BOC Cloud Services

Serviceangebot, Datenschutz, IT-Sicherheit und Compliance

Zuletzt geändert: 2025-09-05

BOC Group
Design your Enterprise

Inhalt

1. Übersicht

BOC Cloud Services ermöglichen es Ihnen, BOC-Produkte sicher und zuverlässig zu nutzen, ohne sie lokal installieren oder eigene IT-Ressourcen bereitstellen zu müssen. Wir bieten verschiedene Serviceoptionen, um die individuellen Anforderungen unserer Kunden zu erfüllen und unser Service und Support Team bietet Ihnen dabei bestmögliche Unterstützung. Dabei profitieren Sie von unserer langjährigen Erfahrung in der Entwicklung erstklassiger Produkte und Lösungen, im Bereitstellen und Betreiben von Services sowie in der Integration von BOC Cloud Services in Kundeninfrastrukturen.

In diesem Dokument geben wir einen Überblick über unser Cloud Service Angebot, einschließlich Service Level Agreement und Berichte, Pflegeservice und Hotline-Support. Darüber hinaus wird gezeigt, wie Datenschutz- und IT-Sicherheitsmaßnahmen umgesetzt werden und wie die Einhaltung verschiedener branchenspezifischer Anforderungen gewährleisten.

Wir nehmen die Sicherheit und den Schutz der Daten unserer Kunden sehr ernst und haben eine Reihe von Maßnahmen ergriffen, um die Vertraulichkeit, Integrität und Verfügbarkeit ihrer Daten zu gewährleisten. Zu diesen Maßnahmen gehören Optionen zur Datenbankverschlüsselung, Verschlüsselung bei der Übertragung, Business Continuity Management und Penetration Tests.

Wir verpflichten uns zur Einhaltung aller einschlägigen Vorschriften und Industrienormen und haben eine Reihe von Zertifizierungen und Audits erhalten, die unser Engagement belegen (ISO 27001, ISO 27018). Außerdem verfügen wir über Verfahren für das Risikomanagement, die Verwaltung von Lieferantenrisken und den Schutz von geistigem Eigentum.

Vielen Dank für Ihr Interesse an BOC Cloud Services. Wir freuen uns darauf, mit Ihnen zusammenzuarbeiten und Ihre Geschäftsanforderungen zu unterstützen.

2. Serviceangebot

BOC Cloud Services ist der bevorzugte Hosting Service Provider für BOC-Produkte (ADONIS, ADOIT, ADOGRC) sowie die dazugehörigen Module, Add-Ons und Web-Services. Kunden haben die Wahl, ihre bestehenden BOC-Lizenzen von BOC Cloud Services betreiben zu lassen (Operations-Only) oder BOC-Produkte als Software-as-a-Service (SaaS) zu beziehen. In beiden Fällen sorgt BOC Cloud Services für einen effizienten und unterbrechungsfreien Betrieb ihrer Services in unserer Cloud-Umgebung.

Um sicherzustellen, dass unsere Kunden die bestmögliche Nutzung unserer Produkte erleben, bieten wir nicht nur eine garantierte Serviceverfügbarkeit (2.2. Service Level Agreement und Berichte), unser SaaS-Angebot beinhaltet auch korrektive und präventive Wartungen (2.3 Softwarepflege) sowie Hotline-Support für Serviceanfragen und Störungsmeldungen (2.4. Hotline).

Weitere Informationen über Module, Add-Ons und Web-Services die den von Ihnen gewählten Service verbessern können, finden Sie auf dem BOC Group Marketplace.

2.1. Servicebeschreibung

Kunden, die sich für BOC Cloud Services entscheiden, erhalten Zugriff auf das komplette Servicepaket für das jeweilige BOC-Produkt ihrer Wahl. Dies beinhaltet:

- Bereitstellung der BOC-Produktinstanz an einem der BOC Cloud Standorte,
- Betrieb der Produkte mit einer 24x7 Serviceverfügbarkeit,
- Integration der Produktinstanz mit vom Kunden verwalteten Identity Providern,
- Automatisierte Sicherung von Kundendaten an zwei getrennten Standorten,
- Rollout von Software-Updates in gemeinsam vereinbarten Wartungsfenstern,
- Überwachung der Verfügbarkeit des Services einschließlich der Systemleistung,

- Kapazitätsüberwachung und Verwaltung der zugrundeliegenden Infrastruktur,
- Regelmäßige Sicherheitsupdates für alle beteiligten Systeme, die außerhalb der üblichen Geschäftszeiten durchgeführt werden,
- Pflege von Plänen für die Geschäftskontinuität und die Wiederherstellung im Katastrophenfall einschließlich regelmäßiger Tests sowie
- Zugang zum BOC Support Desk für Incident- und Problem-Management sowie die Bearbeitung von Serviceanfragen.

