

Vertrag zur Auftragsverarbeitung

Allgemeines

Einleitung

Die cloudscale.ch AG ("Auftragnehmer") bietet virtuelle Server und damit verbundene IT-Infrastruktur-Dienstleistungen (zusammen "Services") an. Im Rahmen der Erbringung dieser Services für den Kunden ("Auftraggeber") verarbeitet der Auftragnehmer potenziell personenbezogene Daten im Auftrag des Auftraggebers ("Auftragsverarbeitung").

Gegenstand

Dieser Vertrag zur Auftragsverarbeitung ("AV-Vertrag") regelt die Rechte und Pflichten sowie Rollen und Zuständigkeiten des Auftragnehmers und des Auftraggebers ("Vertragsparteien") in Bezug auf die Auftragsverarbeitung.

Die Auftragsverarbeitung besteht insbesondere in der Speicherung, Bearbeitung, Bereitstellung, Übermittlung und Löschung von personenbezogenen Daten auf der Infrastruktur des Auftragnehmers ("Hosting-Daten") gemäss den Bestimmungen des Rahmenvertrags.

Dieser AV-Vertrag gilt ausdrücklich nicht in Bezug auf Verarbeitungen personenbezogener Daten, bei denen der Auftragnehmer die Zwecke und Mittel der Verarbeitung bestimmt und somit Verantwortlicher im datenschutzrechtlichen Sinn ist, z.B. bei Verarbeitungen personenbezogener Daten zu Zwecken der Leistungsabrechnung und Zahlungsabwicklung oder der Kommunikation mit dem Auftraggeber.

Hosting-Daten

Im Rahmen der Nutzung der Services entscheidet der Auftraggeber laufend selbst, ob und welche Art von Hosting-Daten er auf den Systemen des Auftragnehmers verarbeitet, von welchen Kategorien betroffener Personen, und zu welchem Zweck.

Entsprechend obliegt dem Auftraggeber die erforderliche Dokumentation sowie die Beurteilung, dass sich die Services des Auftragnehmers im konkreten Fall eignen; der

Auftragnehmer hat keine Kenntnisse über die Verarbeitung oder einen Einfluss darauf.

Von der Auftragsverarbeitung betroffen sein können zudem Hosting-Daten von Personen, denen der Auftraggeber Zugriff auf seine Website(s) oder Applikation(en) gewährt. Dabei handelt es sich insbesondere um personenbezogene Daten, die beim Aufrufen bzw. Ausführen sowie der Nutzung von Websites und Applikationen üblicherweise erhoben werden. Dazu gehören Protokolldaten, die bei der informatorischen Nutzung einer Website oder einer Applikation automatisiert erhoben werden (z.B. die IP-Adresse, das Betriebssystem und der Browser des Geräts des Nutzers sowie das Datum und die Zugriffszeit), vom Nutzer eingegebene Daten sowie sonstige vom Auftraggeber erhobene Nutzungsdaten mit Personenbezug.

Geltung und Dauer

Der Auftragnehmer stellt dem Auftraggeber diesen AV-Vertrag im Cloud Control Panel ("control.cloudscale.ch") in Bezug auf die angebotenen Services zum Abschluss bereit. Hat der Auftraggeber dem AV-Vertrag durch Aktivierung des Bestätigungsfeldes ("Click-to-Accept") auf control.cloudscale.ch zugestimmt, wird der AV-Vertrag für die Vertragsparteien zum verbindlichen Bestandteil ihres Rahmenvertrags betreffend der Erbringung bzw. Inanspruchnahme von Services. Bestehen mehrere Rahmenverträge, gilt dieser AV-Vertrag für alle. Er gilt ab seinem Abschluss und bis zum Ende des Rahmenvertrags und gegebenenfalls darüber hinaus bis zur Löschung der von der Auftragsverarbeitung betroffenen Hosting-Daten durch den Auftragnehmer.

