BESTELLUNG ZUM AUFTRAGSVERARBEITER
- Data Processing Agreement -
(Art. 28 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016)

PRÄAMBEL

a. Zwischen dem KUNDEN und dem ANBIETER, der in dem Vertrag genannt ist, auf den sich dieses Dokument bezieht (im Folgenden ANBIETER), besteht ein Vertrag über die Erbringung von IT-Diensten und/oder damit verbundenen Diensten (im Folgenden DIENST und/oder DIENSTE), dessen integraler Bestandteil die vorliegende Bestellung ist;

b. in diesem Vertrag bezeichnen die Parteien einvernehmlich
- mit dem Begriff „GDPR" die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und
- mit dem Begriff „Datenschutzvorschriften" die Bestimmungen der GDPR sowie alle sonstigen Bestimmungen des Unionsrechts oder des Rechts der Mitgliedstaaten zum Schutz personenbezogener Daten und zu deren freiem Verkehr.

c. bei der Durchführung des DIENSTES ist der KUNDE Verantwortlicher für die Verarbeitung der personenbezogenen Daten im Sinne und für die Zwecke von Art. 4 Abs. 1 Nr. 7 GDPR, und ihm obliegt die Vornahme aller Handlungen, die die Datenschutzvorschriften für die Verarbeitung personenbezogener Daten vorsehen, das heißt die Datenschutzinformation, die Einholung der Einwilligung, das Ergreifen aller Maßnahmen zur Befugniserteilung, Beauftragung und Aufbewahrung sowie sonstiger Maßnahmen, auch zur Einrichtung des Sicherheitssystems, einschließlich der entsprechenden Maßnahmen;

Dies vorausgeschickt, wird zwischen den Parteien

VEREINBART UND FESTGELEGT

wie nachstehend aufgeführt.

1. Bestellung zum Auftragsverarbeiter

1.1 Für die Aufgaben, die dem ANBIETER auf der Grundlage des Vertrags über den DIENST übertragen werden, wird dieser gemäß Art. 4 Abs. 1 Nr. 8 und Art. 28 GDPR zum Auftragsverarbeiter bestellt.

1.2 Der Auftragsverarbeiter erklärt, hinreichende Garantien dafür bieten zu können, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der GDPR erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet.

2. Gegenstand des DPA

2.1 Gegenstand dieser Bestellung ist die Festlegung der Modalitäten und Vertragsbedingungen, zu denen sich der Auftragsverarbeiter verpflichtet, im Auftrag des Verantwortlichen die Vorgänge zur Verarbeitung personenbezogener Daten durchzuführen, wie sie im Vertrag definiert und in der technischen Anlage „Verarbeitungsverzeichnis des Dienstes" näher bezeichnet sind, die auf Anfrage des Verantwortlichen zur Verfügung gestellt wird.

2.2 Im Rahmen ihrer Vertragsbeziehungen verpflichten sich die Parteien, die geltenden, auf die Verarbeitung personenbezogener Daten anwendbaren Vorschriften einzuhalten, insbesondere die GDPR und die Datenschutzvorschriften.

3. Laufzeit des DPA

Diese Bestellung hat dieselbe Laufzeit wie der Vertrag, auf den sie sich bezieht.

4. Beschreibung der Leistungen des Auftragsverarbeiters

4.1 Der Auftragsverarbeiter ist befugt, im Auftrag des Verantwortlichen die personenbezogenen Daten zu verarbeiten, die für die Erbringung des DIENSTES gemäß dem Vertrag erforderlich sind. Für die Daten, die der Verantwortliche bereits bereitgestellt hat und noch bereitstellen wird, gewährleistet dieser, über eine geeignete Rechtsgrundlage im Sinne von Art. 6 GDPR zu verfügen, etwa den Vertrag mit dem Gast, die gesetzlichen Pflichten in den Bereichen öffentliche Sicherheit, Statistik und Steuern und, soweit erforderlich, die Einwilligung.

Der Verantwortliche gewährleistet dem Auftragsverarbeiter, rechtmäßig über alle Informationen zu verfügen, die er dem Auftragsverarbeiter zur Verarbeitung anvertraut, und sichert außerdem zu, dass diese Informationen in keiner Weise Rechte Dritter verletzen.

Der Verantwortliche behält die Inhaberschaft an den Informationen, die dem Auftragsverarbeiter für den DIENST mitgeteilt werden, übernimmt ausdrücklich die umfassende Verantwortung für den Inhalt der betreffenden personenbezogenen Daten und stellt den Auftragsverarbeiter von jeder Pflicht und/oder Last zur unmittelbaren und mittelbaren Prüfung und/oder Kontrolle in dieser Hinsicht frei.

4.2 Die Art der an den Daten vorgenommenen Vorgänge besteht in der Erbringung des DIENSTES und/oder der im Vertrag genannten DIENSTE, weshalb der Verantwortliche erklärt, die entsprechende Verarbeitung der Daten dem Auftragsverarbeiter zu übertragen.

4.3 Der Zweck der Verarbeitung, die Art und die Typologie der verarbeiteten Daten sowie die Kategorien betroffener Personen sind diejenigen, die im „Verarbeitungsverzeichnis des Dienstes" angegeben sind.

4.4 Soweit es in seine Zuständigkeit fällt, führt der Auftragsverarbeiter bei der Verarbeitung der Daten für die Erbringung des DIENSTES die Verarbeitung unter Beachtung von Art. 5 GDPR über die „Grundsätze für die Verarbeitung personenbezogener Daten" durch.

4.5 Für die Ausführung des Auftrags, der Gegenstand dieses Vertrags ist, stellt der Verantwortliche dem Auftragsverarbeiter die Informationen zur Verfügung, die für die Ausführung der Tätigkeiten für den DIENST erforderlich sind, auch solche, die auf die sachgerechte Nutzung des Informationssystems gerichtet sind.

4.6 Der Auftragsverarbeiter bestimmt und beauftragt gemäß Art. 28 Abs. 3 Buchst. b GDPR schriftlich seine befugten Personen und legt dabei den zulässigen Verarbeitungsumfang genau fest. Der Auftragsverarbeiter erklärt, sich bewusst zu sein, dass seine befugten Personen unter seiner Aufsicht handeln.

5. Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich, bei der Wahrnehmung seiner Aufgaben die folgenden Pflichten zu erfüllen und einzuhalten.

5.1 <u>Einhaltung der Weisungen des Verantwortlichen</u>

a. Der Auftragsverarbeiter darf die Daten nur für die oben genannten Zwecke und für die Erbringung der vertraglichen Leistungen verarbeiten.

b. Der Auftragsverarbeiter hat die Daten gemäß den Vorgaben im „Verarbeitungsverzeichnis des Dienstes" zu verarbeiten, und der Verantwortliche erachtet die dort vorgesehenen Sicherheitsmaßnahmen als angemessen.

5.2 <u>Gewährleistung der Vertraulichkeit</u>

a. Der Auftragsverarbeiter gewährleistet die Wahrung der Vertraulichkeit der im Rahmen dieser Bestellung verarbeiteten personenbezogenen Daten.

b. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und dass sie die erforderliche Schulung zur Verarbeitung personenbezogener Daten erhalten.