Um alle Anforderungen in Bezug auf den Datenstandort und Verfügbarkeit zu erfüllen, werden BOC Cloud Services an zwei verschiedenen Datenstandorten bereitgestellt. Die verfügbaren Optionen sind:

Option 1: Deutschland

- Primärer IaaS-Anbieter
  - Amazon Web Services EMEA Sàrl, 38 Avenue John F. Kennedy, L-1855 Luxemburg, Rechenzentrum in Deutschland (eu-central-1).
- Disaster Recovery IaaS-Anbieter:
  - Amazon Web Services EMEA Sàrl, 38 Avenue John F. Kennedy, L-1855 Luxemburg, Rechenzentrum in Frankreich (eu-west-3).

Option 2: Schweiz

- Primärer IaaS-Anbieter
  - Cloudsigma AG, Badenerstrasse 549, 8048 Zürich, Schweiz, Rechenzentrum in der Schweiz.
- Disaster Recovery IaaS-Anbieter:
  - Amazon Web Services EMEA Sàrl, 38 Avenue John F. Kennedy, L-1855 Luxemburg, Rechenzentrum in Frankreich (eu-west-3).

2.2. Service Level Agreement und Berichte

BOC ist sich seiner Verantwortung für die Verfügbarkeit der Services bewusst und hat daher umfangreiche technische und organisatorische Maßnahmen ergriffen, um Systeme so robust wie möglich zu machen und unseren Kunden eine ununterbrochene Benutzererfahrung zu ermöglichen. Sollte es trotz aller vorbeugenden Maßnahmen zu unerwarteten Störungen kommen, werden diese umgehend durch automatische Systemwiederherstellungen oder, falls erforderlich, durch manuelle Maßnahmen unseres erfahrenen Support Desk Teams behoben.

Als Teil der vertraglichen Vereinbarung stellt BOC ein Service Level Agreement (SLA) mit wettbewerbsfähigen Reaktions- und Wiederherstellungszeiten bereit. So garantiert BOC beispielsweise eine 99%ige Verfügbarkeit seiner Services mit geplanten Wartungsfenstern außerhalb der normalen Geschäftszeiten, Reaktionszeiten von weniger als einer Stunde bei Störungsmeldungen und kurze Wiederherstellungszeiten, falls eine Störung zu einer Unterbrechung des Services führen sollte.

Unser Versprechen eines verfügbaren Services wird durch die vertragliche Verpflichtung ergänzt, Service Credits in Höhe von 25 % der jeweiligen Servicegebühr zu gewähren, wenn BOC wiederholt Serviceausfälle nicht innerhalb des garantierten Zeitraums beheben kann.

2.3. Softwarepflege

Im Rahmen der Softwarepflege stellt die BOC Group regelmäßig neue Versionen ihrer Services zur Verfügung. Solche Releases können unter anderem folgendes enthalten:

- Einführung neuer Funktionalitäten,
- Präventivmaßnahmen gegen Sicherheitsbedrohungen und Fehler,
- Korrektur von Fehlern und

- Anpassung des Services an geänderte gesetzliche Anforderungen.

Um den Kunden die bestmögliche Balance zwischen Versionsstabilität und frühzeitigem Zugriff auf neue Funktionalitäten zu ermöglichen, kann jeder Kunde mit einer dedizierten BOC Cloud Instanz selbst entscheiden, wann und wie oft neue Releases in dessen Instanz eingeführt werden. Sicherheitsrelevante Updates können auch sofort und ohne Vorankündigung eingeführt werden.

Je nach Release-Typ der Softwareversion (Major, Minor oder Long-Term-Support (LTS)) gelten unterschiedliche Pflegezeiträume. Informationen zum aktuellen Pflegezeitraum finden Sie im Online-Dokumentationszentrum von ADONIS und ADOIT.

