DESIGNACIÓN COMO ENCARGADO DEL TRATAMIENTO
- Data Processing Agreement -
(Art. 28 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016)

CONSIDERANDO QUE

a. Entre el CLIENTE y el PROVEEDOR indicado en el contrato al que se refiere el presente documento (en adelante, PROVEEDOR) está en vigor un contrato para la prestación de servicios informáticos y/o servicios relacionados con ellos (en adelante, SERVICIO y/o SERVICIOS), del que la presente forma parte integrante;

b. en el presente contrato las partes acuerdan definir
- con el término "GDPR", el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y
- con el término "Normativa de Privacidad", las disposiciones del GDPR, así como todas las demás disposiciones del Derecho de la Unión o del Derecho de los Estados miembros relativas a la protección de los datos personales y a su libre circulación.

c. en la prestación del SERVICIO, el Responsable del tratamiento de los datos personales, con arreglo y a los efectos del art. 4, apdo. 1, n.° 7, del GDPR, es el CLIENTE, y a este le incumbe la realización de todos los actos previstos en la Normativa de Privacidad para el tratamiento de los datos personales, es decir, facilitar la información, recabar el consentimiento y adoptar todas las medidas de autorización, de designación, de conservación y de otro tipo, también para implantar el sistema de seguridad, incluidas las medidas correspondientes;

En virtud de lo anterior, entre las Partes,

SE ACUERDA Y SE ESTIPULA

lo que se indica a continuación.

1. Designación como Encargado del tratamiento

1.1 Para las tareas que, en virtud del contrato relativo al SERVICIO, se confían al PROVEEDOR, este último, con arreglo al art. 4, apdo. 1, n.° 8), y al art. 28 del GDPR, es designado Encargado del tratamiento.

1.2 El Encargado del tratamiento precisa que está en condiciones de ofrecer garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del GDPR y garantice la protección de los derechos de los interesados.

2. Objeto del DPA

2.1 El objeto de la presente designación es definir las modalidades y las condiciones contractuales con las que el Encargado del tratamiento se compromete a efectuar, por cuenta del Responsable del tratamiento, las operaciones de tratamiento de los datos personales definidos en el contrato y especificadas en el anexo técnico "Registro del tratamiento del servicio", puesto a disposición a petición del Responsable del tratamiento.

2.2 En el marco de sus relaciones contractuales, las partes se comprometen a respetar la normativa vigente aplicable al tratamiento de los datos personales y, en particular, el GDPR y la Normativa de Privacidad.

3. Duración del DPA

La presente designación tendrá la duración del contrato al que se refiere.

4. Descripción de las prestaciones del Encargado del tratamiento

4.1 El Encargado del tratamiento está autorizado a tratar, por cuenta del Responsable del tratamiento, los datos personales necesarios para prestar el SERVICIO tal como se prevé en el contrato. Respecto de los datos que el Responsable del tratamiento ya ha facilitado y que facilitará, este garantiza que dispone de una base jurídica adecuada con arreglo al art. 6 del GDPR, como el contrato con el huésped, las obligaciones legales en materia de seguridad pública, estadística y fiscal y, cuando sea necesario, el consentimiento.

El Responsable del tratamiento garantiza al Encargado del tratamiento que dispone legítimamente de toda la información que confiará al Encargado del tratamiento para su tratamiento, y asegura asimismo que dicha información no vulnera en modo alguno derechos de terceros.

El Responsable del tratamiento conserva la titularidad de la información que se comunique al Encargado del tratamiento para el SERVICIO, asume expresamente la más amplia responsabilidad respecto del contenido de los correspondientes datos personales y exonera y mantiene indemne al Encargado del tratamiento de toda obligación y/o carga de comprobación y/o de control directo e indirecto al respecto.

4.2 La naturaleza de las operaciones realizadas sobre los datos es la prestación del SERVICIO y/o de los SERVICIOS indicados en el contrato, por lo que el Responsable del tratamiento declara que confía el correspondiente tratamiento de los datos al Encargado del tratamiento.

4.3 La finalidad del tratamiento, la naturaleza y el tipo de los datos tratados y las categorías de interesados son los especificados en el "Registro del tratamiento del servicio".

4.4 En lo que sea de su competencia, el Encargado del tratamiento, al tratar los datos para la prestación del SERVICIO, efectuará el tratamiento observando el art. 5 del GDPR, sobre los "Principios relativos al tratamiento".

4.5 Para la ejecución del encargo objeto del presente contrato, el Responsable del tratamiento pone a disposición del Encargado del tratamiento la información necesaria para la ejecución de las actividades relativas al SERVICIO, incluida la destinada al uso adecuado del sistema de información.

4.6 El Encargado del tratamiento, con arreglo al art. 28, apdo. 3, letra b), del GDPR, identifica y designa por escrito a sus personas autorizadas, definiendo con precisión el ámbito de tratamiento permitido. El Encargado del tratamiento declara ser consciente de que sus personas autorizadas actúan bajo su autoridad.

5. Obligaciones del Encargado del tratamiento

El Encargado del tratamiento, en el desempeño de sus funciones, se compromete a cumplir y observar las siguientes obligaciones.

5.1 <u>Observancia de las instrucciones dadas por el Responsable</u>

a. El Encargado del tratamiento deberá tratar los datos únicamente para las finalidades antes especificadas y para la ejecución de las prestaciones contractuales.

b. El Encargado del tratamiento deberá tratar los datos de conformidad con lo previsto en el "Registro del tratamiento del servicio", y el Responsable del tratamiento considera adecuadas las medidas de seguridad previstas en él.

5.2 <u>Garantizar la confidencialidad</u>

a. El Encargado del tratamiento garantiza que se respeta la confidencialidad de los datos personales tratados en el marco de la presente designación.

b. El Encargado del tratamiento garantiza que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación legal de confidencialidad adecuada, y que reciban la formación necesaria en materia de tratamiento de datos personales.