5.3 Ergreifen der Maßnahmen zur Sicherheit der Verarbeitung

a. Der Auftragsverarbeiter muss die Verarbeitung der personenbezogenen Daten unter Anwendung der nach Art. 32 GDPR erforderlichen Maßnahmen durchführen. Die getroffenen Sicherheitsmaßnahmen sind diejenigen, die im „Verarbeitungsverzeichnis des Dienstes“ angegeben sind. Der Verantwortliche nimmt zur Kenntnis, dass der Auftragsverarbeiter die Verarbeitung in einigen Fällen mit den vom Verantwortlichen bereitgestellten und konfigurierten Instrumenten durchführt und daher nur dann alle erforderlichen Vorkehrungen treffen muss, wenn die Verarbeitung außerhalb der Kontrolle des vom Verantwortlichen eingerichteten und konfigurierten Instruments erfolgt.

b. Ist der Auftragsverarbeiter Verhaltensregeln beigetreten oder hat er eine Zertifizierung vorgelegt, muss er unter Anwendung der Sicherheitsmaßnahmen arbeiten, die in den Verhaltensregeln oder in den der Zertifizierung zugrunde liegenden Protokollen vorgesehen sind. In diesem Fall akzeptiert der Verantwortliche die Zertifizierung als Nachweis dafür, dass der Auftragsverarbeiter in Bezug auf die durchgeführte Verarbeitung geeignete Maßnahmen getroffen hat, und verzichtet darauf, Audits der Systeme und Verfahren des ANBIETERS durchzuführen.

c. In den in Art. 37 GDPR vorgesehenen Fällen bedient sich der Auftragsverarbeiter seines Datenschutzbeauftragten (DSB oder DPO): Sofern ein solcher benannt ist, sind seine Kontaktdaten im „Verarbeitungsverzeichnis des Dienstes“ angegeben.

d. Gemäß Art. 30 GDPR muss der Auftragsverarbeiter (und gegebenenfalls sein Vertreter, sofern er nicht unter die Ausnahmen nach Absatz 5 dieses Artikels fällt) ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung führen, das die in Abs. 2 dieses Artikels genannten Angaben enthält.

e. Die genannten Verzeichnisse werden schriftlich geführt, auch in elektronischem Format, und dem Verantwortlichen auf dessen Anfrage zur Verfügung gestellt.

5.4 Bestellung von Unterauftragsverarbeitern

a. Gemäß Art. 28 Abs. 2 GDPR erteilt der Verantwortliche dem Auftragsverarbeiter mit dieser Bestellung die ausdrückliche allgemeine schriftliche Genehmigung, weitere Stellen zu bestimmen, die im Auftrag des Auftragsverarbeiters die Rolle von Unterauftragsverarbeitern wahrnehmen. Im Gegenzug zu dieser Genehmigung verpflichtet sich der Auftragsverarbeiter, dem Verantwortlichen die Liste aller gegebenenfalls als Unterauftragsverarbeiter bestimmten Stellen mitzuteilen. Kommt es im Laufe der Zeit zu Änderungen, Hinzufügungen oder Ersetzungen der ursprünglich mitgeteilten Unterauftragsverarbeiter, sind diese neuen Bestellungen dem Verantwortlichen mitzuteilen, der ab Erhalt der Mitteilung 15 Tage Zeit hat, um unter Angabe der Gründe für seinen Einspruch etwaige Einsprüche zu erheben. Kann keine einvernehmliche Lösung gefunden werden, kann der Kunde/Verantwortliche den Vertrag über den genutzten Dienst zu den darin vorgesehenen Bedingungen kündigen. Der Auftragsverarbeiter erklärt und gewährleistet, dass die Unterauftragsverarbeiter hinreichende Garantien dafür bieten, technische und organisatorische Maßnahmen durchzuführen, die geeignet sind, die Einhaltung der Bestimmungen der geltenden Datenschutzvorschriften zu gewährleisten, und verpflichtet sich, die weiteren Auftragsverarbeiter vertraglich zur Einhaltung derselben Pflichten zum Schutz personenbezogener Daten zu verpflichten, die der Auftragsverarbeiter gegenüber dem KUNDEN übernommen hat.

b. Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen weiterhin in vollem Umfang für die Erfüllung der Pflichten des Unterauftragsverarbeiters.

c. Es wird klargestellt, dass der ANBIETER in allen Fällen, in denen der DIENST nicht unmittelbar für den KUNDEN, sondern für dessen Endkunden erbracht wird, als weiterer Auftragsverarbeiter gilt und verpflichtet ist, die Daten zu denselben Bedingungen zu verarbeiten, die in dieser Bestellung für den Auftragsverarbeiter festgelegt sind.

5.5 Unterstützung des Verantwortlichen bei der Ausübung der Rechte der betroffenen Personen

a. Soweit möglich, muss der Auftragsverarbeiter – unter Berücksichtigung der Art der Verarbeitung – den Verantwortlichen unterstützen, damit dieser den Anträgen auf Ausübung der in Kapitel III GDPR genannten Rechte der betroffenen Person nachkommen kann.

Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen.

b. Was das Informationsrecht der betroffenen Personen angeht, obliegt es dem Verantwortlichen, den betroffenen Personen zum Zeitpunkt der Erhebung der Daten die Informationen gemäß Art. 13 und 14 GDPR zu den Verarbeitungsvorgängen zu erteilen.

Erhält der Auftragsverarbeiter unmittelbar Anträge einer betroffenen Person zu der im Auftrag des KUNDEN durchgeführten Verarbeitung personenbezogener Daten, fordert er die betroffene Person auf, sich an den KUNDEN als Verantwortlichen zu wenden, und teilt diesem den von der betroffenen Person erhaltenen Antrag unverzüglich mit, innerhalb von 10 Arbeitstagen nach dessen Eingang.

5.6 Unterstützung des Verantwortlichen bei der Einhaltung der Pflichten nach den Artikeln 32 bis 36 GDPR

a. Der Auftragsverarbeiter muss den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten nach den Art. 32 bis 36 GDPR unterstützen, das heißt:

- Artikel 32. Sicherheit der Verarbeitung;
- Artikel 33. Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde;
- Artikel 34. Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person;
- Artikel 35. Datenschutz-Folgenabschätzung;
- Artikel 36. Vorherige Konsultation.

b. Unterstützung bei der Sicherheit der Verarbeitung – Der Auftragsverarbeiter ist verpflichtet, den Verantwortlichen gemäß Art. 32 GDPR bei der Umsetzung der Sicherheit der Verarbeitung zu unterstützen.

Der Auftragsverarbeiter berichtet auf Anfrage des Verantwortlichen über die getroffenen Sicherheitsmaßnahmen, auch mittels etwaiger Fragebögen und Checklisten, gegebenenfalls nach vorheriger Bewertung auf Projektebene.

c. Besondere, bereits bestehende Sicherheitsmaßnahmen des Auftragsverarbeiters – Der Verantwortliche nimmt zur Kenntnis, dass der Auftragsverarbeiter für den DIENST über angemessene Sicherheitsmaßnahmen im Einklang mit der GDPR verfügt.

Systemadministratoren. In Bezug auf die Tätigkeiten des Auftragsverarbeiters, die die Speicherung der personenbezogenen Daten betreffen, und auf die systemtechnischen Tätigkeiten zur Wartung des Netzes und zur Aktualisierung der zugehörigen Datenbanken und Betriebssysteme haben die Mitarbeiter des Auftragsverarbeiters die Funktion von Systemadministratoren.