Neue Releases werden mit angepasster Dokumentation und einer detaillierten Beschreibung der neuen Funktionalitäten ausgeliefert. Werfen Sie einfach einen Blick auf unsere aktuellen Public Release Announcements (ADONIS / ADOIT) und machen Sie sich mit den neuen Funktionen unserer Services vertraut. Oder abonnieren Sie unseren Newsletter, um Ihre Transformationsinitiativen mit Einblicken aus Expertinnen-Artikeln, Kundenerfahrungen, Produkt-Updates und mehr zu bereichern!

2.4. Hotline

Ein spezialisierter Support Desk ist für alle BOC Cloud Services verfügbar. Der technische Support Desk der BOC Group bearbeitet Störungsmeldungen und Serviceanfragen per E-Mail oder Telefon. Unser Team aus qualifizierten und erfahrenen Fachleuten steht Ihnen während der Geschäftszeiten zur Verfügung und stellt sicher, dass alle Probleme schnell und effektiv gelöst werden. Die Spezialisten der BOC Group beantworten Ihre technischen Fragen zu den BOC Cloud Services mit höchster Priorität. Im Rahmen unseres Service Level Agreements garantieren wir Reaktionszeiten von weniger als einer Stunde.

Die BOC Group hat organisatorische Maßnahmen ergriffen, um sicherzustellen, dass unser Support Desk Team über das Fachwissen und die Kenntnisse verfügt, um alle auftretenden Situationen zu bewältigen, und dass ausreichend personelle Ressourcen auch in Situationen mit hoher Nachfrage verfügbar sind. Wir investieren regelmäßig in Schulungen und Weiterbildungen, um sowohl die Vertraulichkeit Ihrer Daten als auch einen kundenfreundlichen und zuvorkommenden Service zu gewährleisten.

Servicezeiten des BOC Support Desks:

Montag-Freitag, 08:00-18:00 Uhr MEZ, ausgenommen österreichische Feiertage

BOC Support Kanäle:

Telefon: +43 1 905 10 81-2880

E-Mail: hotline@boc-group.com

3. Vertraulichkeit, Integrität und Verfügbarkeit

Als IT-Dienstleister legt die BOC Group höchsten Wert auf den Schutz von Kundendaten im Hinblick auf ihre Vertraulichkeit, Integrität und Verfügbarkeit. Die von der BOC Group implementierten technischen und organisatorischen Maßnahmen zur Gewährleistung der Informationssicherheit und des Datenschutzes umfassen Kontrollen um:

- den Zugriff auf Datenverarbeitungssysteme durch Unbefugte zu verhindern (einschließlich Verschlüsselungsverfahren),
- sicherzustellen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten nur auf jene Daten zugreifen können, die ihrer Zugangsberechtigung entsprechen (Mandantentrennung),

- zu gewährleisten, dass Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können,
- zu gewährleisten, dass nach der Tätigkeit überprüft und festgestellt werden kann, ob und von wem Daten in Datenverarbeitungssysteme eingegeben, verändert oder aus ihnen entfernt wurden (Eingabekontrolle),
- dafür zu sorgen, dass personenbezogene Daten, die im Auftrag anderer verarbeitet werden, nur gemäß den Weisungen des Auftraggebers verarbeitet werden (Auftragskontrolle),
- sicherzustellen, dass Daten vor versehentlicher Zerstörung oder Verlust geschützt sind,
- sicherzustellen, dass die für unterschiedliche Zwecke erhobenen Daten getrennt verarbeitet werden.

3.1. Optionen zur Datenbankverschlüsselung

Um unsere Kunden bei der Einhaltung strenger Compliance-Vorschriften zu unterstützen, bietet BOC Cloud Services verschiedene Modelle zur Datenbankverschlüsselung an, die auf bewährten Verschlüsselungstechnologien des Datenbankherstellers und modernstem Schlüsselmanagement basieren. Die Verschlüsselung wird mittels AES-256 implementiert und umfasst die Verschlüsselung von Dateien, Transaktionsprotokollen und Sicherungskopien. Die Kunden können zwischen den folgenden Schlüsselverwaltungsoptionen wählen.