5.3 Adopción de las medidas de seguridad del tratamiento

a. El Encargado del tratamiento debe llevar a cabo el tratamiento de los datos personales con las medidas exigidas con arreglo al art. 32 del GDPR. Las medidas de seguridad adoptadas son las declaradas en el "Registro del tratamiento del servicio". El Responsable del tratamiento toma nota de que, en algunos casos, el Encargado del tratamiento llevará a cabo el tratamiento mediante las herramientas preparadas y configuradas por aquel y, por tanto, deberá adoptar todas las cautelas necesarias solo cuando el tratamiento se efectúe fuera del control de la herramienta establecida y configurada por el Responsable del tratamiento.

b. Si el Encargado del tratamiento se ha adherido a un código de conducta o ha presentado una certificación, debe operar con las medidas de seguridad previstas en el código de conducta o en los protocolos correspondientes a la certificación. En este caso, el Responsable del tratamiento aceptará la certificación como prueba de que el Encargado del tratamiento ha adoptado medidas adecuadas respecto del tratamiento efectuado, y renuncia a realizar actividades de auditoría sobre los sistemas y los procedimientos del PROVEEDOR.

c. El Encargado del tratamiento, en los casos contemplados en el art. 37 del GDPR, actúa con el apoyo de su propio Delegado de protección de datos (DPD o DPO): si ha sido designado, sus datos de contacto se indican en el "Registro del tratamiento del servicio".

d. De conformidad con el art. 30 del GDPR, el Encargado del tratamiento (y, en su caso, su representante, si no se encuentra en los supuestos de exención previstos en el apartado 5 de dicho artículo) debe llevar un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del Responsable del tratamiento, que contenga lo indicado en el apdo. 2 de dicho artículo.

e. Los registros indicados se llevan por escrito, también en formato electrónico, y se pondrán a disposición del Responsable del tratamiento a petición de este.

5.4 Designación de Subencargados

a. Con arreglo al art. 28, apdo. 2, del GDPR, mediante la presente designación, el Responsable del tratamiento otorga al Encargado del tratamiento una autorización expresa, escrita y general para seleccionar a otros sujetos que desempeñen, por cuenta del propio Encargado, la función de Subencargados. En virtud de dicha autorización, el Encargado del tratamiento se compromete a comunicar al Responsable del tratamiento la lista de todos los sujetos que, en su caso, haya seleccionado como Subencargados. En caso de que con el tiempo se produzcan modificaciones, incorporaciones o sustituciones de los Subencargados comunicados inicialmente, estas nuevas designaciones deberán comunicarse al Responsable del tratamiento, que dispondrá de 15 días desde la recepción de la comunicación para oponerse, en su caso, exponiendo los motivos en que fundamenta su oposición. Cuando no sea posible alcanzar una solución consensuada, el Cliente/Responsable del tratamiento puede desistir del contrato relativo al Servicio utilizado, en los términos previstos en este. El Encargado del tratamiento declara y garantiza que los Subencargados ofrecen garantías suficientes para aplicar medidas técnicas y organizativas idóneas para garantizar el cumplimiento de las disposiciones de la Normativa de Privacidad vigente y se compromete a vincular contractualmente a los otros encargados al cumplimiento de las mismas obligaciones en materia de protección de datos personales asumidas por el Encargado del tratamiento frente al CLIENTE.

b. Si el Subencargado del tratamiento incumple sus obligaciones en materia de protección de datos, el Encargado del tratamiento sigue siendo plenamente responsable, ante el Responsable del tratamiento, del cumplimiento de las obligaciones del Subencargado del tratamiento.

c. Se precisa que, en todos los casos en que el SERVICIO no se preste directamente al CLIENTE, sino a los clientes finales de este, el PROVEEDOR se configura como otro Encargado del tratamiento y estará obligado a tratar los datos en las mismas condiciones establecidas en el presente acto de designación para el Encargado del tratamiento.

5.5 Asistencia al Responsable para el ejercicio de los derechos de los interesados

a. En la medida de lo posible, el Encargado del tratamiento, teniendo en cuenta la naturaleza del tratamiento, debe asistir al Responsable del tratamiento para que este pueda responder a las solicitudes de ejercicio de los derechos del interesado previstos en el Capítulo III del GDPR.

El Encargado del tratamiento, en la medida en que sea posible, asistirá al Responsable del tratamiento mediante medidas técnicas y organizativas apropiadas.

b. En relación con el derecho de información de los interesados, corresponde al Responsable del tratamiento facilitar a los interesados la información prevista en los arts. 13 y 14 del GDPR respecto de las operaciones de tratamiento, en el momento de la recogida de los datos.

Cuando reciba directamente solicitudes de un interesado relativas al tratamiento de datos personales efectuado por cuenta del CLIENTE, el Encargado de dicho tratamiento invita al interesado a dirigirse al CLIENTE, como Responsable del tratamiento, y comunica con prontitud a este último la solicitud recibida del interesado, en un plazo de 10 días hábiles desde su recepción.

5.6 Asistencia al Responsable del tratamiento para garantizar el cumplimiento de las obligaciones previstas en los artículos 32 a 36 del GDPR

a. El Encargado del tratamiento, teniendo en cuenta la naturaleza del tratamiento y la información a su disposición, debe asistir al Responsable del tratamiento para garantizar el cumplimiento de las obligaciones previstas en los arts. 32 a 36 del GDPR, es decir:

- el artículo 32. Seguridad del tratamiento;
- el artículo 33. Notificación de una violación de la seguridad de los datos personales a la autoridad de control;
- el artículo 34. Comunicación de una violación de la seguridad de los datos personales al interesado;
- el artículo 35. Evaluación de impacto relativa a la protección de datos;
- el artículo 36. Consulta previa.

b. Asistencia para la Seguridad del tratamiento – El Encargado del tratamiento tiene la obligación de asistir al Responsable del tratamiento en la implantación de la seguridad del tratamiento, de conformidad con el art. 32 del GDPR.

El Encargado del tratamiento, a petición del Responsable del tratamiento, informará sobre las medidas de seguridad adoptadas, también mediante eventuales cuestionarios y listas de control, previa valoración a nivel de proyecto si fuera necesaria.

c. Medidas de seguridad específicas del Encargado del tratamiento ya implantadas – El Responsable del tratamiento toma nota de que, para el SERVICIO, el Encargado del tratamiento tiene en vigor medidas de seguridad adecuadas en cumplimiento del GDPR.

Administradores de sistemas. En relación con las actividades realizadas por el Encargado del tratamiento relativas a la conservación de los datos personales y con las actividades de sistemas destinadas al mantenimiento de la red y a la actualización de las correspondientes bases de datos y sistemas operativos, los operadores del Encargado del tratamiento tendrán la función de Administradores de sistemas.