Verhältnis zu anderen vertraglichen Vereinbarungen

Die Bestimmungen dieses AV-Vertrags ergänzen die Bestimmungen der übrigen vertraglichen Vereinbarungen zwischen den Vertragsparteien. Bei Abweichungen gehen die Bestimmungen dieses AV-Vertrags, sofern nicht ausdrücklich anders vereinbart, vor.

Vertrag zur Auftragsverarbeitung

Rollen und Zuständigkeiten

Verantwortlicher

Der Auftraggeber bestätigt und der Auftragnehmer anerkennt, dass der Auftraggeber für die Verarbeitung der Hosting-Daten gemäss anwendbarem Datenschutzrecht verantwortlich ist und bleibt. Der Auftraggeber nimmt somit die Rolle des Verantwortlichen ein.

Das gilt gegenüber dem Auftragnehmer auch, wenn der Auftraggeber gegenüber Dritten als Auftragsverarbeiter tätig ist und den Auftragnehmer aus Sicht solcher Dritter als Unter-Auftragsverarbeiter nutzt.

Auftragsverarbeiter

Der Auftragnehmer anerkennt, dass der Auftraggeber verpflichtet ist, dem Auftragnehmer bei Inanspruchnahme von Services einige seiner Pflichten aus dem anwendbaren Datenschutzrecht vertraglich zu übertragen.

Der Auftragnehmer nimmt in Bezug auf die Verarbeitung betroffener Hosting-Daten die Rolle des Auftragsverarbeiters ein.

Pflichten des Auftragnehmers

Beschränkung der Auftragsverarbeitung

Der Auftragnehmer verpflichtet sich, die Hosting-Daten nur gemäss den anwendbaren vertraglichen Vereinbarungen und den dokumentierten Weisungen des Auftraggebers zu verarbeiten.

Die dokumentierten Weisungen ergeben sich aus der Beschreibung der Services inkl. allfälliger Dokumentation durch den Auftragnehmer sowie die Nutzung und Konfiguration der Services und Features durch den Auftraggeber und ihm zuzurechnende Dritte.

Vorbehalten bleiben in jedem Fall Einschränkungen durch sowie die Erfüllung von gesetzlichen oder regulatorischen Pflichten. In solchen Fällen informiert der Auftragnehmer den Auftraggeber vorgängig, soweit ihm dies im konkreten Fall nicht verboten ist.

Sorgfalt und Vertraulichkeit

Der Auftragnehmer sorgt für die Einhaltung der Bestimmungen dieses AV-Vertrags durch die mit der Auftragsverarbeitung betrauten Mitarbeiter und die anderen für den Auftragnehmer tätigen Personen, die Zugriff auf die Hosting-Daten erhalten. Der Auftragnehmer verpflichtet sich zudem, Personen mit Zugriff auf die Hosting-Daten zur Wahrung der Vertraulichkeit (auch über die Dauer ihrer Tätigkeit für den Auftragnehmer hinaus) zu verpflichten.

Technische und organisatorische Massnahmen (TOM)

Der Auftragnehmer verpflichtet sich, im Interesse der Vertraulichkeit, der Integrität und der vertragsgemässen Verfügbarkeit der Hosting-Daten, den angebotenen Services angemessene technische und organisatorische Massnahmen zu treffen. Der Auftragnehmer implementiert insbesondere Massnahmen zur physischen Sicherheit, logischen Sicherheit und Personalsicherheit sowie Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen. Bei der Auswahl der Massnahmen berücksichtigt der Auftragnehmer auch den Stand der Technik sowie die Implementierungskosten. Der Auftragnehmer passt die getroffenen technischen und organisatorischen Massnahmen laufend an, soweit er dies für geboten hält, wobei das Schutzniveau der im Anhang dokumentierten Massnahmen nicht unterschritten werden darf.

Die Beurteilung, ob das Schutzniveau der dokumentierten Massnahmen für die im konkreten Fall zu verarbeitenden Hosting-Daten angemessen ist und damit eine Nutzung der Services zulässt, obliegt dem Auftraggeber.

