS DE SEGURANÇA BÁSICAS NIS2

A Octorate faz parte do Grupo Zucchetti, entidade essencial nos termos da Legislação NIS2, e aplica as medidas de segurança básicas definidas pela ACN (agência italiana de cibersegurança) segundo o modelo do Grupo. Os itens a seguir indicam, para cada área prevista no modelo, as medidas adotadas pela Octorate para os Serviços.

**Confiabilidade dos fornecedores.** A Octorate trata os Dados do Cliente somente com os Suboperadores indicados entre os destinatários, vinculados por acordos em conformidade com o artigo 28 e escolhidos entre fornecedores com certificações de segurança reconhecidas (ISO/IEC 27001, SOC 2, PCI DSS). Cada novo fornecedor é avaliado antes do uso e comunicado ao Cliente. A Octorate participa do processo de qualificação de fornecedores do Grupo Zucchetti por meio do ponto focal do grupo.

**Funções e responsabilidades.** Encarregado de Proteção de Dados, que pode ser contatado pelo e-mail dpo@octorate.com. Pontos focais internos para a segurança e os incidentes indicados no procedimento de gestão de incidentes. Para as obrigações NIS2, a Octorate se reporta ao ponto de contato NIS e ao ponto focal CSIRT designados pelo Grupo Zucchetti para o setor de hospitalidade, com o respectivo substituto, indicados no procedimento de gestão de incidentes.

**Confiabilidade dos recursos humanos.** Pessoal autorizado ao tratamento, instruído sobre a Legislação aplicável e vinculado à confidencialidade, com acessos limitados às suas funções e revogados no término do vínculo.

**Conformidade e auditoria.** Informações e verificações à disposição do Cliente mediante solicitação. Infraestruturas em fornecedores certificados e submetidos a auditorias de terceiros, em particular Aruba S.p.A. (ISO/IEC 27001, 27017, 27018 e ANSI/TIA-942 Rating 4), Complior AB (PCI DSS), Google Cloud e MongoDB (ISO/IEC 27001 e SOC 2).

**Gestão de vulnerabilidades.** Atualizações e correções de segurança aplicadas com prioridade. Para o OctoAgent, varredura de vulnerabilidades e revisão da configuração da nova infraestrutura até 30 de novembro de 2026, primeiro penetration test externo até 31 de março de 2027 e depois uma vez por ano, com gestão dos resultados e das correções. Para a plataforma Octorate, testes de vulnerabilidade e penetration tests no âmbito do programa do Grupo Zucchetti, no qual a Octorate está incluída por meio do ponto focal do grupo.

**Continuidade operacional e disaster recovery.** Backups da plataforma Octorate diários e conservados por 30 dias, com procedimentos de restauração. Para o OctoAgent, backups diários conservados por 7 dias, semanais por 4 semanas e cópia diária em Frankfurt conservada por 90 dias. Data centers certificados ANSI/TIA-942 Rating 4 para a plataforma Octorate. Monitoramento contínuo da disponibilidade dos Serviços.

**Gestão de identidades e acessos.** Credenciais pessoais, privilégio mínimo com perfis e permissões configurados pelo Cliente, regras sobre a força das senhas, bloqueio dos acessos não autorizados, registro dos acessos e revisão das contas de usuário. Autenticação de dois fatores com código OTP para a plataforma Octorate e para o acesso ao OctoAgent com credenciais Octorate. Acesso interno ao OctoAgent para a equipe operacional do estabelecimento com os limites indicados nas medidas de segurança implementadas no software. Acessos técnicos e administrativos à infraestrutura do OctoAgent pelo console do provedor de nuvem com autenticação de dois fatores, em rede privada não exposta à internet, com o servidor de acesso ao banco de dados ligado somente quando necessário. Acessos e alterações administrativas registrados e monitorados.