3.1.1. Key managed by BOC

BOC verwaltet den Verschlüsselungsschlüssel (Key Encryption Key - KEK) in Azure Key Vault. Kunden können jederzeit die Verschlüsselung der von SaaS-Kunden verwendeten Datenbank beantragen. Diese Option ist für alle BOC Cloud Standorte verfügbar.

3.1.2. Bring Your Own Key (BYOK)

Es kann auch ein Bring Your Own Key Modell zur Datenbankverschlüsselung verwendet werden. Dazu muss der Kunde einen Verschlüsselungsschlüssel von einem der unterstützten HSM-Modelle exportieren, um diesen in das BOC Key Vault importieren zu können. Diese Option ist für alle BOC Cloud Standorte verfügbar.

3.1.3. Hold Your Own Key (HYOK)

Wenn der Kunde lieber seine eigenen Schlüssel für den Schutz des Datenverschlüsselungsschlüssel (Data Encryption Key - DEK) verwenden möchte, ist die beste Wahl das Hold Your Own Key Modell zu nutzen. Dabei verwaltet der Kunde einen Schlüsselspeicher in seinem Azure-Konto und weist einen Schlüssel für die SaaS-Datenbank zu. Diese Option ist für alle BOC Cloud Standorte verfügbar.

3.2. Verschlüsselung bei der Übertragung

Der gesamte Datenverkehr zur und von der BOC Cloud-Plattform wird bei der Übertragung über das öffentliche Internet mit modernsten kryptografischen Methoden verschlüsselt. Dazu gehören HTTPS mit TLS >=1.2 für den Datenverkehr der Endnutzer sowie des API-Zugangs und TLS 1.3 und IPSec für den administrativen Zugang des Betriebsteams und für Site-to-Site-Verbindungen.

3.3. Business Continuity Management

Die Cloud Services von BOC sind das Betriebsmodell für viele Kunden, die auf optimale Zuverlässigkeit, Leistung und Sicherheit für ihre BOC Produktkonten angewiesen sind. Um diese Servicequalitätsmerkmale auch in ungünstigen Situationen zu gewährleisten, hat BOC einen auf einer Folgenabschätzung basierenden Business Continuity Plan speziell für die angebotenen Cloud Services entwickelt, der alle relevanten Services und Anlagen umfasst.

BOC-Produkte speichern Daten in relationalen Datenbanken und im Dateisystem auf dem Webserver. Um die Daten im Falle einer unbeabsichtigten Löschung oder Änderung sowie in Katastrophenszenarien, in denen die produktiven Datensätze verloren gehen oder beschädigt werden, zu schützen, wurde ein robustes Sicherungs- und Wiederherstellungsverfahren in die BOC Cloud Services Plattform implementiert.

BOC unterhält dafür einen sekundären Standort für die Wiederherstellung von Services, der sich in angemessener Entfernung zum primären Standort befindet. BOC Cloud Services betreibt die Basisservices an diesen Standorten und führt regelmäßig Wiederherstellungstests durch.

3.4. Penetration Tests

Um die Sicherheit unserer Systeme und Anwendungen zu gewährleisten, führt die BOC Group in regelmäßigen Intervallen Penetration-Tests durch. Durch die regelmäßige Durchführung dieser Tests können Schwachstellen erkannt und behoben werden, bevor sie von einem Angreifer ausgenutzt werden können. Dies dient nicht nur dem Schutz unserer eigenen Systeme, sondern auch dem Schutz der Kunden und ihrer Daten.

Penetration Tests simulieren Hackerangriffe unter kontrollierten Bedingungen und erfüllen zwei Hauptfunktionen. Erstens helfen sie sicherzustellen, dass die Sicherheitsverpflichtungen eingehalten werden. Zweitens dienen sie Schwachstellen in Systemen zu erkennen, um diese in weiterer Folge beheben zu können. Berichte über die durchgeführten Penetration Tests können auf Anfrage gerne zur Verfügung gestellt werden.

4. Compliance

4.1. Datenschutz

Die BOC Group hat sich verpflichtet die Privatsphäre ihrer Kunden und deren Mitarbeiter zu schützen und hat robuste Maßnahmen ergriffen, um die Sicherheit und Vertraulichkeit von persönlichen Daten zu gewährleisten. Ihre Daten werden von uns auf faire und verantwortungsvolle Weise verarbeitet.