Verhalten bei Datensicherheitsverletzung

Der Auftragnehmer verpflichtet sich, den Auftraggeber ohne Verzug schriftlich zu informieren, sobald der Auftragnehmer Kenntnis von einer Datensicherheitsverletzung erlangt, die Hosting-Daten betrifft. Dabei hat der

Vertrag zur Auftragsverarbeitung

Auftragnehmer dem Auftraggeber die Art und das Ausmass der Verletzung sowie mögliche Abhilfemassnahmen schriftlich mitzuteilen.

Die Vertragsparteien treffen gemeinsam die erforderlichen Massnahmen, um den Schutz der Hosting-Daten sicherzustellen und mögliche nachteilige Folgen für die betroffenen Personen als auch für die Vertragsparteien zu mildern.

Überdies verpflichtet sich der Auftragnehmer, dem Auftraggeber auf schriftliche Anfrage ausreichende Informationen zur Verfügung zu stellen, damit dieser allfälligen Pflichten gemäss dem anwendbaren Datenschutzrecht nachkommen kann, insbesondere Melde- und Informationspflichten.

Erfüllung von Betroffenenrechten

Der Auftragnehmer verpflichtet sich, den Auftraggeber auf schriftliche Anfrage und gegen separate angemessene Vergütung sowie im Rahmen der betrieblichen Ressourcen und Möglichkeiten des Auftragnehmers bei der Erfüllung von Betroffenenrechten (z.B. Auskunfts-, Berichtigungs- und Löschansprüche betreffend Hosting-Daten) gemäss anwendbarem Datenschutzrecht zu unterstützen. Richtet sich eine betroffene Person mit Anfragen direkt an den Auftragnehmer, wird dieser die betroffene Person an den Auftraggeber verweisen und diesen schriftlich darüber informieren. Voraussetzung dafür ist, dass der Auftragnehmer eine solche Zuordnung an den Auftraggeber gestützt auf die Angaben der betroffenen Person vornehmen kann.

Unterstützung bei Konsultationen

Der Auftragnehmer ist auf schriftliche Anfrage und gegen separate angemessene Vergütung sowie im Rahmen seiner betrieblichen Ressourcen und Möglichkeiten bereit, den Auftraggeber bei Datenschutz-Folgenabschätzungen und bei Konsultationen von Aufsichtsbehörden zu unterstützen.

Herausgabe und Löschung von Hosting-Daten

Der Auftraggeber bestimmt selbst über die Hosting-Daten und deren Format. Im Rahmen der Nutzung der Services hat er jederzeit Zugriff, um die Hosting-Daten an einen anderen Ort zu sichern oder zu löschen. Mit Ende des Rahmenvertrags werden die Hosting-Daten beim Auftragnehmer gelöscht.

Von diesen Punkten ausgenommen sind Logs auf Infrastrukturebene des Auftragnehmers, wie z.B. von Netzwerk-Geräten, sowie Fälle, in denen Hosting-Daten erst zu einem späteren Zeitpunkt gelöscht werden können, insbesondere gemäss gesetzlichen und regulatorischen Verpflichtungen.

Unter-Auftragsverarbeiter

Abgrenzung von Nebenleistungen

Als Unter-Auftragsverarbeiter im Sinne dieses AV-Vertrags sind jene Dienstleister zu verstehen, welche unmittelbar in die Verarbeitung von Hosting-Daten involviert sind und dabei in Kontakt mit den Hosting-Daten kommen.

Nicht hierzu gehören Basisinfrastruktur-Dienstleistungen wie Internet-Konnektivität sowie Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikations-, Post- oder Transportdienstleistungen, bei Wartung und Support durch Hersteller oder bei der Entsorgung von Datenträgern in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Hosting-Daten auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen bzw. Kontrollmassnahmen zu treffen.

Abgrenzung von anderen Auftragsverarbeitern

Zieht der Auftragnehmer bei der Verarbeitung von Hosting-Daten Dritte bei, bleibt er gegenüber dem Auftraggeber Auftragsverarbeiter und erfüllt die diesbezüglichen Pflichten aus diesem AV-

Vertrag zur Auftragsverarbeitung

Vertrag. Der beigezogene Dritte ist Unter-Auftragsverarbeiter des Auftragnehmers.