Die vom Garante per la privacy (italienische Datenschutzbehörde) in der Verfügung vom 27. November 2008 vorgesehenen Pflichten werden vom Auftragsverarbeiter erfüllt; insbesondere obliegt es dem Auftragsverarbeiter, die persönlichen Eigenschaften der Systemadministratoren zu beurteilen, die individuellen Bestellungen vorzunehmen, die von ihnen ausgeführten Tätigkeiten zu überprüfen und für die Protokollierung der entsprechenden Zugriffe zu sorgen. In Bezug auf die Vorgaben dieser Verfügung verpflichtet sich der Auftragsverarbeiter, dem Verantwortlichen die aktuelle Liste der Systemadministratoren mitzuteilen; die Mitteilung dieser Daten kann in elektronischer Form oder auf Papier erfolgen, und der Verantwortliche betrachtet diese Pflicht auch dann als erfüllt, wenn die aktuelle Liste der Namen dieser Systemadministratoren auf Anfrage des Verantwortlichen lediglich zur Verfügung gestellt wird.

5.7 Unterstützung bei der Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

Der Auftragsverarbeiter ist verpflichtet, den Verantwortlichen bei der Erfüllung seiner Pflichten zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde gemäß Art. 33 GDPR zu unterstützen. Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten spätestens 48 Stunden, nachdem sie ihm bekannt geworden ist. Dieser Meldung sind die in Abs. 3 des Art. 33 ausdrücklich genannten Angaben beizufügen, die dem Verantwortlichen ermöglichen, diese Verletzung erforderlichenfalls der zuständigen Aufsichtsbehörde zu melden.

Es obliegt nämlich ausschließlich dem Kunden, soweit er Verantwortlicher ist, festzustellen, ob der Vorfall als Data Breach einzustufen ist und ob das Risiko für die betroffenen Personen so hoch ist, dass die Meldung an die Aufsichtsbehörde und die Benachrichtigung der betroffenen Personen gemäß den genannten Artikeln 33 und 34 der Verordnung erforderlich sind.
Der Auftragsverarbeiter stellt sicher, dass die Pflichten dieses Artikels auch von den Unterauftragsverarbeitern eingehalten werden, deren er sich für die Erbringung des DIENSTES an den KUNDEN/Verantwortlichen bedient, indem er sie verpflichtet, dem Auftragsverarbeiter etwaige Sicherheitsvorfälle rechtzeitig und ohne ungerechtfertigte Verzögerung mitzuteilen, sobald sie ihnen bekannt geworden sind, und zwar in der Weise und innerhalb der Fristen, die in den jeweiligen Vereinbarungen vorgesehen sind.

5.8 Unterstützung bei der Pflicht zur Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person
Der Auftragsverarbeiter ist verpflichtet, den Verantwortlichen bei der Erfüllung der Pflichten zur Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person gemäß Art. 34 GDPR zu unterstützen; diese Benachrichtigung ist jedoch in jedem Fall stets vom Verantwortlichen vorzunehmen.

5.9 Unterstützung durch den Auftragsverarbeiter bei der Erfüllung der Pflicht des Verantwortlichen zur Datenschutz-Folgenabschätzung
Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung der Pflichten zur Risikoanalyse und zur Datenschutz-Folgenabschätzung gemäß Art. 35 GDPR, indem er über das „Verarbeitungsverzeichnis des Dienstes“ alle ihm vorliegenden zweckdienlichen Informationen bereitstellt.

5.10 Unterstützung durch den Auftragsverarbeiter bei der Erfüllung der Pflicht des Verantwortlichen zur vorherigen Konsultation
Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der in Art. 36 GDPR vorgesehenen vorherigen Konsultation der Aufsichtsbehörde, indem er dem Verantwortlichen über das „Verarbeitungsverzeichnis des Dienstes“ alle ihm vorliegenden zweckdienlichen Informationen bereitstellt.

5.11 Unterstützung durch den Auftragsverarbeiter bei Inspektionen/Anfragen der zuständigen Behörde.
Der Auftragsverarbeiter unterstützt den Verantwortlichen und arbeitet mit ihm zusammen bei Inspektionen/Anfragen der Behörden, die ihn in irgendeiner Weise betreffen können.
Bei Inspektionen beim Auftragsverarbeiter, die den Verantwortlichen betreffen, wird der Verantwortliche unverzüglich benachrichtigt, sofern dies im Hinblick auf die Voraussetzungen der durchgeführten gerichtlichen Ermittlung möglich ist.

5.12 Aufbewahrungsfristen der Daten: Löschung oder Rückgabe aller personenbezogenen Daten nach Beendigung des Auftrags
Nach Abschluss der Erbringung der Verarbeitungsleistungen muss der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten zurückgeben oder löschen und die vorhandenen Kopien löschen.
Die im Besitz des Auftragsverarbeiters befindlichen Daten sind dem Verantwortlichen auf dessen Anfrage vor der Beendigung über die Exportfunktionen der Plattform in gängigen strukturierten Formaten zurückzugeben; und/oder innerhalb der im „Verarbeitungsverzeichnis des Dienstes“ festgelegten Fristen zu löschen.
Etwaige weitere Backup-Kopien dieser Daten können für den im „Verarbeitungsverzeichnis des Dienstes“ angegebenen weiteren Zeitraum ausschließlich zu Sicherheitszwecken aufbewahrt werden und sind nicht zur Weitergabe und Verbreitung bestimmt.
Abweichend von den vorstehenden Punkten muss der Auftragsverarbeiter die Daten in den Fällen aufbewahren, in denen das Unionsrecht oder das Recht der Mitgliedstaaten ihre Aufbewahrung vorsieht, und zwar für die in diesen Vorschriften oder Anordnungen vorgeschriebenen Fristen.

5.13 Bereitstellung aller Informationen an den Verantwortlichen, die zum Nachweis der Einhaltung der Pflichten erforderlich sind
Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der in Art. 28 GDPR niedergelegten Pflichten erforderlich sind, und muss Überprüfungen, einschließlich Inspektionen, die vom Verantwortlichen oder von einem anderen von diesem beauftragten Prüfer – zu den im nachfolgenden Art. 8 näher festgelegten Bedingungen und Modalitäten – oder von den Behörden durchgeführt werden, ermöglichen und dazu beitragen.

5.14 Fall, in dem eine Weisung an den Auftragsverarbeiter als Verstoß gegen die GDPR angesehen wird
Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung des Verantwortlichen gegen die GDPR oder gegen andere nationale Datenschutzbestimmungen oder Datenschutzbestimmungen der Union verstößt, muss er den Verantwortlichen unverzüglich informieren.

5.15 Einhaltung der Grundsätze „Privacy by Design“ und „Privacy by Default“
Der Auftragsverarbeiter hat bei der Ausführung des Auftrags die Grundsätze des Datenschutzes durch Technikgestaltung (Privacy by Design) und des Datenschutzes durch datenschutzfreundliche Voreinstellungen zu beachten. Die DIENSTE werden in standardisierter, für alle Kunden gleicher Form erbracht und sind nach diesen Grundsätzen gestaltet.

6. Pflichten des Verantwortlichen

6.1 Der Verantwortliche muss:
- dem Auftragsverarbeiter die in Art. 4 dieser Klauseln vorgesehenen Daten bereitstellen;
- alle Weisungen zur Verarbeitung der Daten durch den Auftragsverarbeiter schriftlich dokumentieren;
- vorab und während der gesamten Dauer der Verarbeitung darüber wachen, dass der Auftragsverarbeiter die in der europäischen Datenschutzverordnung vorgesehenen Pflichten einhält;
- die Verarbeitung beaufsichtigen und dabei Audits und Inspektionen durchführen.