Las obligaciones previstas por el Garante per la privacy (autoridad italiana de protección de datos) en la resolución de 27 de noviembre de 2008 serán gestionadas por el Encargado del tratamiento; en particular, será el Encargado del tratamiento quien valore las características subjetivas de los administradores de sistemas, efectúe las designaciones individuales, verifique las actividades realizadas por ellos y se ocupe del registro de los correspondientes accesos. En relación con lo previsto en dicha resolución, el Encargado del tratamiento se obliga a comunicar al Responsable del tratamiento la lista actualizada de los Administradores de sistemas; la comunicación de dichos datos podrá realizarse en formato electrónico o en papel, y el Responsable del tratamiento considera cumplida dicha obligación también con la simple puesta a disposición de la lista actualizada de los nombres de dichos Administradores de sistemas a petición del Responsable del tratamiento.

5.7 Asistencia para la obligación de Notificación de una violación de la seguridad de los datos personales a la autoridad de control

El Encargado del tratamiento tiene la obligación de asistir al Responsable del tratamiento en el cumplimiento de sus obligaciones de notificación de una violación de la seguridad de los datos personales a la autoridad de control, de conformidad con el art. 33 del GDPR. El Encargado del tratamiento notifica al Responsable del tratamiento toda violación de la seguridad de los datos personales en un plazo máximo de 48 horas desde que tenga conocimiento de ella. Dicha notificación va acompañada de lo expresamente indicado en el apdo. 3 del art. 33, útil para permitir al Responsable del tratamiento, si es necesario, notificar dicha violación a la autoridad de control competente.

En efecto, corresponde exclusivamente al Cliente, cuando sea Responsable del tratamiento, determinar si el incidente puede calificarse como Data Breach y si el riesgo para los interesados es tal que exige la notificación a la Autoridad de control y la comunicación a los interesados afectados con arreglo a los citados artículos 33 y 34 del Reglamento.

El Encargado del tratamiento garantiza que también los Subencargados a los que recurre para la prestación del SERVICIO al CLIENTE/Responsable del tratamiento cumplan las obligaciones del presente artículo, obligándolos a comunicar al Encargado del tratamiento con prontitud y sin dilación indebida los eventuales incidentes de seguridad, tan pronto como tengan conocimiento de ellos, en la forma y en los plazos previstos en los respectivos acuerdos.

5.8 Asistencia para la obligación de comunicación de una violación de la seguridad de los datos personales al interesado

El Encargado del tratamiento tiene la obligación de asistir al Responsable del tratamiento en el cumplimiento de las obligaciones de comunicación de una violación de la seguridad de los datos personales al interesado, de conformidad con el art. 34 del GDPR; en todo caso, dicha comunicación deberá ser efectuada siempre por el Responsable del tratamiento.

5.9 Asistencia del Encargado del tratamiento en el cumplimiento de la obligación del Responsable del tratamiento de realizar la evaluación de impacto relativa a la protección de datos

El Encargado del tratamiento asistirá al Responsable del tratamiento en el cumplimiento de las obligaciones de análisis de riesgos y de evaluación de impacto relativa a la protección de datos, de conformidad con el art. 35 del GDPR, facilitando toda la información útil de que disponga a través del "Registro del tratamiento del servicio".

5.10 Asistencia del Encargado del tratamiento en el cumplimiento de la obligación del Responsable del tratamiento de realizar la consulta previa

El Encargado del tratamiento asiste al Responsable del tratamiento en la consulta previa a la autoridad de control, prevista en el art. 36 del GDPR, facilitando al Responsable toda la información útil de que disponga a través del "Registro del tratamiento del servicio".

5.11 Asistencia del Encargado del tratamiento en caso de inspecciones/requerimientos de la autoridad competente.

El Encargado del tratamiento asiste al Responsable del tratamiento y colabora con él en caso de inspecciones/requerimientos de la autoridad pública que puedan afectarle de algún modo.

En caso de inspecciones realizadas al Encargado del tratamiento que afecten al Responsable del tratamiento, se informará de inmediato al Responsable del tratamiento, siempre que ello sea posible en atención a los presupuestos de la investigación judicial que se lleve a cabo.

5.12 Plazos de conservación de los datos: supresión o devolución de todos los datos personales al término del encargo

Una vez finalizada la prestación de los servicios de tratamiento, el Encargado del tratamiento, a elección del Responsable del tratamiento, deberá devolver o suprimir todos los datos personales y suprimir las copias existentes.

Los datos en poder del Encargado del tratamiento deberán devolverse al Responsable del tratamiento, a petición de este, mediante las funciones de exportación de la plataforma, en formatos estructurados de uso común, antes de la finalización del contrato; y/o suprimirse en los plazos definidos en el "Registro del tratamiento del servicio".

Las eventuales copias de seguridad adicionales de dichos datos podrán conservarse durante el periodo adicional indicado en el "Registro del tratamiento del servicio", con fines exclusivamente de seguridad y sin que se destinen a la comunicación ni a la difusión.

No obstante lo indicado en los puntos anteriores, el Encargado del tratamiento deberá conservar los datos en los casos en que el Derecho de la Unión o de los Estados miembros prevea su conservación, en los términos impuestos por dicha normativa o por dichas disposiciones.

5.13 Puesta a disposición del Responsable del tratamiento de toda la información necesaria para demostrar el cumplimiento de las obligaciones

El Encargado del tratamiento pondrá a disposición del Responsable del tratamiento toda la información necesaria para demostrar el cumplimiento de las obligaciones previstas en el art. 28 del GDPR y debe permitir y contribuir a la realización de las auditorías, incluidas las inspecciones, por parte del Responsable del tratamiento o de otro sujeto designado por este, en los términos y en la forma que se definen con más detalle en el art. 8 siguiente, o por parte de las autoridades.

5.14 Caso en que una instrucción dada al Encargado del tratamiento se considere contraria al GDPR

Si el Encargado del tratamiento considera, en su opinión, que una instrucción del Responsable del tratamiento infringe el GDPR u otras disposiciones, nacionales o de la Unión, relativas a la protección de datos, deberá informar inmediatamente al Responsable del tratamiento.

5.15 Observancia de los principios de "privacy by design" y de "privacy by default"

En el desempeño del encargo, el Encargado del tratamiento deberá actuar observando los principios de protección de datos desde el diseño (privacy by design) y de protección de datos por defecto. Los SERVICIOS se prestan de forma estándar, igual para todos los clientes, y están diseñados conforme a estos principios.