Wir sind nach den international anerkannten Standards für das Informationssicherheitsmanagement und den Schutz personenbezogener Daten in der Cloud, ISO 27001 und ISO 27018, zertifiziert. Darüber hinaus halten wir uns als europäischer Anbieter streng an die DSGVO-Anforderungen und sind vollständig konform mit den EU-Datenschutzbestimmungen.

Als SaaS-Anbieter agieren wir in der Rolle eines Auftragsverarbeiters und sind dem Schutz der Privatsphäre unserer Nutzer verpflichtet. In dieser Eigenschaft verarbeiten wir personenbezogene Daten nur im Auftrag unserer Kunden und verwenden diese Daten nur für die in der Auftragsverarbeitungsvereinbarung festgelegten Zwecke. Diese Vereinbarungen gewährleisten, dass die Verarbeitung personenbezogener Daten in Übereinstimmung mit den einschlägigen Datenschutzgesetzen, einschließlich der DSGVO, erfolgt. Insbesondere werden wir

- personenbezogene Daten nur auf dokumentierte Weisung des Kunden verarbeiten,
- sicherstellen, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen Verschwiegenheitspflicht unterliegen,
- geeignete technische und organisatorische Maßnahmen treffen (siehe Abschnitt 3 Vertraulichkeit, Integrität und Verfügbarkeit dieses Dokuments)
- einen weiteren Auftragsverarbeiter nur mit vorheriger Genehmigung beauftragen
- unsere Kunden bei der Erfüllung ihrer Verpflichtung zur Beantwortung von Betroffenenanfragen zu unterstützen.

Datenschutz und die Einhaltung der DSGVO haben für uns höchste Priorität. Deshalb nutzen wir für die Speicherung und Verarbeitung von Kundendaten ausschließlich europäische Rechenzentren. Kunden von BOC Cloud Services können zwischen unseren beiden primären IaaS-Anbietern wählen. Entweder Amazon Web Services EMEA Sàrl (AWS) mit seinem Rechenzentrum in Deutschland oder Cloudsigma AG mit dem Rechenzentrum in der Schweiz. Für Disaster Recovery Zwecke verwenden wir das AWS-Rechenzentrum in Frankreich.

Diese IaaS-Services wurden speziell entwickelt, um die strengen Anforderungen europäischer Unternehmen zu erfüllen. Durch die Nutzung europäischer Rechenzentren können wir sicherstellen, dass Kundendaten ausschließlich in Europa gespeichert und verarbeitet werden. Das hilft unseren Kunden, Ihre spezifischen Datenschutzanforderungen zu erfüllen und die Einhaltung der einschlägigen Vorschriften zu gewährleisten.

Im Hinblick auf eine der bekanntesten datenschutzrechtlichen Entscheidung des Europäischen Gerichtshofs (EuGH), die so genannte Schrems II Entscheidung, möchten wir versichern, dass wir gemeinsam mit unseren IaaS-Anbietern zusätzliche Maßnahmen ergriffen haben, um die vom EuGH aufgezeigten Risiken zu mindern. Zu unseren Maßnahmen gehört die Option für Kunden, ein Hold Your Own Key (HYOK) Modell zu nutzen, bei dem die Kunden die Kontrolle über ihre Verschlüsselungsschlüssel behalten. Gemeinsam mit unseren IaaS-Anbietern stellen wir außerdem sicher, dass wir Anfragen von Strafverfolgungsbehörden ablehnen und, falls die Behörden dies verlangen, nur das erforderliche Minimum an Daten offenlegen.

4.2. Zertifizierungen

4.2.1. ISO 27001

Bei der BOC Group haben die Sicherheit und Vertraulichkeit der Daten unserer Kunden höchste Priorität. Die BOC Cloud Services sind nach ISO 27001 zertifiziert, was unser Engagement für die Einhaltung der höchsten Branchenstandards für das Informationssicherheitsmanagement unterstreicht.

ISO 27001 ist eine der anerkanntesten globalen Normen für das Informationssicherheitsmanagement. Sie umreißt eine Reihe von bewährten Verfahren und Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines Informationssicherheitsmanagementsystems (ISMS). Ein ISMS ist ein Rahmenwerk, das Organisationen bei der Verwaltung und dem Schutz ihrer sensiblen Daten, einschließlich Finanzinformationen, geistigem Eigentum und persönlichen Daten, unterstützt.