Davon zu unterscheiden sind Fälle, in denen der Auftragnehmer dem Auftraggeber einen direkten Vertragsschluss mit dem Drittdienstleister vermittelt und der Drittdienstleister direkt Auftragsverarbeiter des Auftraggebers wird. In solchen Fällen hat der Auftraggeber selbst dafür besorgt zu sein, unter dem anwendbaren Datenschutzrecht allenfalls notwendige Vereinbarungen mit dem Drittdienstleister zu treffen.

Beizug von Unter-Auftragsverarbeitern

Der Auftragnehmer ist berechtigt, Unter-Auftragsverarbeiter im Rahmen der Erbringung von Services beizuziehen. Der Auftragnehmer wird den Auftraggeber vorab in geeigneter Weise informieren, sobald der Auftragnehmer nach Inkrafttreten dieses AV-Vertrags in Bezug auf bestehende Services neue Unter-Auftragsverarbeiter beizieht oder bestehende austauscht. Mit Ablauf von 30 Tagen nach dem Datum der Mitteilung gilt der neue oder ausgetauschte Unter-Auftragsverarbeiter als genehmigt. Im Fall der Ablehnung hat der Auftraggeber innert dieser Frist die Möglichkeit der Kündigung gemäss den vertraglichen Bestimmungen bzw. die Möglichkeit, den betroffenen Service nicht weiter zu nutzen.

Vereinbarung mit Unter-Auftragsverarbeitern

Beim Beizug von Unter-Auftragsverarbeitern ist der Auftragnehmer verpflichtet, mit diesen im erforderlichen Umfang eine Vereinbarung zu treffen, die dem Auftragnehmer die Einhaltung der Bestimmungen dieses AV-Vertrags ermöglicht.

Übermittlung in Drittländer

Der Auftragnehmer verpflichtet sich, bei Übermittlung von personenbezogenen Daten in Drittländer einen geeigneten Datenschutz zu gewährleisten, z.B. durch genehmigte Standarddatenschutzklauseln. Als Drittländer

gelten alle Länder ausserhalb der Schweiz und des Europäischen Wirtschaftsraumes (EWR).

Pflichten des Auftraggebers

Rechtmässigkeit der Auftragsverarbeitung

Der Auftraggeber ist für die Rechtmässigkeit der Verarbeitung der Hosting-Daten, einschliesslich der Zulässigkeit der Auftrags- bzw. Unter-Auftragsverarbeitung, verantwortlich.

Schutz der Hosting-Daten

Der Auftraggeber trifft in seinem Verantwortungsbereich (z.B. für seine eigenen Systeme und Applikationen sowie im Rahmen seiner Nutzung der Services) selbständig angemessene technische und organisatorische Massnahmen zum Schutz der Hosting-Daten.

Informationspflicht

Der Auftraggeber verpflichtet sich, den Auftragnehmer unverzüglich zu informieren, wenn er in der Erbringung von Services durch den Auftragnehmer Verletzungen von anwendbarem Datenschutzrecht feststellt.

Informations- und Prüfrecht

Informationsrecht

Der Auftraggeber ist berechtigt, vom Auftragnehmer auf schriftliche Anfrage alle Informationen zu erhalten, die er vernünftigerweise zum Nachweis der Einhaltung dieses AV-Vertrags gegenüber betroffenen Personen oder Datenschutz-Aufsichtsbehörden benötigt.

Prüfrecht

Der Auftraggeber ist berechtigt, selbst oder mit einem beauftragten und zur Vertraulichkeit verpflichteten Prüfer die Einhaltung dieses AV-Vertrags durch den Auftragnehmer zu prüfen. Werden nach Vorlage entsprechender Nachweise

Vertrag zur Auftragsverarbeitung

Verletzungen des AV-Vertrags durch den Auftragnehmer festgestellt, hat dieser so bald wie möglich und kostenlos geeignete Korrekturmassnahmen zu implementieren.