7. Orte, an denen die Daten aufbewahrt werden und künftig aufbewahrt werden

7.1 Die Daten werden vom Auftragsverarbeiter an den im „Verarbeitungsverzeichnis des Dienstes“ angegebenen Orten verarbeitet. Sollte die Verarbeitung in Ländern außerhalb der EU erfolgen, stellt der Auftragsverarbeiter dem Verantwortlichen die Garantien zur Verfügung, die je nach dem Ort, an dem die Verarbeitung erfolgt, getroffen wurden.

7.2 Ist der Auftragsverarbeiter nach dem Unionsrecht oder dem Recht des Mitgliedstaats, dem er unterliegt, verpflichtet, Daten an ein Drittland oder eine internationale Organisation zu übermitteln, muss er dem Verantwortlichen diese rechtliche Anforderung vor der Übermittlung mitteilen, um die Genehmigung einzuholen, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

8. Kontrollen

8.1 Der Verantwortliche behält sich vor, auch durch regelmäßige Überprüfungen die genaue Einhaltung der gesetzlichen Bestimmungen über die Verarbeitung dieser Daten und die Einhaltung seiner in diesem Dokument enthaltenen Weisungen zu überwachen. Der Auftragsverarbeiter muss dem Verantwortlichen unter voller Mitwirkung regelmäßige Überprüfungen der Angemessenheit der getroffenen Sicherheitsmaßnahmen und der Einhaltung der Datenschutzvorschriften und der Anordnungen des Verantwortlichen ermöglichen.

8.2 Jedes Audit des Verantwortlichen ist mit dem Auftragsverarbeiter mit einer Vorankündigung von mindestens 10 Arbeitstagen zu vereinbaren. Verursachen diese Tätigkeiten Lasten und Kosten, die in diesem Vertrag nicht vorgesehen sind, sind alle Anfragen des Verantwortlichen hinsichtlich der Art ihrer Durchführung abzustimmen und auf Projektebene zu behandeln, wobei für ihre Umsetzung eine Bewertung, auch in wirtschaftlicher Hinsicht, festzulegen ist (sei es für Penetrationstests, Vulnerability Assessments oder Sonstiges).

8.3 Jede Information, die in Erfüllung der Pflichten des Auftragsverarbeiters oder des Verantwortlichen geteilt wird, ist als vertraulich eingestuft und darf daher nur mit vorheriger schriftlicher Genehmigung der anderen Partei verbreitet, weitergegeben oder im Internet veröffentlicht werden. Jede beauftragte Person, die die Information verarbeitet, hat eine Vertraulichkeitsvereinbarung unterzeichnet, die das Verbot der Weitergabe an Unbefugte vorsieht, auch nach Beendigung des Arbeitsverhältnisses und solange die Informationen nicht aus Gründen, die diesen Personen nicht zuzurechnen sind, öffentlich

bekannt sind. Jede Verletzung der Vertraulichkeit dieser Informationen wird nach Maßgabe der gesetzlichen und vertraglichen Bestimmungen geahndet.

Unverbindliche Übersetzung des italienischen Originals. Bei Abweichungen ist der italienische Text maßgebend.

Verfasser	Datenschutzbüro Zucchetti Spa
Freigabe	Fabrizio Scuppa, gesetzlicher Vertreter der Octorate S.r.l.

Version Revision

Version	Verfasser	Konsultation des DPO	Ausgabedatum	Grund der Revision
0	Datenschutzbü-ro		12/11/2026	Erstausgabe

OCTORATE

AUFTRAGSVERARBEITER					
Firmenname	Octorate Srl				
MwSt.-Nr.	13493861002				
Adresse	Via Filippo Caruso 23				
Ort	Roma	**PLZ**	00173	**Prov.**	RM
Gesetzlicher Vertreter	Fabrizio Scuppa				

MIT DER VERARBEITUNG BEAUFTRAGTE PERSONEN
Personal von Octorate für Kundensupport, Onboarding und Schulung, Entwickler und Systemtechniker, zur Verarbeitung befugt und unterwiesen, mit auf die jeweiligen Aufgaben beschränkten Zugriffsrechten. Für OctoAgent das Entwicklungsteam (4 Personen) und das Supportteam (3 Personen) der iManager S.r.l., die als Unterauftragsverarbeiter unter den Empfängern aufgeführt ist.

KONTAKTDATEN			
Auftragsverarbeiter	Octorate Srl	legal@octorate.com	06 4542 0568
Vertreter des Auftragsverarbeiters	Entfällt		
Datenschutzbeauftragter (DPO)	DPO von Octorate	dpo@octorate.com	

BESCHREIBUNG
System zur Verwaltung von Buchungen, Raten und Verfügbarkeiten, Distribution über die angebundenen Kanäle, Website und Booking Engine, Kommunikation mit den Gästen, Erfüllung der Pflichten gegenüber Polizia di Stato (italienische Staatspolizei), ISTAT (italienisches Statistikamt) und Agenzia delle Entrate (italienische Steuerbehörde), Zahlungsintegrationen, tägliche Abläufe des Betriebs und, soweit aktiviert, automatisierte Bearbeitung der Konversationen mit OctoAgent.

ZWECK DER VERARBEITUNG

Erbringung der Dienste von Octorate im Auftrag des Kunden, das heißt Verwaltung von Buchungen, Raten und Verfügbarkeiten, Distribution über die angebundenen Kanäle, Website und Booking Engine, Kommunikation mit den Gästen, Erfüllung der Pflichten gegenüber Polizia di Stato, ISTAT und Agenzia delle Entrate, Zahlungsintegrationen, tägliche Abläufe des Betriebs und, soweit aktiviert, automatisierte Bearbeitung der Konversationen mit OctoAgent, einschließlich Support und Wartung der Dienste.
Art der Verarbeitung. Erheben, Erfassen, Organisation, Ordnen, Speicherung, Abfragen, Bearbeitung, Auslesen, Offenlegung durch Übermittlung an die vom Kunden angegebenen Empfänger, Löschen. Für OctoAgent auch automatisierte Verarbeitung mittels KI-Modellen zur Erzeugung von Antworten, Übersetzungen, Zusammenfassungen, Transkriptionen, Klassifizierungen und Meldungen.
Dauer und Häufigkeit. Für die gesamte Dauer des Vertragsverhältnisses, fortlaufend. Die Aufbewahrungsfristen je Kategorie sind in den Fristen für die Löschung der Daten angegeben.

KATEGORIE DER BETROFFENEN PERSONEN

Gäste und Buchende, einschließlich Begleitpersonen und minderjähriger Gäste im Rahmen der gesetzlichen Pflichten. Personen, die den Betrieb wegen Informationen oder Angeboten kontaktieren. Nutzer des Kontos des Kunden, das heißt Inhaber, Personal und freie Mitarbeiter. Eigentümer der verwalteten Einheiten, bei Property Managern, die das Eigentümerportal nutzen. Lieferanten und Partner des Kunden, die gegebenenfalls in der Plattform erfasst sind.