Um nach ISO 27001 zertifiziert zu werden, muss eine Organisation eine Reihe von Anforderungen erfüllen, unter anderem:

- Entwicklung und Dokumentation einer Reihe von Strategien und Verfahren für das Management der Informationssicherheit
- Führen eines Inventars der relevanten Anlagen
- Durchführung von Risikobewertungen zur Ermittlung potenzieller Bedrohungen für die Informationsbestände der Organisation
- Durchführung von Kontrollen, um festgestellte Risiken zu minimieren
- Regelmäßige Überprüfung und Überwachung der Wirksamkeit des ISMS
- Ableitung von Verbesserungsinitiativen aus internen und externen Audits

Durch die Erfüllung dieser Anforderungen und den Nachweis der Konformität mit der Norm ISO 27001 kann BOC Cloud Services seinen Kunden und Stakeholdern versichern, dass strenge Maßnahmen zum Schutz sensibler Daten und zur Vermeidung von Datenschutzverletzungen ergriffen werden.

Die international anerkannten Auditoren bescheinigten uns folgende *Overall Impression*: "*The ISMS has already reached a very high level of maturity. For all tasks required by the standard as well as all other relevant procedures, all processes are described in a central process house and illustrated with the in-house tool ADONIS. This enables a very structured approach to be recognized in general. Supporting customers is a recognizably high priority, and therefore all requirements that customers request to support their data protection responsibilities are covered by the corresponding processes.*"

Auf Anfrage stellen wir Ihnen gerne das aktuelle Zertifikat sowie das vollständige Statement of Applicability (SoA) zur Verfügung, welche unser Engagement für die Einhaltung höchster Sicherheits- und Compliance-Standards belegen.

4.2.2. ISO 27018

Wir sind nicht nur nach ISO 27001 zertifiziert, sondern halten uns auch an die Norm ISO/IEC 27018, die sich speziell mit dem Schutz personenbezogener Daten in der Cloud befasst. Diese Norm beschreibt bewährte Verfahren für den Umgang mit und die Verarbeitung von personenbezogenen Daten in einer Cloud-Computing-Umgebung, einschließlich des Schutzes von personenbezogenen Daten, Sicherheit und Compliance. Durch die Einhaltung dieses Standards stellt BOC sicher, dass die personenbezogenen Daten unserer Kunden mit der

größtmöglichen Sorgfalt und Respekt behandelt werden und dass diese Daten in Übereinstimmung mit den einschlägigen Datenschutzbestimmungen verarbeitet werden.

Bitte fordern Sie das vollständige Statement of Applicability (SoA) und unser aktuelles Zertifikat an, um weitere Informationen über unser Engagement für den Datenschutz in der Cloud zu erhalten.

4.3. Sicherheitsaudit

Um sicherzustellen, dass wir die höchsten Sicherheitsstandards einhalten, führen wir regelmäßig interne und externe Audits durch. Unsere internen Audits dienen dazu, mögliche Abweichungen oder Schwachstellen in unseren Systemen und Prozessen zu ermitteln und Maßnahmen zu deren Behebung zu ergreifen. Wir unterziehen uns ebenfalls externen Audits, um Zertifizierungen wie ISO 27001 und ISO 27018 zu erhalten, die unser Engagement für die Einhaltung branchenweit anerkannter Standards belegen.

Zusätzlich zu diesen regelmäßigen Audits werden auf Anfrage unserer Kunden weitere individuelle Kundenaudits durchgeführt. Auf diese Weise können wir auf alle spezifischen Anliegen oder Anforderungen unserer Kunden eingehen und unser Engagement für die Erfüllung ihrer Bedürfnisse unter Beweis stellen.