Nachweis von Massnahmen

Der Nachweis der Einhaltung dieses AV-Vertrags kann auch erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach ISO/IEC 27001).

Einschränkung der Informations- und Prüfrechte

Die vorstehenden Informations- und Prüfrechte des Auftraggebers bestehen nur insoweit, als die vertraglichen Bestimmungen dem Auftraggeber keine anderen Informations- und Prüfrechte einräumen, die den einschlägigen Anforderungen des anwendbaren Datenschutzrechts entsprechen. Weiter stehen diese Informations- und Prüfrechte unter dem Vorbehalt des Verhältnismässigkeitsgebots und der Wahrung der schutzwürdigen Interessen (insbesondere Sicherheits- und Geheimhaltungsinteressen) des Auftragnehmers. Vorbehältlich einer anderslautenden Vereinbarung zwischen den Vertragsparteien trägt der Auftraggeber sämtliche Kosten der Information und Prüfung, einschliesslich nachgewiesener interner Kosten des Auftragnehmers.

Änderung dieses AV-Vertrags

Einseitiges Änderungsrecht

Der Auftragnehmer behält sich vor, diesen AV-Vertrag zu ändern, (a) wenn dies zur Anpassung an rechtliche Entwicklungen erforderlich erscheint, oder (b) wenn dies nicht zu einer Verschlechterung der Gesamtsicherheit der Auftragsverarbeitung führt und sich (nach Ermessen des Auftragnehmers) nicht erheblich nachteilig auf die Rechte der von der Auftragsverarbeitung betroffenen Personen auswirkt.

Genehmigung

Der Auftragnehmer teilt dem Auftraggeber beabsichtigte Änderungen dieses AV-Vertrags gemäss Abschnitt "Einseitiges Änderungsrecht" spätestens 30 Tage vor Wirksamwerden schriftlich mit; mit Ablauf dieser Frist gelten die Änderungen als genehmigt. Im Fall der Ablehnung hat der Auftraggeber innert dieser Frist die Möglichkeit der Kündigung gemäss den vertraglichen Bestimmungen.

Schlussbestimmungen

Elektronische Gültigkeit

Dieser AV-Vertrag kann auf elektronischem Weg zwischen den Vertragsparteien vereinbart und geändert werden.

Schriftliche Mitteilungen

Verlangt dieser AV-Vertrag eine schriftliche Aufforderung oder Mitteilung, so genügt (für Mitteilungen an den Auftraggeber) eine E-Mail an die unter control.cloudscale.ch hinterlegte Adresse des Auftraggebers bzw. (für Mitteilungen an den Auftragnehmer) eine E-Mail an support@cloudscale.ch dem Schriftformerfordernis.

Vertrag zur Auftragsverarbeitung

Rechtswahl und Gerichtsstand

Die gemäss Rahmenvertrag festgelegte Rechts- und Gerichtsstands-Wahl gilt für sämtliche Streitigkeiten und Ansprüche im Zusammenhang mit diesem AV-Vertrag. Davon unberührt bleiben zwingend anwendbares Recht und zwingende Gerichtsstände.

Salvatorische Klausel

Sollten einzelne oder mehrere Bestimmungen dieses AV-Vertrags unwirksam oder nichtig sein oder werden, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. An die Stelle der unwirksamen oder nichtigen Bestimmungen tritt diejenige Regelung, welche die Vertragsparteien bei Kenntnis des Mangels zum Zeitpunkt des Abschlusses des AV-Vertrags nach Treu und Glauben sowie nach wirtschaftlicher Betrachtungsweise getroffen hätten. Gleiches gilt im Fall etwaiger Lücken des AV-Vertrags.

Inkrafttreten

Diese Fassung ist ab 1. September 2023 anwendbar und ersetzt die bisherige Vereinbarung zur Auftragsdatenverarbeitung.