KATEGORIEN PERSONENBEZOGENER DATEN

Buchungs- und Aufenthaltsdaten. Vor- und Nachname, Kontaktdaten, Sprache, Nationalität, An- und Abreisedaten, Einheit und Kategorie, Anzahl und Zusammensetzung der Gäste, Beträge, Herkunftskanal, Präferenzen und vom Kunden oder vom Gast eingegebene Anmerkungen.
Daten für die Erfüllung gesetzlicher Pflichten. Für die Alloggiati-Meldescheine Personenstammdaten, Geburtsort und Geburtsdatum, Staatsangehörigkeit, Art, Nummer und Ausstellungsort des Ausweisdokuments. Für das ISTAT statistische Daten zu den Gästeströmen. Für die Steuerdokumente Steuerdaten der Gäste, Steuernummer und MwSt.-Nr.
Zahlungsdaten. Als Buchungsgarantie erhobene Kreditkartendaten, die gemäß den PCI-DSS-Standards verschlüsselt gespeichert werden und von Octorate nicht direkt entschlüsselt werden können, sowie von den Gateways und Zahlungsinstituten mitgeteilte Transaktionsergebnisse.
Kommunikation. Inhalt und Anhänge der Nachrichten, die mit den Gästen per E-Mail, über die Nachrichtenfunktionen der OTA-Portale, WhatsApp, SMS und den Chat der Website ausgetauscht werden. Mit OctoAgent auch die von den Gästen gesendeten Bilder, die Zusammenfassungen, die Transkriptionen und die Audioaufzeichnungen der Anrufe bei aktivem Sprachmodul, die Zeilen zum Gedankengang des Agenten und die vom Kunden genehmigten Lektionen.
Online-Check-in mit OctoAgent. Vom Gast für den Check-in gesendetes Bild des Ausweisdokuments, aus dem OctoAgent die Personenstammdaten ausliest. Das Lichtbild des Dokuments wird vor der Übermittlung an das KI-Modell unkenntlich gemacht.

Website und Booking Engine. Daten der Besucher und der Buchenden auf der Website und in der Booking Engine des Kunden, gemäß den Datenschutzhinweisen und der Cookie-Richtlinie des Kunden.
Nutzer des Kontos. Name, E-Mail, Rolle, Zugangsdaten, Zugriffs- und Aktivitätslogs, die für den Betrieb und die Sicherheit der Plattform erforderlich sind.
Besondere Kategorien von Daten. In den Diensten nicht vorgesehen. Von den Gästen unaufgefordert mitgeteilte Informationen, zum Beispiel gesundheitliche, ernährungsbezogene oder religiöse Bedürfnisse, werden unter der Verantwortung des Kunden verarbeitet.

KEINE NUTZUNG FÜR EIGENE ZWECKE

Octorate nutzt die Kundendaten nicht für eigene Zwecke. Octorate kann Daten in aggregierter und anonymer Form, die weder eine Identifizierung des Kunden noch der betroffenen Personen zulassen, für statistische Zwecke, für Sicherheitszwecke und zur Verbesserung der Dienste verarbeiten.

KATEGORIE DER EMPFÄNGER, AN DIE DIE DATEN WEITERGEGEBEN WERDEN KÖNNEN

Liste der vom Kunden allgemein genehmigten Unterauftragsverarbeiter, mit dem Land und den Garantien für die Datenübermittlung jedes Anbieters. Die OTA-Portale, die öffentlichen Stellen, die Gateways und die Zahlungsinstitute sind keine Unterauftragsverarbeiter und erhalten die Daten wie bei den Stellen angegeben, die die Daten als eigenständige Verantwortliche erhalten.

- Aruba S.p.A. (Italien). Hosting, Datenbank, Speicher und Backup der Octorate-Plattform (PMS, Channel Manager, Booking Engine). Übermittlungsgarantie innerhalb des EWR.
- Complior AB (vormals 24 Solutions) (Schweden). Mit der Plattform verbundene, nach PCI DSS zertifizierte Umgebung für die Kreditkartendaten. Übermittlungsgarantie innerhalb des EWR.
- iManager S.r.l., Via del Muro Linari 31, 00173 Roma, Steuernummer und MwSt.-Nr. 16082961000 (Italien). Entwicklung, Betrieb und Anwendungshosting der OctoAgent-Plattform. Übermittlungsgarantie innerhalb des EWR.
- Google Cloud (Google Cloud EMEA Limited) (Irland, Rechenzentrum in Mailand). Hosting von OctoAgent. Übermittlungsgarantie innerhalb des EWR, Standardvertragsklauseln für etwaige Zugriffe aus Drittländern.
- MongoDB Atlas (MongoDB Limited) (Irland, Rechenzentren in Mailand und Frankfurt). Datenbank von OctoAgent und Backup. Übermittlungsgarantie innerhalb des EWR, Standardvertragsklauseln für etwaige Zugriffe aus Drittländern.
- OpenAI (OpenAI Ireland Limited, Vertragspartner für den EWR) (Irland, Verarbeitung auch in den Vereinigten Staaten). KI-Modelle von OctoAgent, Erzeugung von Antworten, Zusammenfassungen, Transkriptionen, Auslesen der Daten aus den Dokumenten, über das Konto von iManager. KI-Modelle der anderen Funktionen der Octorate-Plattform, über das Konto von Octorate. Übermittlungsgarantie Standardvertragsklauseln, die im DPA von OpenAI enthalten sind, wobei OpenAI nicht über die DPF-Zertifizierung verfügt.
- Openapi S.r.l. (Openapi.com) (Italien). Versand von SMS an die Gäste durch OctoAgent. Übermittlungsgarantie innerhalb des EWR.

- Better Stack (EU). Überwachung der Verfügbarkeit und Alarme von OctoAgent, Datenregion EU, nur wenn in den Logs personenbezogene Daten enthalten sind. Übermittlungsgarantie innerhalb des EWR.
- Microsoft Clarity (Microsoft) (Irland, USA). Analyse der Nutzung der OctoAgent-Konsole durch die Nutzer der Betriebe, mit aktiver Maskierung. Übermittlungsgarantie Angemessenheit (DPF) oder Standardvertragsklauseln.
- Meta (WhatsApp Business Platform) (Irland, USA). WhatsApp-Nachrichtenverkehr zwischen Betrieben und Gästen. Übermittlungsgarantie Angemessenheit (DPF) oder Standardvertragsklauseln.
- Mailchimp Transactional (Mandrill, The Rocket Science Group LLC) und SparkPost (Bird) (USA, EU). Für die Domain octorate.com autorisierte E-Mail-Versanddienste für E-Mails, die nicht von den Mailservern von Octorate ausgehen. OctoAgent nutzt sie nicht. Übermittlungsgarantie Angemessenheit (DPF) oder Standardvertragsklauseln.
- Mailgun (Mailgun Technologies, Inc., Sinch-Gruppe) (USA, EU). Dienst für den Versand der E-Mails der Dienste. Übermittlungsgarantie Standardvertragsklauseln.
- Intercom (Intercom R&D Unlimited Company) (Irland, USA). Support-Chat der Octorate-Plattform, nur wenn darüber Daten der Gäste laufen. OctoAgent nutzt ihn nicht. Übermittlungsgarantie Angemessenheit (DPF).

Der Telefondienst des Sprachmoduls von OctoAgent wird von Vonage auf der Grundlage eines auf den Kunden lautenden Vertrags erbracht, der auf Veranlassung von Octorate aktiviert wird, sodass Vonage kein Unterauftragsverarbeiter von Octorate ist. Änderungen dieser Liste werden dem Kunden mitgeteilt. Die aktuelle Fassung ist auf Anfrage an legal@octorate.com erhältlich.

DATENÜBERMITTLUNG INS AUSLAND

Die Kundendaten werden in Rechenzentren in der Europäischen Union gespeichert, die in den Sicherheitsmaßnahmen für das Rechenzentrum angegeben sind.