6. Obligaciones del Responsable del tratamiento

6.1 El Responsable del tratamiento debe:

- facilitar al Encargado del tratamiento los datos previstos en el art. 4 de las presentes cláusulas;
- documentar por escrito todas las instrucciones relativas al tratamiento de los datos por parte del Encargado del tratamiento;
- velar, de forma previa y durante todo el tratamiento, por el cumplimiento de las obligaciones previstas en el reglamento europeo de protección de datos por parte del Encargado del tratamiento;
- supervisar el tratamiento, realizando auditorías e inspecciones.

7. Lugares en los que se conservan y se conservarán los datos

7.1 Los datos serán tratados por el Encargado del tratamiento en los lugares indicados en el "Registro del tratamiento del servicio". Si el tratamiento tuviera que realizarse en países no pertenecientes a la UE, el Encargado del tratamiento pondrá a disposición del Responsable del tratamiento las garantías adoptadas en función del lugar en que se lleve a cabo el tratamiento.

7.2 Si el Encargado del tratamiento estuviera obligado a efectuar una transferencia de datos a un tercer país o a una organización internacional en virtud del Derecho de la Unión o del Derecho del Estado miembro al que esté sujeto, deberá informar al Responsable del tratamiento de dicha exigencia legal antes de la transferencia con el fin de obtener autorización, salvo que el Derecho prohíba dicha información por razones importantes de interés público.

8. Controles

8.1 El Responsable del tratamiento se reserva la facultad de velar, también mediante verificaciones periódicas, por la estricta observancia de las disposiciones legales sobre el tratamiento de dichos datos y por el cumplimiento de sus instrucciones indicadas en el presente documento. El Encargado del tratamiento deberá permitir al Responsable del tratamiento, prestándole plena colaboración, verificaciones periódicas sobre la adecuación de las medidas de seguridad adoptadas y sobre el cumplimiento de la Normativa de Privacidad y de las disposiciones del propio Responsable del tratamiento.

8.2 Toda actividad de auditoría por parte del Responsable del tratamiento deberá acordarse con el Encargado del tratamiento, con un preaviso de al menos 10 días hábiles. Cuando dichas actividades conlleven cargas y gastos no previstos en el presente

contrato, todas las solicitudes del Responsable del tratamiento deberán acordarse en cuanto a sus modalidades de ejecución y gestionarse a nivel de proyecto, con la definición de una valoración, también económica, para su realización (ya se trate de actividades de pruebas de penetración, análisis de vulnerabilidades u otras).

8.3 Toda información compartida en cumplimiento de las obligaciones del Encargado del tratamiento o del Responsable del tratamiento se clasifica como confidencial y, por tanto, no podrá difundirse, comunicarse ni publicarse en la red sin la previa autorización escrita de la otra parte. Toda persona autorizada que trate la información habrá firmado un acuerdo de confidencialidad que establecerá la prohibición de comunicarla a sujetos no autorizados incluso después de la extinción de la relación laboral y hasta que la información sea de dominio público por causas no imputables a dichas personas. Toda vulneración de la confidencialidad de dicha información será sancionada en los términos legales y contractuales.

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

Traducción de cortesía del original italiano. En caso de diferencias, prevalece el texto italiano.

Autor	Oficina de Privacidad de Zucchetti Spa
Aprobación	Fabrizio Scuppa, representante legal de Octorate S.r.l.

Versión Revisión

Versión	Autor	Consulta al DPO	Fecha de emisión	Motivo de la revisión
0	Oficina de Privacidad		12/11/2026	Primera emisión

OCTORATE

ENCARGADO DEL TRATAMIENTO					
Denominación social	Octorate Srl				
N.° de IVA	13493861002				
Dirección	Via Filippo Caruso 23				
Ciudad	Roma	**C.P.**	00173	**Prov.**	RM
Representante Legal	Fabrizio Scuppa				

PERSONAS AUTORIZADAS PARA EL TRATAMIENTO
Personal de Octorate dedicado al soporte al cliente, al onboarding y a la formación, desarrolladores y técnicos de sistemas, autorizado e instruido para el tratamiento, con accesos limitados a sus funciones. Para OctoAgent, el equipo de desarrollo (4 personas) y el equipo de soporte (3 personas) de iManager S.r.l., Subencargado indicado entre los destinatarios.

DATOS DE CONTACTO			
Encargado del tratamiento	Octorate Srl	legal@octorate.com	06 4542 0568
Representante del encargado	N.A.		
Delegado de protección de datos (DPO)	DPO de Octorate	dpo@octorate.com	

DESCRIPCIÓN
Sistema de gestión de las reservas, de las tarifas y de la disponibilidad, distribución en los canales conectados, sitio web y booking engine, comunicaciones con los huéspedes, obligaciones ante la Polizia di Stato (policía italiana), el ISTAT (instituto italiano de estadística) y la Agenzia delle Entrate (agencia tributaria italiana), integraciones de pago, operativa diaria del establecimiento y, cuando esté activo, gestión automatizada de las conversaciones con OctoAgent.

FINALIDAD DEL TRATAMIENTO
Prestación de los Servicios de Octorate por cuenta del Cliente, es decir, gestión de las reservas, de las tarifas y

de la disponibilidad, distribución en los canales conectados, sitio web y booking engine, comunicaciones con los huéspedes, obligaciones ante la Polizia di Stato, el ISTAT y la Agenzia delle Entrate, integraciones de pago, operativa diaria del establecimiento y, cuando esté activo, gestión automatizada de las conversaciones con OctoAgent, junto con la asistencia y el mantenimiento de los Servicios.
Naturaleza del tratamiento. Recogida, registro, organización, estructuración, conservación, consulta, procesamiento, extracción, comunicación por transmisión a los destinatarios indicados por el Cliente, supresión. Para OctoAgent, también procesamiento automatizado mediante modelos de inteligencia artificial para generar respuestas, traducciones, resúmenes, transcripciones, clasificaciones e incidencias.
Duración y frecuencia. Durante toda la relación contractual, de forma continua. Los periodos de conservación por categoría se indican en los plazos para la supresión de los datos.