Vertrag zur Auftragsverarbeitung

Anhang 1: Technische und organisatorische Massnahmen

Abgrenzung der Zuständigkeiten

Der Auftragnehmer bietet IT-Infrastruktur-Dienstleistungen (Infrastructure-as-a-Service / IaaS) an. Bedingt durch die Natur dieser Services bestimmt der Auftraggeber allein über die Daten und deren Verarbeitung. Ebenso ist der Auftraggeber allein verantwortlich für sämtliche Software innerhalb der virtuellen Server ("Kunden-Server"), die der Auftraggeber als Service bzw. Produkt vom Auftragnehmer bezieht, für das Management weiterer durch ihn verwaltbarer Zugriffsrechte sowie für sämtliche Interaktionen mit der bereitgestellten Self-Service-Plattform ("Control Panel" und "API") im Kontext seines Vertragsverhältnisses. Im Hinblick auf die Daten, Kunden-Server und die Self-Service-Plattform sowie die Personen, denen er hierfür Berechtigungen erteilt, trifft der Auftraggeber selbständig die für angemessen erachteten technischen und organisatorischen Massnahmen (inklusive Backups in Abhängigkeit der konkreten Daten, benutzten Formate, Schutzbedarf etc.).

Technische und organisatorische Massnahmen der cloudscale.ch AG

Im Folgenden werden die technischen und organisatorischen Massnahmen beschrieben, die im Zuständigkeitsbereich des Auftragnehmers für die Sicherheit der Hosting-Daten getroffen werden.

Physische Sicherheit:

- Der Zutritt zum Bürostandort wird mittels elektronisch gestütztem Schlüssel-Schliess-System auf berechnigte Personen eingeschränkt. Die Vergabe und Rücknahme von Schlüsseln wird protokolliert.
- Durch ein Schliess-System mit persönlichen Badges und/oder anderweitige Identifizierung (z.B. ID/Biometrie) stellen die jeweiligen

Datacenter-Betreiber sicher, dass nur berechnigte Personen Zutritt zu den Cloud-Systemen des Auftragnehmers haben.

- Die jeweiligen Datacenter-Betreiber sind vertraglich verpflichtet sicherzustellen, dass Dritte an den Cloud-Standorten von einer berechnigten Person vorangemeldet und/oder begleitet werden.
- Die jeweiligen Datacenter-Betreiber stellen eine redundante, unterbrechungsfreie Stromzufuhr samt Notstromversorgung mittels Diesel-Generatoren sowie eine redundant ausgelegte Klimatisierung sicher.
- Die jeweiligen Datacenter-Betreiber setzen Brandschutzmassnahmen um, insbesondere durch Einsatz von Branderkennungs- und Brandbekämpfungssystemen.
- Die Arbeitsgeräte der Mitarbeiter des Auftragnehmers setzen Datenträgerverschlüsselung gemäss interner Richtlinie ein.
- Hosting-Daten werden auf den Datenträgern in den Storage-Clustern ("at rest") nur verschlüsselt abgelegt.
- Hosting-Daten werden in den Storage-Clustern zum Schutz gegen Systemausfälle bzw. Hardware-Defekte (nicht jedoch zur Wiederherstellung früherer Datenstände) repliziert gespeichert.
- Netzwerkverbindungen der Kunden-Server untereinander und ins Internet sind redundant ausgelegt.
- Alle für den Betrieb der Kunden-Server relevanten Systeme sind redundant ausgelegt oder es stehen Hot-Standby-Systeme bereit.
- Die Systeme sind darauf ausgelegt, dass auch bei einem schwerwiegenden Ereignis (z.B. Feuer) an einem Cloud-Standort der Betrieb an den anderen Standorten aufrechterhalten werden kann.

