Vertrag zur Auftragsverarbeitung

gemäß Art. 28 EU-DSGVO

zwischen dem

Kunden

- Verantwortlicher - nachstehend „Auftraggeber“ genannt –

und

Immosolve GmbH

Tegelbarg 43, 24576 Bad Bramstedt

vertreten durch den Geschäftsführer Alexander Köth

- Auftragsverarbeiter - nachstehend „Auftragnehmer“ genannt

Empro

Gegenstand und Dauer des Auftrags

Gegenstand

Gegenstand des Auftrags zur Datenverarbeitung durch den Auftragnehmer ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

Einrichtung, Betrieb, Wartung und Support einer Softwarelösung mit Bezug zu Maklerdienstleistungen für den Auftraggeber.

Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Vereinbarung über die Einrichtung, Betrieb, Wartung und Support der durch den Auftragnehmer bereitgestellten Softwarelösung (Leistungsvereinbarung).

Konkretisierung des Auftragsinhalts

(1) Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers

- Einrichtung und Betrieb einer Software für die professionelle Immobilienvermietung und -vermarktung als Software as a Service (SaaS)
- Individuelle Anpassungen der Software-Funktionsweise für den Auftraggeber
- Wartung und Support der Software

(2) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Übermittlung der Auftraggeber-Daten in ein Land außerhalb von EU/EWR („Drittland“) erfolgt nur wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(3) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien

- Adress- und Kontaktdaten
- Vertragsdaten
- Bankverbindungs- und Kontodaten
- Angebotsdaten
- Leistungs- und Abrechnungsdaten
- Aktivitätenprotokoll
- Mitarbeiterdaten

(4) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Interessenten
- Kunden/Mieter
- Makler/ Vermittler
- Lieferanten/ Dienstleister
- Mitarbeiter

Pflichten des Auftraggebers

(1) Die Verantwortung für die rechtliche Zulässigkeit der Verarbeitung personenbezogener Daten in der Software (gem. Art. 5 und 6 DSGVO) obliegt ausschließlich dem Auftraggeber.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

(3) Die Datenverarbeitung durch den Auftragnehmer erfolgt im Rahmen der Zurverfügungstellung einer standardisierten, aber konfigurierbaren Software über das Internet. Der Auftraggeber übt sein Weisungsrecht in Bezug auf die Daten durch Einrichtung und Benutzung der Software aus. Im Übrigen sind Weisungen mindestens in Textform (z.B. E-Mail) zu erteilen. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich mindestens in Textform (z.B. E-Mail). Weisungsfrei ist die angemessene Fortentwicklung und Anpassung der Software durch den Auftragnehmer. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

(4) Für die Bearbeitung von Rechten der betroffenen Personen (Art. 15-20 DSGVO) und für die Umsetzung der Informationspflichten nach Art. 13 und 14 DSGVO ist allein der Auftraggeber zuständig. Der Auftragnehmer wird den Auftraggeber insoweit bei der Wahrnehmung seiner Verpflichtungen unterstützen.

Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag, gegen die DSGVO oder gegen andere Datenschutzbestimmungen der EU oder der Mitgliedstaaten verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Ausführung der Weisung bis zu einer Bestätigung oder Änderung der Weisung durch den Auftraggeber auszusetzen.

(3) Soweit der Auftragnehmer durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist, die personenbezogenen Daten auch ohne Weisung des Auftraggebers zu verarbeiten, teilt der Auftragnehmer dem Auftraggeber den Grund der Verarbeitung und die entsprechenden rechtlichen Anforderungen rechtzeitig vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(4) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- Schriftliche Benennung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Als (externer) Datenschutzbeauftragte ist RA David Oberbeck, Herting Oberbeck Datenschutz GmbH, datenschutzbeauftragter@immosolve.de benannt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
- Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum

Empro

Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer bei der Bearbeitung zu unterstützen.

Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen. ***Anlage 1*** spezifiziert die technisch-organisatorischen Maßnahmen des Auftragnehmers.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern

sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

(2) Vor dem Einsatz eines neuen Unterauftragnehmers hat der Auftragnehmer den Auftraggeber hiervon eine angemessene Zeit zuvor zu unterrichten. Der Auftraggeber kann aus wichtigem Grund dem Einsatz eines neuen Unterauftragnehmers innerhalb von vier Wochen widersprechen. Ein wichtiger Grund liegt insbesondere dann vor, wenn tatsächliche Anhaltspunkte bestehen, dass der Unterauftragnehmer nicht willens oder in der Lage ist, eine datenschutzkonforme Verarbeitung der Daten sicherzustellen.

Im Falle eines Widerspruchs verpflichten sich die Parteien, auf eine für beide vertretbare Lösung hinzuwirken. Sollte binnen vier Wochen kein Kompromiss gefunden werden können, kann entweder der Auftragnehmer entscheiden, den Unterauftragnehmer nicht einzusetzen oder der Auftraggeber ein Sonderkündigungsrecht geltend machen.

(3) Der Auftraggeber stimmt der Beauftragung der nachfolgend genannten Unterauftragnehmer unter der Bedingung zu, dass zwischen Auftragnehmer und Unterauftragnehmer eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO besteht.