CATEGORÍA DE INTERESADOS

Huéspedes y personas que realizan la reserva, incluidos acompañantes y huéspedes menores de edad dentro de los límites de las obligaciones legales. Personas que contactan con el establecimiento para solicitar información o presupuestos. Usuarios de la cuenta del Cliente, es decir, titular, personal y colaboradores. Propietarios de las unidades gestionadas, en el caso de los property managers que utilizan el portal de propietarios. Proveedores y socios del Cliente que, en su caso, estén registrados en la plataforma.

CATEGORÍAS DE DATOS PERSONALES

Datos de reserva y de estancia. Nombre y apellidos, datos de contacto, idioma, nacionalidad, fechas de llegada y de salida, unidad y tipología, número y composición de los huéspedes, importes, canal de procedencia, preferencias y notas introducidas por el Cliente o por el huésped.
Datos para el cumplimiento de las obligaciones legales. Para las fichas de registro de huéspedes (schedine Alloggiati), datos identificativos, lugar y fecha de nacimiento, ciudadanía, tipo, número y lugar de expedición del documento de identidad. Para el ISTAT, datos estadísticos sobre los flujos. Para los documentos fiscales, datos fiscales de los huéspedes, código fiscal y número de IVA.
Datos de pago. Datos de la tarjeta de crédito obtenidos como garantía de la reserva, conservados cifrados conforme a los estándares PCI-DSS y que Octorate no puede descifrar directamente, resultados de las transacciones comunicados por las pasarelas y las entidades de pago.
Comunicaciones. Contenido y archivos adjuntos de los mensajes intercambiados con los huéspedes por correo electrónico, mensajería de los portales OTA, WhatsApp, SMS y chat del sitio web. Con OctoAgent, también las imágenes enviadas por los huéspedes, los resúmenes, las transcripciones y las grabaciones de audio de las llamadas cuando el módulo de voz está activo, las líneas de razonamiento del agente y las lecciones aprobadas por el Cliente.
Check-in online con OctoAgent. Imagen del documento de identidad enviada por el huésped para el check-in, de la que OctoAgent extrae los datos identificativos. La fotografía del documento se oculta antes del envío al modelo de inteligencia artificial.
Sitio web y booking engine. Datos de los visitantes y de las personas que reservan en el sitio web y en el

booking engine del Cliente, conforme a la política de privacidad y a la política de cookies del Cliente.
Usuarios de la cuenta. Nombre, correo electrónico, rol, credenciales, logs de acceso y de actividad, necesarios para el funcionamiento y la seguridad de la plataforma.
Categorías especiales de datos. No previstas por los Servicios. La información comunicada espontáneamente por los huéspedes, por ejemplo necesidades de salud, alimentarias o religiosas, se trata bajo la responsabilidad del Cliente.

NINGÚN USO PARA FINES PROPIOS

Octorate no utiliza los Datos del Cliente para fines propios. Octorate puede procesar datos de forma agregada y anónima, que no permiten identificar ni al Cliente ni a los interesados, con fines estadísticos, de seguridad y de mejora de los Servicios.

CATEGORÍA DE DESTINATARIOS A LOS QUE PODRÁN COMUNICARSE LOS DATOS

Lista de los Subencargados autorizados con carácter general por el Cliente, con el país y las garantías para la transferencia de los datos de cada proveedor. Los portales OTA, los organismos públicos, las pasarelas y las entidades de pago no son Subencargados y reciben los datos según se indica entre los sujetos que reciben los datos como responsables del tratamiento independientes.

- Aruba S.p.A. (Italia). Hosting, base de datos, almacenamiento y copias de seguridad de la plataforma Octorate (PMS, Channel Manager, Booking Engine). Garantía de transferencia dentro del EEE.
- Complior AB (antes 24 Solutions) (Suecia). Entorno certificado PCI DSS conectado a la plataforma para los datos de las tarjetas de crédito. Garantía de transferencia dentro del EEE.
- iManager S.r.l., Via del Muro Linari 31, 00173 Roma, código fiscal y n.º de IVA 16082961000 (Italia). Desarrollo, gestión y hosting de aplicaciones de la plataforma OctoAgent. Garantía de transferencia dentro del EEE.
- Google Cloud (Google Cloud EMEA Limited) (Irlanda, centro de datos de Milán). Hosting de OctoAgent. Garantía de transferencia dentro del EEE, cláusulas tipo para eventuales accesos desde terceros países.
- MongoDB Atlas (MongoDB Limited) (Irlanda, centros de datos de Milán y Fráncfort). Base de datos de OctoAgent y copias de seguridad. Garantía de transferencia dentro del EEE, cláusulas tipo para eventuales accesos desde terceros países.
- OpenAI (OpenAI Ireland Limited, parte contratante para el EEE) (Irlanda, tratamiento también en Estados Unidos). Modelos de inteligencia artificial de OctoAgent, generación de respuestas, resúmenes, transcripciones, extracción de los datos de los documentos, a través de la cuenta de iManager. Modelos de inteligencia artificial de las demás funciones de la plataforma Octorate, a través de la cuenta de Octorate. Garantía de transferencia Cláusulas tipo incluidas en el DPA de OpenAI, que no tiene la certificación DPF.
- Openapi S.r.l. (Openapi.com) (Italia). Envío de SMS a los huéspedes desde OctoAgent. Garantía de transferencia dentro del EEE.
- Better Stack (UE). Monitorización de la disponibilidad y alarmas de OctoAgent, región de datos UE,

solo si por los logs pasan datos personales. Garantía de transferencia dentro del EEE.

- Microsoft Clarity (Microsoft) (Irlanda, EE. UU.). Análisis del uso de la consola de OctoAgent por parte de los usuarios de los establecimientos, con enmascaramiento activo. Garantía de transferencia Adecuación (DPF) o cláusulas tipo.
- Meta (WhatsApp Business Platform) (Irlanda, EE. UU.). Mensajería de WhatsApp entre establecimientos y huéspedes. Garantía de transferencia Adecuación (DPF) o cláusulas tipo.
- Mailchimp Transactional (Mandrill, The Rocket Science Group LLC) y SparkPost (Bird) (EE. UU., UE). Servicios de envío de correo electrónico autorizados para el dominio octorate.com, para los correos electrónicos que no salen de los servidores de correo de Octorate. OctoAgent no los utiliza. Garantía de transferencia Adecuación (DPF) o cláusulas tipo.
- Mailgun (Mailgun Technologies, Inc., grupo Sinch) (EE. UU., UE). Servicio de envío de los correos electrónicos de los Servicios. Garantía de transferencia Cláusulas tipo.
- Intercom (Intercom R&D Unlimited Company) (Irlanda, EE. UU.). Chat de soporte de la plataforma Octorate, solo si pasan por él datos de los huéspedes. OctoAgent no lo utiliza. Garantía de transferencia Adecuación (DPF).