**Segurança física.** Dados armazenados exclusivamente nos data centers dos fornecedores indicados neste

Registro, com o controle dos acessos físicos previsto pelas certificações dos fornecedores.
**Treinamento e conscientização.** Treinamento da equipe sobre a proteção de dados pessoais e sobre a segurança da informação, com conteúdos diferenciados para pessoal geral, técnico e diretoria, segundo o programa do Grupo Zucchetti, no qual a Octorate está incluída por meio do ponto focal do grupo.
**Segurança dos dados.** Transmissão com protocolo TLS, criptografia dos dados em repouso nos bancos de dados da plataforma Octorate e do OctoAgent, dados dos cartões de crédito em ambiente certificado PCI DSS, separação lógica dos dados dos clientes, backups armazenados na União Europeia, eliminação segura no encerramento.
**Proteção das redes e das comunicações.** Proteção de perímetro dos fornecedores de hosting, infraestrutura serverless do OctoAgent em rede privada não exposta à internet, firewall de aplicação no OctoAgent com registro dos bloqueios, canais de comunicação oficiais com o Cliente (e-mail da conta e avisos na plataforma), usados também para as comunicações sobre incidentes.
**Monitoramento de eventos.** Para o OctoAgent, verificação a cada minuto da disponibilidade do serviço por monitoramento externo, dos erros de aplicação, dos tempos de resposta, dos erros nas chamadas ao Octorate e aos fornecedores dos modelos, da memória e das filas de trabalho, dos bloqueios do firewall de aplicação e dos acessos e das alterações administrativas, com alarmes para a equipe técnica. Logs de aplicação conservados por 90 dias, logs de auditoria e logs técnicos das requisições por 400 dias, sem os conteúdos dos hóspedes. Os logs técnicos contêm o endereço IP de quem se conecta e só podem ser acessados pela equipe de desenvolvimento da iManager. Para a plataforma Octorate, logs das requisições HTTP conservados por 45 dias e logs dos acessos dos administradores de sistema, inalteráveis, conservados por pelo menos 6 meses.
**Gestão e notificação de incidentes.** Procedimento escrito para detectar, avaliar, conter e comunicar os incidentes. O fornecedor que gerencia o OctoAgent avisa a Octorate em até 12 horas após a detecção de um incidente que afete os dados ou o serviço, mesmo com informações parciais, com atualização e análise em até 48 horas e relatório final em até 20 dias, para que o Grupo possa cumprir os prazos de 72 horas e de um mês perante o CSIRT Italia. A Octorate notifica a violação ao Cliente em até 48 horas a partir do momento em que toma conhecimento dela e, para os incidentes significativos nos termos da Legislação NIS2, aciona o ponto focal do Grupo Zucchetti para a notificação ao CSIRT Italia, com pré-notificação em até 24 horas e notificação em até 72 horas.
**Desenvolvimento seguro.** Desenvolvimento segundo práticas de segurança desde a concepção, atualizações e correções de segurança, ambientes de desenvolvimento e de produção separados e liberação controlada de versões.
**Manutenção ordinária e evolutiva.** Atualizações e novas funcionalidades lançadas por meio de um processo de gestão de mudanças e comunicadas ao Cliente de acordo com a seção Evolução e alteração dos serviços dos Termos e Condições. Para o OctoAgent, migração da infraestrutura concluída em 20 de outubro de 2026, com revisão da configuração até 30 de novembro de 2026.
**Descomissionamento.** Eliminação dos Dados do Cliente no prazo de 30 dias contados do encerramento e no prazo de 5 dias úteis mediante solicitação, conforme indicado nos prazos para a eliminação dos dados, com sobrescrita dos backups de forma rotativa. Descarte seguro das mídias a cargo dos fornecedores de infraestrutura, de acordo com as respectivas certificações.
**Subcontratação e cadeia de suprimentos.** Lista dos Suboperadores entre os destinatários, com obrigações contratuais equivalentes às da designação como operador, incluindo as medidas de segurança básicas NIS2 aplicáveis, e com a possibilidade de o Cliente se opor às alterações no prazo de 15 dias contados da comunicação.