Vertrag zur Auftragsverarbeitung

Logische Sicherheit:

- Zugriffsberechtigungen auf die Cloud-Systeme des Auftragnehmers werden gemäss interner Richtlinie vergeben und überprüft. Bei Mitarbeiter-Austritten werden die Berechtigungen zeitnah gemäss dokumentiertem Prozess entzogen.
- Das Netzwerk ist gemäss interner Vorgabe in verschiedene Zonen unterteilt und der Datenverkehr zwischen den Zonen wird eingeschränkt.
- Management-Zugänge zu produktiven Systemen der Cloud-Infrastruktur sind nur über verschlüsselte Verbindungen erreichbar.
- Die Kunden-Server sind durch "Full Virtualization" voneinander getrennt.
- Volumes können via Control Panel und API nur an Server im entsprechenden Kundenprojekt angeschlossen werden.
- Private Layer-2-Netze von Kunden-Servern sind durch Einsatz von VLAN oder VXLAN voneinander getrennt.

Personalsicherheit:

- Die Mitarbeiter werden im Bereich Informationssicherheit (z.B. zu gesetzlichen Bestimmungen oder aktuellen Bedrohungen) mehrmals pro Jahr geschult bzw. sensibilisiert.

Regelmässige Überprüfung, Bewertung und Evaluierung:

- Der Betrieb der produktiven Systeme wird 24/7 via Monitoring-Systeme (intern betriebenes Monitoring-System und externe Monitoring-Dienste) überwacht und das Technik-Team (zu Bürozeiten) bzw. der Pikett-Mitarbeiter (ausserhalb der Bürozeiten) bei Überschreiten definierter Schwellwerte automatisch alarmiert.
- Erfasste Security Incidents werden nachbearbeitet bzw. reviewed.

- Die cloudscape.ch AG ist nach ISO/IEC 27001, 27017 und 27018 zertifiziert. Es wird ein Informationssicherheits-Managementsystem (ISMS) gepflegt, um die Zertifizierungen aufrecht zu erhalten.

Sicherheitsrelevante Funktionen der Services

Im Folgenden werden Funktionen und Eigenschaften der Services beschrieben, die der Auftraggeber nutzen kann, um in seinem Verantwortungsbereich die Sicherheit der Daten und deren Verarbeitung zu unterstützen.

- Fingerprints der initialen SSH-Host-Keys von Kunden-Servern können im Control Panel verifiziert werden (sofern dies vom Image des Kunden-Servers unterstützt wird).
- Für den Zugriff auf das Control Panel wird optional Zwei-Faktor-Authentifizierung (2FA, TOTP-basiert) bzw. die Nutzung eines externen Identity-Providers unterstützt.
- Private Netze erlauben die Segmentierung bzw. Abschottung virtueller Server untereinander und gegenüber dem Internet.
- Der Zugriff von fremden Accounts bzw. Organizations und/oder API-Keys auf eigene Projekte kann wahlweise als "read/write" oder als "read-only" gewährt werden.
- Der Zugriff auf Objekte im Object Storage kann auf "Private" oder "Public" gesetzt bzw. mittels Policies gesteuert werden.
- Hosting-Daten können durch den Auftraggeber zusätzlich verschlüsselt werden (z.B. mittels LUKS bei Nutzung des CSI-Drivers oder mittels SSE-C beim Object Storage).
- Mehrere Cloud-Standorte erlauben (zusätzlich zu Backups ausserhalb der Infrastruktur des Auftragnehmers) geo-redundant ausgelegte Setups und/oder die

Vertrag zur Auftragsverarbeitung

geo-redundante Speicherung der Hosting-Daten je nach Bedarfsanalyse des Auftraggebers.

- Floating IPs ermöglichen das Verschieben einer gleichbleibenden öffentlichen IP-Adresse zwischen bestimmten Kunden-Servern in einem Fail-over-Setup, z.B. bei Wartungen oder Incidents.
- Mittels Konfiguration von Anti-Affinity kann sichergestellt werden, dass eine Gruppe von Kunden-Servern auf unterschiedlichen physischen Hosts läuft, z.B. in einem Fail-over- bzw. Load-balancing-Setup.
- Durch Abonnieren der Statusmeldungen des Auftragnehmers können vor Wartungsarbeiten, bei denen relevante Auswirkungen auf die Services des Auftraggebers erwartet werden, angemessene Vorkehrungen (z.B. ein Fail-over) getroffen werden.