El servicio telefónico del módulo de voz de OctoAgent lo presta Vonage mediante un contrato a nombre del Cliente, activado por indicación de Octorate, por lo que Vonage no es un Subencargado de Octorate. Las modificaciones de esta lista se comunican al Cliente. La versión actualizada está disponible previa solicitud a legal@octorate.com.

TRANSFERENCIA DE DATOS AL EXTRANJERO

Los Datos del Cliente se conservan en centros de datos situados en la Unión Europea, indicados en las medidas de seguridad relativas al centro de datos.

Octorate transfiere Datos del Cliente a terceros países, también a través de Subencargados, únicamente de conformidad con el Capítulo V del GDPR, en virtud de una decisión de adecuación de la Comisión Europea, incluido el marco EU-US Data Privacy Framework para los proveedores certificados, o de las cláusulas contractuales tipo adoptadas mediante la Decisión de Ejecución (UE) 2021/914 de la Comisión, completadas con las medidas complementarias que en su caso sean necesarias. Las garantías aplicadas a cada Subencargado se indican en la lista de destinatarios. Para los modelos de inteligencia artificial de OctoAgent y de las demás funciones de la plataforma, los datos necesarios para la generación de los contenidos se transmiten a OpenAI, que los trata también en Estados Unidos en virtud de las cláusulas contractuales tipo incluidas en su acuerdo de tratamiento de datos.

Las transmisiones a portales OTA, pasarelas de pago, software de terceros conectado por el Cliente mediante API, huéspedes y otros destinatarios indicados por el Cliente, incluso situados en terceros países, se realizan siguiendo instrucciones del Cliente, que es responsable de ellas.

PLAZOS PARA LA SUPRESIÓN DE LOS DATOS

Datos de reserva, de estancia y datos identificativos de los huéspedes. Durante toda la vigencia del contrato y

hasta 30 días después de su finalización, salvo instrucción distinta del Cliente.
Mensajes y conversaciones con los huéspedes. Durante toda la vigencia del contrato, salvo supresión anticipada siguiendo instrucciones del Cliente.
Transcripciones, resúmenes y grabaciones de las llamadas, lecciones y líneas de razonamiento de OctoAgent. Durante toda la vigencia del contrato, salvo supresión anticipada siguiendo instrucciones del Cliente.
Datos enviados a los modelos de inteligencia artificial (OpenAI). No almacenados por el proveedor para usos posteriores. OpenAI los conserva hasta 30 días para el control de abusos y después los suprime.
Datos para las fichas Alloggiati, el ISTAT y los documentos fiscales. Durante el tiempo necesario para la transmisión y para cumplir las obligaciones de conservación previstas por la ley.
Logs técnicos y de seguridad. Para la plataforma Octorate, logs de las solicitudes HTTP 45 días y logs de los accesos de los administradores de sistemas al menos 6 meses, salvo obligaciones legales. Para OctoAgent, logs de aplicación 90 días y logs de auditoría 400 días. En los logs de OctoAgent no se registran los contenidos de los huéspedes, es decir, mensajes, correo electrónico, teléfono y documentos. Los logs técnicos de las solicitudes, conservados 400 días por motivos de seguridad, contienen la dirección IP de quien se conecta. A los logs accede únicamente el equipo de desarrollo de iManager.
Copias de seguridad. Sobrescritura automática según los ciclos indicados a continuación. Para OctoAgent, copias de seguridad diarias conservadas 7 días, semanales 4 semanas y copia diaria en Fráncfort conservada 90 días. Para la plataforma Octorate, copias de seguridad diarias conservadas 30 días.
Antes de la finalización del contrato, el Cliente puede exportar los Datos del Cliente mediante las funciones de exportación de la plataforma, en formatos estructurados de uso común. Previa solicitud escrita recibida antes de la finalización, Octorate presta asistencia para la devolución de los datos que no pueden exportarse de forma autónoma, a cambio de las contraprestaciones que en su caso se acuerden.
En un plazo de 30 días desde la finalización del contrato, Octorate suprime los Datos del Cliente y las copias existentes, salvo las copias de seguridad, que se sobrescriben de forma rotatoria como se indica más arriba, y salvo los datos que Octorate debe conservar por obligaciones legales, entre ellos los documentos fiscales y los logs exigidos por la normativa, que se conservan durante el tiempo prescrito y después se suprimen. Las solicitudes de supresión recibidas durante la relación contractual se ejecutan en un plazo de 5 días hábiles, según lo previsto en los Términos y Condiciones. Previa solicitud, Octorate certifica por escrito que la supresión se ha efectuado.

SUJETOS QUE RECIBEN LOS DATOS COMO RESPONSABLES DEL TRATAMIENTO INDEPENDIENTES

Los portales OTA, las pasarelas y las entidades de pago, la Polizia di Stato, el ISTAT, la Agenzia delle Entrate y los demás sujetos a los que los Servicios transmiten datos siguiendo instrucciones del Cliente tratan los datos como responsables del tratamiento independientes o conforme a sus respectivos acuerdos con el Cliente. Octorate se limita a la transmisión técnica y no responde del tratamiento realizado por dichos sujetos. Lo mismo vale para Vonage, que presta el servicio telefónico del módulo de voz de OctoAgent mediante un contrato a nombre del Cliente.

REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO

Octorate lleva el registro de las categorías de actividades de tratamiento efectuadas por cuenta de los clientes con arreglo al artículo 30, apartado 2, del GDPR y lo pone a disposición del Cliente previa solicitud a legal@octorate.com.

DESCRIPCIÓN GENERAL DE LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD

1. MEDIDAS DE SEGURIDAD IMPLEMENTADAS EN EL SOFTWARE

Medidas de seguridad adoptadas en la plataforma Octorate y en OctoAgent.