Octorate übermittelt Kundendaten, auch über Unterauftragsverarbeiter, nur unter Einhaltung von Kapitel V der GDPR an Drittländer, und zwar auf der Grundlage eines Angemessenheitsbeschlusses der Europäischen Kommission, einschließlich des EU-US Data Privacy Framework für zertifizierte Anbieter, oder der mit dem Durchführungsbeschluss (EU) 2021/914 der Kommission erlassenen Standardvertragsklauseln, ergänzt durch die gegebenenfalls erforderlichen zusätzlichen Maßnahmen. Die für jeden Unterauftragsverarbeiter angewandten Garantien sind in der Liste der Empfänger angegeben. Für die KI-Modelle von OctoAgent und der anderen Funktionen der Plattform werden die für die Erzeugung der Inhalte erforderlichen Daten an OpenAI übermittelt, das sie auf der Grundlage der in seiner Vereinbarung über die Datenverarbeitung enthaltenen Standardvertragsklauseln auch in den Vereinigten Staaten verarbeitet.

Die Übermittlungen an OTA-Portale, Zahlungsgateways, vom Kunden über APIs angebundene Software Dritter, Gäste und andere vom Kunden angegebene Empfänger, auch in Drittländern, erfolgen auf Weisung des Kunden, der dafür verantwortlich ist.

FRISTEN FÜR DIE LÖSCHUNG DER DATEN

Buchungs- und Aufenthaltsdaten sowie Gästestammdaten. Für die gesamte Vertragslaufzeit und bis zu 30 Tage nach der Beendigung, sofern der Kunde keine abweichende Weisung erteilt.
Nachrichten und Konversationen mit den Gästen. Für die gesamte Vertragslaufzeit, sofern keine vorzeitige Löschung auf Weisung des Kunden erfolgt.
Transkriptionen, Zusammenfassungen und Aufzeichnungen der Anrufe, Lektionen und Zeilen zum Gedankengang von OctoAgent. Für die gesamte Vertragslaufzeit, sofern keine vorzeitige Löschung auf Weisung des Kunden erfolgt.
An die KI-Modelle (OpenAI) gesendete Daten. Vom Anbieter nicht für spätere Verwendungen gespeichert. OpenAI bewahrt sie bis zu 30 Tage zur Missbrauchskontrolle auf und löscht sie anschließend.
Daten für Alloggiati-Meldescheine, ISTAT und Steuerdokumente. Für die zur Übermittlung erforderliche Zeit und für die gesetzlich vorgesehenen Aufbewahrungspflichten.
Technische Logs und Sicherheitslogs. Für die Octorate-Plattform Logs der HTTP-Anfragen 45 Tage und Zugriffslogs der Systemadministratoren mindestens 6 Monate, vorbehaltlich gesetzlicher Pflichten. Für OctoAgent Anwendungslogs 90 Tage und Audit-Logs 400 Tage. In den Logs von OctoAgent werden die Inhalte der Gäste, das heißt Nachrichten, E-Mails, Telefon und Dokumente, nicht aufgezeichnet. Die technischen Logs der Anfragen, die aus Sicherheitsgründen 400 Tage aufbewahrt werden, enthalten die IP-Adresse der Person, die sich verbindet. Auf die Logs greift nur das Entwicklungsteam von iManager zu.
Backups. Automatisches Überschreiben nach den nachstehend angegebenen Zyklen. Für OctoAgent tägliche Backups, die 7 Tage aufbewahrt werden, wöchentliche Backups, die 4 Wochen aufbewahrt werden, und eine tägliche Kopie in Frankfurt, die 90 Tage aufbewahrt wird. Für die Octorate-Plattform tägliche Backups, die 30 Tage aufbewahrt werden.
Vor der Beendigung kann der Kunde die Kundendaten über die Exportfunktionen der Plattform in gängigen strukturierten Formaten exportieren. Auf schriftliche Anfrage, die vor der Beendigung eingeht, unterstützt Octorate bei der Rückgabe der Daten, die nicht selbstständig exportiert werden können, zu den gegebenenfalls vereinbarten Entgelten.
Innerhalb von 30 Tagen nach der Beendigung löscht Octorate die Kundendaten und die vorhandenen Kopien, mit Ausnahme der Backups, die wie oben angegeben rollierend überschrieben werden, und mit Ausnahme der Daten, die Octorate aufgrund gesetzlicher Pflichten aufbewahren muss, darunter die Steuerdokumente und die gesetzlich vorgeschriebenen Logs, die für die vorgeschriebene Zeit aufbewahrt und anschließend gelöscht werden. Löschungsanträge, die während des Vertragsverhältnisses eingehen, werden innerhalb von 5 Arbeitstagen ausgeführt, wie in den Allgemeinen Geschäftsbedingungen vorgesehen. Auf Anfrage bestätigt Octorate die erfolgte Löschung schriftlich.

STELLEN, DIE DIE DATEN ALS EIGENSTÄNDIGE VERANTWORTLICHE ERHALTEN

Die OTA-Portale, die Gateways und Zahlungsinstitute, die Polizia di Stato, das ISTAT, die Agenzia delle Entrate und die anderen Stellen, an die die Dienste auf Weisung des Kunden Daten übermitteln, verarbeiten die Daten als eigenständige Verantwortliche oder gemäß ihren jeweiligen Vereinbarungen mit dem Kunden. Octorate beschränkt sich auf die technische Übermittlung und haftet nicht für die von diesen Stellen durchgeführte Verarbeitung. Dasselbe gilt für Vonage, das den Telefondienst des Sprachmoduls von OctoAgent auf

der Grundlage eines auf den Kunden lautenden Vertrags erbringt.

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

Octorate führt gemäß Artikel 30 Absatz 2 der GDPR das Verzeichnis zu den Kategorien von im Auftrag der Kunden durchgeführten Tätigkeiten der Verarbeitung und stellt es dem Kunden auf Anfrage an legal@octorate.com zur Verfügung.

ALLGEMEINE BESCHREIBUNG DER TECHNISCHEN UND ORGANISATORISCHEN SICHERHEITSMASSNAHMEN

1. IN DER SOFTWARE UMGESETZTE SICHERHEITSMASSNAHMEN

In der Octorate-Plattform und in OctoAgent getroffene Sicherheitsmaßnahmen.

- *Verwaltung der Zugangsdaten*

• Persönliche Zugangsdaten für jeden Nutzer, Regeln zur Passwortstärke, Sperrung unbefugter Zugriffe und Protokollierung der Zugriffe.
• Zwei-Faktor-Authentifizierung mit OTP-Code für die Octorate-Plattform und für den Zugang zu OctoAgent mit Octorate-Zugangsdaten.
• OctoAgent sieht auch einen internen Zugang für das operative Personal des Betriebs vor, das kein Octorate-Benutzerkonto hat, zum Beispiel Personen, die Anrufe entgegennehmen, Instandhaltung und Reinigung, ohne Zwei-Faktor-Authentifizierung und nicht für Nutzer mit Administratorrechten bestimmt. Die Ausweitung der Zwei-Faktor-Authentifizierung auf die internen Nutzer wird derzeit mit dem Anbieter geprüft.