Unterauftragnehmer	**Anschrift/Land**	**Leistung**
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855 Luxemburg	Cloud Hosting Service Provider
Datadog Inc.	620 8th Ave Fl 45, New York, New York 10018-1741	Technisches Monitoring
Mapbox Inc.	1133 15th St NW, Suite 825, Washington DC 20005	Kartendienst und Vervollständigung von Adresseingaben
Azure/ Open AI	**Microsoft Ireland Operations, Ltd.** Attn: Data Privacy One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521, Ireland	Bereitstellung von KI-Diensten

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer bei diesen Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die zwei Wochen im Voraus anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem

Empro

Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann durch die Vorlage aktueller Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) erfolgen.

(4) Die Kosten für die Durchführung von Kontrollen durch den Auftraggeber, insbesondere die Kosten für die Durchführung von Penetrationstests, trägt der Auftraggeber.

Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung oder in diesem Vertrag enthalten oder auf ein Fehlverhalten des Auftraggebers zurückzuführen sind, kann der Auftragnehmer eine angemessene Vergütung beanspruchen.

Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, dass eine Weisung gegen Datenschutzvorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(3) Der Auftraggeber teilt dem Auftraggeber die weisungsberechtigten Personen in Textform (z.B. E-Mail) mit.

(4) Beim Auftragnehmer sind zum Empfang von Weisungen des Auftraggebers und deren Umsetzung berechtigt:

- Alexander Köth, Geschäftsführer
- Nils Eckelt, Leitung Cloud-Entwicklung
- Hannes Mehr, Leitung DevOps

Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das

Empro

Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Schlussbestimmungen

(1) Änderungen, Ergänzungen oder eine Aufhebung dieser Vereinbarung bedürfen - soweit hierin nichts anderes bestimmt ist - zu ihrer Rechtswirksamkeit der elektronischen Form oder der Schriftform. Dies gilt auch für eine Aufhebung des vorgenannten Formerfordernisses.

(2) Der Auftragnehmer ist berechtigt, den Inhalt dieser Vereinbarung mit dem Einvernehmen des Auftraggebers zu ändern. Im Falle der Änderung der Auftragnehmer den Auftragnehmer den Änderungsvorschlag unter Benennung des Grundes und des konkreten Umfangs in Textform per E-Mail an die benannte Kontaktperson mitteilen. Die Änderungen gelten als genehmigt, wenn der Auftraggeber ihnen nicht schriftlich widerspricht (E-Mail an die im Impressum angegebene Adresse reicht). Der Auftragnehmer wird den Auftraggeber auf diese Folge in der Mitteilung besonders hinweisen. Der Widerspruch muss innerhalb von vier Wochen nach Zugang der Mitteilung bei dem Auftragnehmer eingegangen sein. Übt der Auftraggeber sein Widerspruchsrecht aus, gilt der Änderungswunsch als abgelehnt. Der Vertrag wird dann ohne die vorgeschlagenen Änderungen fortgesetzt.

Sofern der Auftraggeber sein Widerspruchsrecht ausübt, ist Auftragnehmer zur Kündigung des Vertrages berechtigt. Die Kündigungsfrist beträgt sieben (7) Tage.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam sein oder werden, wird hierdurch die Wirksamkeit der Vereinbarung im Übrigen nicht berührt. Die Parteien werden die unwirksame Bestimmung durch eine dieser nach Sinn und Zweck möglichst nahekommende wirksame Bestimmung ersetzen. Die vorstehende Regelung gilt im Falle unbeabsichtigter Vertragslücken entsprechend.

Empro

Anlage 1: Technisch-organisatorische Maßnahmen

Allgemeine Informationen

Name der Organisation / Verantwortlicher i.S. Art. 4 Nr. 7 DSGVO: Immosolve GmbH

Betriebsstätte 1 (Firmensitz): Tegelbarg 43, 24576 Bad Bramstedt. Betriebsstätte ist der Sitz der Gesellschaft. Dieser Betriebsstätte ist die Mehrheit der Mitarbeiter zugeordnet und der einzige Entwicklungsstandort der Gesellschaft. Die Arbeitsplätze sind mobil (Laptops) gestaltet. Im internen IT-Netzwerk befinden sich keinerlei Geräte, auf denen Daten dauerhaft gespeichert werden. Es umfasst ausschließlich Hardware für die Bürokommunikation und zur Anbindung an das Internet.

Rechenzentrum: Amazon Web Services EMEA SARL (AWS), 38 Avenue John F. Kennedy, L-1855 Luxemburg.
Eine Übersicht zu den Sicherheitsanforderungen AWS ist unter folgendem Link einsehbar: https://aws.amazon.com/de/compliance/data-center/controls/

Vertraulichkeit

Zutrittskontrolle

Der Betrieb der IT-Systeme erfolgt in externen Rechenzentren (AWS) und bei externen Dienstleistern (Software-as-a-Service). Die Zutrittskontrolle wird durch den Anbieter AWS durch ein entsprechendes Sicherheitskonzept gewährleistet. Weitere Informationen sind unter folgendem Link abrufbar: https://aws.amazon.com/de/security/.