- Gestión de las credenciales de acceso

• Credenciales personales para cada usuario, reglas sobre la robustez de las contraseñas, bloqueo de los accesos no autorizados y registro de los accesos.
• Autenticación de dos factores con código OTP para la plataforma Octorate y para el acceso a OctoAgent con credenciales de Octorate.
• OctoAgent prevé también un acceso interno para el personal operativo del establecimiento que no tiene una cuenta de usuario de Octorate, por ejemplo quien atiende el teléfono, mantenimiento y limpieza, sin autenticación de dos factores y no destinado a usuarios con facultades de administrador. La extensión de la autenticación de dos factores a los usuarios internos se está evaluando con el proveedor.

- Minimización

• Roles y permisos configurables por el Cliente, para limitar el acceso a los datos a las funciones de cada usuario.
- Identificación de quien tiene acceso al sistema
• Logs técnicos que permiten reconstruir las actividades realizadas en la plataforma. Para OctoAgent, logs de aplicación conservados 90 días, logs de auditoría y logs técnicos de las solicitudes conservados 400 días, sin los contenidos de los huéspedes. Los logs técnicos contienen la dirección IP de quien se conecta y solo son accesibles para el equipo de desarrollo de iManager. Para la plataforma Octorate, logs de las solicitudes HTTP conservados 45 días. Los accesos de los administradores de sistemas se registran de forma no modificable y los logs correspondientes se conservan al menos 6 meses, según lo previsto en la resolución del Garante (autoridad italiana de protección de datos) sobre los administradores de sistemas.
• Accesos del personal de asistencia a la cuenta del Cliente conforme a las medidas para los servicios de asistencia indicadas más adelante.

- Técnicas de cifrado

• Transmisión de los datos con protocolo TLS en todos los Servicios.
• Datos de las tarjetas de crédito conservados cifrados conforme al estándar PCI DSS, que Octorate no puede descifrar directamente.
• Cifrado de los datos en reposo en las bases de datos de la plataforma Octorate y de OctoAgent.

- Privacy by default

• Servicios prestados de forma estándar, igual para todos los clientes, y diseñados conforme a los principios de protección de datos desde el diseño y por defecto. Separación lógica de los datos de los distintos clientes en la plataforma.

- Derechos de los interesados

• El Cliente puede exportar los datos de la plataforma en formatos estructurados de uso común. Octorate asiste al Cliente para responder a las solicitudes de los interesados. Las solicitudes de supresión recibidas durante la relación contractual se ejecutan en un plazo de 5 días hábiles.

2. ENCARGADO DEL TRATAMIENTO: MEDIDAS DE SEGURIDAD IMPLEMENTADAS PARA LOS SERVICIOS DE ASISTENCIA

Octorate presta asistencia a los Clientes de forma remota, a través del chat de la plataforma, el correo electrónico y el teléfono, con personal autorizado e instruido para el tratamiento. Las solicitudes recibidas por chat y por correo electrónico se registran como tickets en Intercom, indicado entre los destinatarios. Cuando es necesario para resolver la solicitud, el personal de asistencia accede a la cuenta del Cliente desde el panel interno de Octorate, con credenciales personales y sin utilizar la contraseña del Cliente. Octorate no se conecta a los dispositivos del Cliente con programas de control remoto.

El personal de asistencia trata los datos del Cliente únicamente para resolver la solicitud. Los archivos y las exportaciones para la asistencia se reciben del Cliente como archivos adjuntos en el chat de la plataforma y se utilizan únicamente para esa solicitud. Permanecen adjuntos a la conversación en Intercom durante la vigencia del contrato. Se suprimen en los plazos indicados en este Registro para los Datos del Cliente, es decir, en un plazo de 30 días desde la finalización del contrato, salvo las obligaciones de conservación previstas por la ley, o antes a petición del Cliente.

3. ENCARGADO DEL TRATAMIENTO: MEDIDAS DE SEGURIDAD RELATIVAS AL CENTRO DE DATOS

Plataforma Octorate. Infraestructura en Aruba S.p.A., en centros de datos situados en Italia con certificación ISO/IEC 27001, 27017, 27018 y ANSI/TIA-942 Rating 4. Copias de seguridad diarias de la base de datos conservadas 30 días, con procedimientos de restauración.
Tarjetas de crédito. Datos de las tarjetas de crédito en un entorno certificado PCI DSS en Complior AB, Suecia.
OctoAgent. Desde el 20 de octubre de 2026, hosting en Google Cloud en Milán con base de datos MongoDB Atlas en Milán y duplicado de las copias de seguridad en Fráncfort, en sustitución de Scaleway en París, donde los datos se suprimieron tras la migración. Proveedores con certificaciones ISO/IEC 27001 y SOC 2. Copias de seguridad diarias conservadas 7 días, semanales 4 semanas y copia diaria en Fráncfort conservada 90 días.
Correos electrónicos del sistema. Los correos electrónicos del sistema de la plataforma salen de los servidores de correo de Octorate alojados por Aruba o de los servicios de envío de correo electrónico indicados entre los destinatarios.

4. MEDIDAS DE SEGURIDAD BÁSICAS NIS2

Octorate forma parte del Grupo Zucchetti, entidad esencial con arreglo a la Normativa NIS2, y aplica las medidas de seguridad básicas definidas por la ACN (agencia italiana de ciberseguridad) según el modelo del Grupo. Los puntos siguientes recogen, para cada área prevista en el modelo, las medidas adoptadas por Octorate para los Servicios.

Fiabilidad de los proveedores. Octorate trata los Datos del Cliente únicamente con los Subencargados indicados entre los destinatarios, vinculados por acuerdos conformes con el artículo 28 y elegidos entre proveedores con certificaciones de seguridad reconocidas (ISO/IEC 27001, SOC 2, PCI DSS). Cada nuevo proveedor es evaluado antes de su uso y comunicado al Cliente. Octorate participa en el proceso de homologación de proveedores del Grupo Zucchetti a través de la persona de referencia del grupo.

Funciones y responsabilidades. Delegado de protección de datos disponible en dpo@octorate.com. Personas de referencia internas para la seguridad y los incidentes indicadas en el procedimiento de gestión de incidentes. Para las obligaciones NIS2, Octorate se remite al punto de contacto NIS y a la persona de referencia CSIRT designados por el Grupo Zucchetti para el sector hospitality, con su correspondiente sustituto, indicados en el procedimiento de gestión de incidentes.

Fiabilidad de los recursos humanos. Personal autorizado para el tratamiento, instruido sobre la Normativa aplicable y sujeto a confidencialidad, con accesos limitados a sus funciones y revocados al finalizar la relación.