- *Datenminimierung*

• Vom Kunden konfigurierbare Rollen und Berechtigungen, um den Zugriff auf die Daten auf die Aufgaben des jeweiligen Nutzers zu beschränken.
- Identifizierung der Personen mit Zugang zum System
• Technische Logs, mit denen sich die in der Plattform durchgeführten Tätigkeiten nachvollziehen lassen. Für OctoAgent Anwendungslogs, die 90 Tage aufbewahrt werden, sowie Audit-Logs und technische Logs der Anfragen, die 400 Tage aufbewahrt werden, ohne die Inhalte der Gäste. Die technischen Logs enthalten die IP-Adresse der Person, die sich verbindet, und sind nur für das Entwicklungsteam von iManager zugänglich. Für die Octorate-Plattform Logs der HTTP-Anfragen, die 45 Tage aufbewahrt werden. Die Zugriffe der Systemadministratoren werden unveränderbar protokolliert, und die entsprechenden Logs werden mindestens 6 Monate aufbewahrt, wie in der Verfügung des Garante (italienische Datenschutzbehörde) zu den Systemadministratoren vorgesehen.
• Zugriffe des Supportpersonals auf das Konto des Kunden gemäß den weiter unten angegebenen Maßnahmen für die Supportdienste.

- *Verschlüsselungstechniken*

• Datenübertragung mit dem TLS-Protokoll in allen Diensten.
• Kreditkartendaten, die gemäß dem Standard PCI DSS verschlüsselt gespeichert werden und von Octorate nicht direkt entschlüsselt werden können.
• Verschlüsselung der ruhenden Daten in den Datenbanken der Octorate-Plattform und von OctoAgent.

- *Privacy by Default*

• Dienste, die in standardisierter, für alle Kunden gleicher Form erbracht werden und nach den Grundsätzen des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen gestaltet sind. Logische Trennung der Daten der verschiedenen Kunden in der Plattform.

- *Rechte der betroffenen Personen*

• Der Kunde kann die Daten aus der Plattform in gängigen strukturierten Formaten exportieren. Octorate unterstützt den Kunden dabei, den Anträgen der betroffenen Personen nachzukommen. Löschungsanträge, die während des Vertragsverhältnisses eingehen, werden innerhalb von 5 Arbeitstagen ausgeführt.

2. AUFTRAGSVERARBEITER: FÜR DIE SUPPORTDIENSTE UMGESETZTE SICHERHEITSMASSNAHMEN

Octorate leistet den Kunden Support aus der Ferne über den Chat der Plattform, per E-Mail und per Telefon, mit Personal, das zur Verarbeitung befugt und unterwiesen ist. Die über Chat und E-Mail eingegangenen Anfragen werden als Tickets in Intercom erfasst, das unter den Empfängern aufgeführt ist. Wenn es zur Lösung der Anfrage erforderlich ist, greift das Supportpersonal über das interne Panel von Octorate auf das Konto des Kunden zu, mit persönlichen Zugangsdaten und ohne das Passwort des Kunden zu verwenden. Octorate verbindet sich nicht mit Fernsteuerungsprogrammen mit den Geräten des Kunden.
Das Supportpersonal verarbeitet die Daten des Kunden nur, um die Anfrage zu lösen. Dateien und Exporte für den Support werden vom Kunden als Anhänge im Chat der Plattform empfangen und nur für diese Anfrage verwendet. Sie bleiben für die Vertragslaufzeit der Konversation in Intercom beigefügt. Sie werden innerhalb der in diesem Verzeichnis für die Kundendaten angegebenen Fristen gelöscht, das heißt innerhalb von 30 Tagen nach der Beendigung, vorbehaltlich der gesetzlichen Aufbewahrungspflichten, oder früher auf Anfrage des Kunden.

3. AUFTRAGSVERARBEITER: SICHERHEITSMASSNAHMEN FÜR DAS RECHENZENTRUM

Octorate-Plattform. Infrastruktur bei Aruba S.p.A. in Rechenzentren in Italien, die nach ISO/IEC 27001, 27017, 27018 und ANSI/TIA-942 Rating 4 zertifiziert sind. Tägliche Backups der Datenbank, die 30 Tage aufbewahrt werden, mit Wiederherstellungsverfahren.
Kreditkarten. Kreditkartendaten in einer nach PCI DSS zertifizierten Umgebung bei Complior AB, Schweden.
OctoAgent. Seit dem 20. Oktober 2026 Hosting bei Google Cloud in Mailand mit Datenbank MongoDB Atlas in Mailand und Kopie der Backups in Frankfurt, anstelle von Scaleway in Paris, wo die Daten nach der Migration gelöscht wurden. Anbieter mit den Zertifizierungen ISO/IEC 27001 und SOC 2. Tägliche Backups, die 7 Tage aufbewahrt werden, wöchentliche Backups, die 4 Wochen aufbewahrt werden, und eine tägliche Kopie in Frankfurt, die 90 Tage aufbewahrt wird.
System-E-Mails. Die System-E-Mails der Plattform werden von den bei Aruba gehosteten Mailservern von Octorate oder von den unter den Empfängern aufgeführten E-Mail-Versanddiensten versendet.

4. GRUNDLEGENDE NIS2-SICHERHEITSMASSNAHMEN

Octorate gehört zur Zucchetti-Gruppe, einer wesentlichen Einrichtung im Sinne der NIS2-Vorschriften, und wendet die von der ACN (italienische Agentur für Cybersicherheit) festgelegten grundlegenden Sicherheitsmaßnahmen nach dem Modell der Gruppe an. Die folgenden Punkte führen für jeden im Modell vorgesehenen Bereich die Maßnahmen auf, die Octorate für die Dienste getroffen hat.

Zuverlässigkeit der Anbieter. Octorate verarbeitet die Kundendaten nur mit den unter den Empfängern aufgeführten Unterauftragsverarbeitern, die durch Vereinbarungen gemäß Artikel 28 gebunden sind und unter Anbietern mit anerkannten Sicherheitszertifizierungen (ISO/IEC 27001, SOC 2, PCI DSS) ausgewählt wurden. Jeder neue Anbieter wird vor seinem Einsatz bewertet und dem Kunden mitgeteilt. Octorate nimmt über den Ansprechpartner der Gruppe am Verfahren der Zucchetti-Gruppe zur Qualifizierung der Anbieter teil.

Rollen und Verantwortlichkeiten. Datenschutzbeauftragter erreichbar unter dpo@octorate.com. Interne Ansprechpartner für Sicherheit und Sicherheitsvorfälle, die im Verfahren zur Bewältigung von Sicherheitsvorfällen angegeben sind. Für die NIS2-Pflichten wendet sich Octorate an die NIS-Kontaktstelle und den CSIRT-Ansprechpartner, die von der Zucchetti-Gruppe für den Bereich Hospitality benannt wurden, mit dem jeweiligen Stellvertreter, die im Verfahren zur Bewältigung von Sicherheitsvorfällen angegeben sind.

Zuverlässigkeit des Personals. Zur Verarbeitung befugtes Personal, das in den anwendbaren Vorschriften unterwiesen und zur Vertraulichkeit verpflichtet ist, mit auf die jeweiligen Aufgaben beschränkten Zugriffsrechten, die bei Beendigung des Arbeitsverhältnisses entzogen werden.

Compliance und Audits. Informationen und Überprüfungen stehen dem Kunden auf Anfrage zur Verfügung. Infrastrukturen bei zertifizierten Anbietern, die Audits durch Dritte unterliegen, insbesondere Aruba S.p.A. (ISO/IEC 27001, 27017, 27018 und ANSI/TIA-942 Rating 4), Complior AB (PCI DSS), Google Cloud und MongoDB (ISO/IEC 27001 und SOC 2).