Zugangskontrolle

Für die Kontrolle der internen Zugänge zu IT-Systemen existiert ein schriftliches Berechtigungskonzept, dass die Vergabe und den Entzug von Berechtigungen auf die einzelnen Systeme detailliert beschreibt.

Weitere Maßnahmen der internen Zugriffe auf die IT-Systeme:

- Benutzerauthentifizierung: Implementierung von starken Authentifizierungsverfahren für alle Mitarbeiter, die Zugang zu den Rechnersystemen benötigen.
- Regelmäßige Passwortwechsel und Passwortrichtlinien
- Physische Sicherheitsmaßnahmen: Es ist sichergestellt, dass der physische Zugang zu den Büros und den darin befindlichen Rechnern kontrolliert wird.
- VPN-Zugänge für Remote-Arbeit
- Richtlinien zur Geräteverwendung

Zugriffskontrolle

Es existieren Berechtigungs-/ Authentifizierungskonzepte nach dem Need-to-know-Prinzip. Die Zugriffsberechtigungen werden regelmäßig geprüft und aktualisiert.

Empro

Die Mitarbeiter haben sich verpflichtet mit besonderer Sorgfalt die personenbezogenen Daten zu behandeln. Alle Mitarbeiten sind außerdem zur Einhaltung der internen IT-Sicherheitsrichtlinie verpflichtet.

Weitere Maßnahmen der Zugriffskontrolle:

- Befristung und/oder Minimierung der Zugriffsrechte
- Kontrolle des Fernzugriffs: Besondere Sicherheitsmaßnahmen für den Fernzugriff, wie die Verwendung von VPNs und die Einschränkung des Zugriffs auf Unternehmensnetzwerke von externen Standorten.
- Sichere Authentifizierungsverfahren: Einsatz von starken Authentifizierungsmethoden wie Multi-Faktor-Authentifizierung (MFA) für den Zugriff auf sensible Systeme und Daten.
- Schulung der Mitarbeiter: Bewusstseinsschaffung und Schulung der Mitarbeiter in Bezug auf die Bedeutung von Zugriffskontrollen und den verantwortungsvollen Umgang mit Zugriffsrechten.

Trennungskontrolle

Die Daten von Mandanten werden in der Datenbank eindeutig über eine Mandanten-ID gekennzeichnet und von anderen Mandantendaten getrennt.

Pseudonymisierung

Soweit möglich, findet eine Pseudonymisierung der Datensätze statt.

Integrität

Weitergabekontrolle

Die Weitergabe von Daten an Kunden erfolgt auf unterschiedlichen Wegen, je nach Kundenwunsch, wie beispielsweise Webservices oder Secured File Transfer Protocol (SFTP).

Weitere Maßnahmen der Weitergabekontrolle:

- Verschlüsselung der Datenübertragung: Einsatz von starken Verschlüsselungstechnologien wie SSL/TLS für die Übertragung sensibler Daten über das Internet.
- Verträge und Vereinbarungen mit Dritten: Sicherstellen, dass Drittanbieter, die im Auftrag Daten übertragen, angemessene Sicherheitsmaßnahmen implementiert haben und vertraglich zur Einhaltung dieser Maßnahmen verpflichtet sind.

Eingabekontrolle

Wir haben verschiedene Maßnahmen zur Sicherstellung der internen Eingabekontrolle getroffen. Hierzu zählen:

- Protokollierung von Benutzeraktivitäten
- Sichere und nachvollziehbare Löschvorgänge
- Regelmäßige Audits und Compliance-Überprüfungen

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Der Betrieb der IT-Systeme erfolgt in externen Rechenzentren (AWS) und bei externen Dienstleistern (Software-as-a-Service). Die Verfügbarkeitskontrolle wird durch den Anbieter AWS durch ein entsprechendes Sicherheitskonzept gewährleistet. Weitere Informationen sind unter folgendem Link abrufbar: https://aws.amazon.com/de/security/.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutz-Management

Immosolve unterhält ein Information Security Management System (ISMS) und ein Datenschutzmanagementsystem (DMS). Beides wird in Kooperation mit dem Datenschutzbeauftragten laufend aktualisiert und überprüft. Einmal jährlich findet ein umfassendes Audit statt, um eventuelle Abweichungen zu identifizieren. Mitarbeiterschulungen zum Datenschutz finden ebenfalls jährlich statt. Penetrationstests werden spätestens alle zwei Jahre wiederholt.

Incident-Response-Management

Für das Incident-Response-Management sind verschiedene Eskalationswege im internen Betriebskonzept, welches Bestandteil des ISMS ist, dokumentiert.

Auftragskontrolle

Alle beauftragten Dienstleister werden gemäß Art. 28 DSGVO vertraglich auf die gesetzlichen Vorgaben verpflichtet. Darüber hinaus haben wir die folgenden Maßnahmen integriert:

- Regelmäßige Audits und Überprüfungen bei Dienstleistern
- Zertifizierungen und Compliance-Nachweise der Dienstleister
- Sicherstellung der Löschung oder Rückgabe der Daten