Conformidad y auditoría. Información y verificaciones a disposición del Cliente previa solicitud. Infraestructuras en proveedores certificados y sometidos a auditorías de terceros, en particular Aruba S.p.A. (ISO/IEC 27001, 27017, 27018 y ANSI/TIA-942 Rating 4), Complior AB (PCI DSS), Google Cloud y MongoDB (ISO/IEC 27001 y SOC 2).

Gestión de las vulnerabilidades. Actualizaciones y correcciones de seguridad aplicadas con prioridad. Para OctoAgent, escaneo de vulnerabilidades y revisión de la configuración de la nueva infraestructura a más tardar el 30 de noviembre de 2026, primera prueba de penetración externa a más tardar el 31 de marzo de 2027 y después una vez al año, con gestión de los resultados y de las correcciones. Para la plataforma Octorate, pruebas de vulnerabilidad y pruebas de penetración en el marco del programa del Grupo Zucchetti, en el que Octorate está incluida a través de la persona de referencia del grupo.

Continuidad operativa y recuperación ante desastres. Copias de seguridad de la plataforma Octorate diarias y conservadas 30 días, con procedimientos de restauración. Para OctoAgent, copias de seguridad diarias conservadas 7 días, semanales 4 semanas y copia diaria en Fráncfort conservada 90 días. Centros de datos con certificación ANSI/TIA-942 Rating 4 para la plataforma Octorate. Monitorización continua de la disponibilidad de los Servicios.

Gestión de identidades y accesos. Credenciales personales, mínimo privilegio con roles y permisos configurados por el Cliente, reglas sobre la robustez de las contraseñas, bloqueo de los accesos no autorizados, registro de los accesos y revisión de las cuentas de usuario. Autenticación de dos factores con código OTP para la plataforma Octorate y para el acceso a OctoAgent con credenciales de Octorate. Acceso interno a OctoAgent para el personal operativo del establecimiento con los límites indicados en las medidas de seguridad implementadas en el software. Accesos técnicos y administrativos a la infraestructura de OctoAgent a través de la consola del proveedor de nube con autenticación de dos factores, en una red privada no expuesta a internet, con el servidor de acceso a la base de datos encendido solo cuando es necesario. Accesos y modificaciones administrativas registrados y monitorizados.

Seguridad física. Datos conservados exclusivamente en los centros de datos de los proveedores indicados

en este Registro, con el control de los accesos físicos previsto en las certificaciones de los proveedores.
Formación y concienciación. Formación del personal sobre la protección de los datos personales y sobre la seguridad informática, con contenidos diferenciados para el personal general, el personal técnico y la dirección según el programa del Grupo Zucchetti, en el que Octorate está incluida a través de la persona de referencia del grupo.
Seguridad de los datos. Transmisión con protocolo TLS, cifrado de los datos en reposo en las bases de datos de la plataforma Octorate y de OctoAgent, datos de las tarjetas de crédito en un entorno certificado PCI DSS, separación lógica de los datos de los clientes, copias de seguridad conservadas en la Unión Europea, supresión segura a la finalización del contrato.
Protección de las redes y de las comunicaciones. Protección perimetral de los proveedores de hosting, infraestructura de OctoAgent serverless en una red privada no expuesta a internet, firewall de aplicaciones en OctoAgent con registro de los bloqueos, canales de comunicación oficiales con el Cliente (correo electrónico de la cuenta y avisos en la plataforma) utilizados también para las comunicaciones sobre los incidentes.
Monitorización de los eventos. Para OctoAgent, control cada minuto de la disponibilidad del servicio desde el exterior, de los errores de aplicación, de los tiempos de respuesta, de los errores hacia Octorate y hacia los proveedores de los modelos, de la memoria y las colas de trabajo, de los bloqueos del firewall de aplicaciones y de los accesos y las modificaciones administrativas, con alarmas al equipo técnico. Logs de aplicación conservados 90 días, logs de auditoría y logs técnicos de las solicitudes 400 días, sin los contenidos de los huéspedes. Los logs técnicos contienen la dirección IP de quien se conecta y solo son accesibles para el equipo de desarrollo de iManager. Para la plataforma Octorate, logs de las solicitudes HTTP conservados 45 días y logs de los accesos de los administradores de sistemas, no modificables, conservados al menos 6 meses.
Gestión y notificación de los incidentes. Procedimiento escrito para detectar, evaluar, contener y comunicar los incidentes. El proveedor que gestiona OctoAgent avisa a Octorate en un plazo de 12 horas desde la detección de un incidente que afecte a los datos o al servicio, incluso con información parcial, con actualización y análisis en un plazo de 48 horas e informe final en un plazo de 20 días, de modo que el Grupo pueda cumplir los plazos de 72 horas y de un mes ante el CSIRT Italia. Octorate notifica la violación de la seguridad al Cliente en un plazo de 48 horas desde que tiene conocimiento de ella y, para los incidentes significativos con arreglo a la Normativa NIS2, activa a la persona de referencia del Grupo Zucchetti para la notificación al CSIRT Italia, con alerta temprana en un plazo de 24 horas y notificación en un plazo de 72 horas.
Desarrollo seguro. Desarrollo conforme a prácticas de seguridad desde el diseño, actualizaciones y correcciones de seguridad, entornos de desarrollo y de producción separados y lanzamientos controlados.
Mantenimiento ordinario y evolutivo. Actualizaciones y nuevas funcionalidades lanzadas mediante un proceso de gestión de cambios y comunicadas al Cliente conforme a la sección Evolución y modificación de los servicios de los Términos y Condiciones. Para OctoAgent, migración de la infraestructura completada el 20 de octubre de 2026, con revisión de la configuración a más tardar el 30 de noviembre de 2026.
Retirada. Supresión de los Datos del Cliente en un plazo de 30 días desde la finalización del contrato y en un plazo de 5 días hábiles previa solicitud, como se indica en los plazos para la supresión de los datos, con sobrescritura rotatoria de las copias de seguridad. Retirada segura de los soportes a cargo de los proveedores de infraestructura conforme a sus respectivas certificaciones.
Subcontratación y cadena de suministro. Lista de los Subencargados entre los destinatarios, con obligaciones contractuales equivalentes a las de la designación como encargado del tratamiento, incluidas las medidas de seguridad básicas NIS2 aplicables, y con la posibilidad de que el Cliente se oponga a las

modificaciones en un plazo de 15 días desde la comunicación.