Schwachstellenmanagement. Sicherheitsupdates und Sicherheitskorrekturen werden vorrangig eingespielt. Für OctoAgent Schwachstellenscan und Überprüfung der Konfiguration der neuen Infrastruktur bis zum 30. November 2026, erster externer Penetrationstest bis zum 31. März 2027 und danach einmal jährlich, mit Bearbeitung der Ergebnisse und der Korrekturen. Für die Octorate-Plattform Schwachstellentests und Penetrationstests im Rahmen des Programms der Zucchetti-Gruppe, in das Octorate über den Ansprechpartner der Gruppe eingebunden ist.

Betriebskontinuität und Disaster Recovery. Tägliche Backups der Octorate-Plattform, die 30 Tage aufbewahrt werden, mit Wiederherstellungsverfahren. Für OctoAgent tägliche Backups, die 7 Tage aufbewahrt werden, wöchentliche Backups, die 4 Wochen aufbewahrt werden, und eine tägliche Kopie in Frankfurt, die 90 Tage aufbewahrt wird. Nach ANSI/TIA-942 Rating 4 zertifizierte Rechenzentren für die Octorate-Plattform. Kontinuierliche Überwachung der Verfügbarkeit der Dienste.

Identitäts- und Zugriffsmanagement. Persönliche Zugangsdaten, Prinzip der geringsten Berechtigung mit vom Kunden konfigurierten Rollen und Berechtigungen, Regeln zur Passwortstärke, Sperrung unbefugter Zugriffe, Protokollierung der Zugriffe und Überprüfung der Benutzerkonten. Zwei-Faktor-Authentifizierung mit OTP-Code für die Octorate-Plattform und für den Zugang zu OctoAgent mit Octorate-Zugangsdaten. Interner Zugang zu OctoAgent für das operative Personal des Betriebs mit den Einschränkungen, die in den in der Software umgesetzten Sicherheitsmaßnahmen angegeben sind. Technische und administrative Zugriffe auf die Infrastruktur von OctoAgent über die Konsole des Cloud-Anbieters mit Zwei-Faktor-Authentifizierung, über ein privates, nicht im Internet exponiertes Netz, wobei der Server für den

Datenbankzugriff nur bei Bedarf eingeschaltet wird. Administrative Zugriffe und Änderungen werden protokolliert und überwacht.

Physische Sicherheit. Die Daten werden ausschließlich in den Rechenzentren der in diesem Verzeichnis angegebenen Anbieter gespeichert, mit der in den Zertifizierungen der Anbieter vorgesehenen physischen Zutrittskontrolle.

Schulung und Sensibilisierung. Schulung des Personals zum Schutz personenbezogener Daten und zur IT-Sicherheit, mit unterschiedlichen Inhalten für allgemeines Personal, technisches Personal und Geschäftsleitung gemäß dem Programm der Zucchetti-Gruppe, in das Octorate über den Ansprechpartner der Gruppe eingebunden ist.

Datensicherheit. Übertragung mit dem TLS-Protokoll, Verschlüsselung der ruhenden Daten in den Datenbanken der Octorate-Plattform und von OctoAgent, Kreditkartendaten in einer nach PCI DSS zertifizierten Umgebung, logische Trennung der Daten der Kunden, in der Europäischen Union gespeicherte Backups, sichere Löschung bei Beendigung.

Schutz der Netze und der Kommunikation. Perimeterschutz der Hosting-Anbieter, Serverless-Infrastruktur von OctoAgent in einem privaten, nicht im Internet exponierten Netz, Anwendungsfirewall für OctoAgent mit Protokollierung der Blockierungen, offizielle Kommunikationskanäle zum Kunden (E-Mail des Kontos und Hinweise in der Plattform), die auch für Mitteilungen über Sicherheitsvorfälle genutzt werden.

Überwachung von Ereignissen. Für OctoAgent minütliche Kontrolle der Verfügbarkeit des Dienstes von außen, der Anwendungsfehler, der Antwortzeiten, der Fehler gegenüber Octorate und gegenüber den Anbietern der Modelle, des Arbeitsspeichers und der Arbeitswarteschlangen, der Blockierungen der Anwendungsfirewall sowie der administrativen Zugriffe und Änderungen, mit Alarmen an das technische Team. Anwendungslogs werden 90 Tage aufbewahrt, Audit-Logs und technische Logs der Anfragen 400 Tage, ohne die Inhalte der Gäste. Die technischen Logs enthalten die IP-Adresse der Person, die sich verbindet, und sind nur für das Entwicklungsteam von iManager zugänglich. Für die Octorate-Plattform Logs der HTTP-Anfragen, die 45 Tage aufbewahrt werden, und unveränderbare Zugriffslogs der Systemadministratoren, die mindestens 6 Monate aufbewahrt werden.

Bewältigung und Meldung von Sicherheitsvorfällen. Schriftliches Verfahren zur Erkennung, Bewertung, Eindämmung und Mitteilung von Sicherheitsvorfällen. Der Anbieter, der OctoAgent betreibt, benachrichtigt Octorate innerhalb von 12 Stunden nach der Feststellung eines Sicherheitsvorfalls, der die Daten oder den Dienst betrifft, auch mit unvollständigen Informationen, mit Aktualisierung und Analyse innerhalb von 48 Stunden und Abschlussbericht innerhalb von 20 Tagen, damit die Gruppe die Fristen von 72 Stunden und von einem Monat gegenüber dem CSIRT Italia einhalten kann. Octorate meldet dem Kunden die Verletzung innerhalb von 48 Stunden, nachdem sie Octorate bekannt geworden ist, und schaltet bei erheblichen Sicherheitsvorfällen im Sinne der NIS2-Vorschriften den Ansprechpartner der Zucchetti-Gruppe für die Meldung an das CSIRT Italia ein, mit Frühwarnung innerhalb von 24 Stunden und Meldung innerhalb von 72 Stunden.

Sichere Entwicklung. Entwicklung nach Sicherheitspraktiken von der Konzeption an, Sicherheitsupdates und Sicherheitskorrekturen, getrennte Entwicklungs- und Produktionsumgebungen und kontrollierte Releases.

Laufende Wartung und Weiterentwicklung. Updates und neue Funktionen werden über einen Änderungsmanagementprozess bereitgestellt und dem Kunden gemäß dem Abschnitt Weiterentwicklung und Änderung der Dienste der Allgemeinen Geschäftsbedingungen mitgeteilt. Für OctoAgent wurde die Migration der Infrastruktur am 20. Oktober 2026 abgeschlossen, mit Überprüfung der Konfiguration bis zum 30. November 2026.

Außerbetriebnahme. Löschung der Kundendaten innerhalb von 30 Tagen nach der Beendigung und

innerhalb von 5 Arbeitstagen auf Anfrage, wie in den Fristen für die Löschung der Daten angegeben, mit rollierendem Überschreiben der Backups. Sichere Entsorgung der Datenträger durch die Infrastrukturanbieter gemäß den jeweiligen Zertifizierungen.

Unterauftragsvergabe und Lieferkette. Liste der Unterauftragsverarbeiter unter den Empfängern, mit vertraglichen Pflichten, die denen der Bestellung zum Auftragsverarbeiter gleichwertig sind, einschließlich der anwendbaren grundlegenden NIS2-Sicherheitsmaßnahmen, und mit der Möglichkeit für den Kunden, innerhalb von 15 Tagen nach der Mitteilung Einspruch gegen die Änderungen zu erheben.