4.4. Benachrichtigungen

Trotz aller Bemühungen und vorbeugender Maßnahmen können Sicherheitsvorfälle nie zu 100% ausgeschlossen werden. Für solche Kundendaten betreffende Notfallsituationen bzw. Datenschutzverletzungen ist ein klar definierter Prozess vorhanden. Wir verfügen über ein ausgereiftes Verfahren, um auf solche Vorfälle reagieren zu können und diese effektiv zu beheben. Dieser Prozess umfasst:

- Die Identifizierung und Bewertung von Art und Umfang des Vorfalls,
- die Eindämmung des Vorfalls, um weitere Auswirkungen zu verhindern,
- die Untersuchung der Ursache des Vorfalls,
- das Einleiten von Maßnahmen, um ähnliche Vorfälle in Zukunft zu verhindern,
- die Benachrichtigung betroffener Parteien, wie gesetzlich vorgeschrieben oder in den Verträgen unserer Kunden vorgesehen sowie
- die Regelmäßige Berichterstattung über den Stand des Vorfalls und die getroffenen Maßnahmen

Um sicherzustellen, dass die Auswirkungen auf den Betrieb so gering wie möglich sind, kümmert sich ein spezielles Team der BOC Group um die Reaktion auf diese Vorfälle und arbeitet dabei eng mit unseren Kunden zusammen. Unser Ziel ist es, alle Vorfälle schnell und effektiv zu beheben und zu verhindern, dass sie sich in Zukunft wiederholen.

4.5. Risikomanagement

Das Risikomanagement umfasst zyklische Prozesse zur Identifizierung, Analyse, Bewertung und Behandlung von Informationssicherheitsrisiken, um die Kriterien der Risikoakzeptanz zu erfüllen. Der Hauptzweck des Risikomanagements ist die systematische Kontrolle des Risikoniveaus und die Unterstützung bei der Entscheidungsfindung in Bezug auf Investitionen in Sicherheitsmaßnahmen sowie die Integration von neuen Technologien. Das BOC-Risikomanagementprogramm basiert auf dem ISO/ICE 27005-Standard und den Best Practices für die Risikobewertung des NIST (National Institute of Standards and Technology); sowohl Ex-ante-Indikatoren (d. h. proaktiver Ansatz) als auch Ex-post-Indikatoren (d. h. reaktiver Ansatz) werden für die Risikokontrolle bzw. die Durchführung von Präventiv- oder Korrekturmaßnahmen berücksichtigt.

Das BOC-Risikomanagementprogramm berücksichtigt sowohl den internen als auch den externen Kontext des Unternehmens, einschließlich der Anforderungen und Erwartungen der Kunden von BOC Cloud Services in Bezug auf Sicherheit und Datenschutz. Das bedeutet, dass alle Informationen und IKT-Ressourcen (entweder im Besitz von BOC oder von Dritten), wie z. B. Infrastrukturelemente, Systeme, Services, Einrichtungen sowie Prozesse und Verfahren, die für die Entwicklung, den Betrieb und den Support von BOC Cloud Services relevant sind, einer regelmäßigen Risikoidentifizierung, -bewertung und -behandlung unterzogen werden.

In der Identifizierungsphase werden mögliche Bedrohungen und relevante Schwachstellen von Assets definiert und Risikoszenarien formuliert. Darüber hinaus werden die identifizierten Risiken analysiert, um festzustellen, ob die vorhandenen Kontrollen und Maßnahmen für die jeweilige Bedrohung ausreichend sind; andernfalls werden die Risiken bewertet, um ihre wahrscheinlichen Auswirkungen und die Wahrscheinlichkeit ihres Eintretens abzuschätzen. Darüber hinaus werden den bewerteten Risiken Risikobehandlungsstrategien (d. h. vermindern, akzeptieren, verlagern, vermeiden) zugewiesen und die Behandlungsmaßnahmen werden nach Prioritäten geordnet. Die behandelten Risiken müssen nach einem definierten Zeitplan erneut bewertet werden, um die Wirksamkeit der durchgeführten Maßnahmen und die Akzeptanz der Restrisiken zu überprüfen. Die bewerteten Risiken werden der höchsten Managementebene gemeldet, wo weitere Initiativen diskutiert und geplant werden.

Das Risikomanagementprogramm und die Prozesse von BOC werden im Rahmen jährlicher Überprüfungen sowie durch Messung und Analyse der wichtigsten Leistungsindikatoren auf ihre Wirksamkeit hin überwacht, bewertet und bei Bedarf angepasst.

4.6. Lieferantenmanagement

Die BOC Group ist darauf angewiesen, dass die Zulieferer ihre Leistungen in Übereinstimmung mit den gesetzlichen Vorschriften sowie den branchenspezifischen Best Practices und Standards erbringen. Jeder Lieferant wird nach strengen Richtlinien ausgewählt, um die Risiken für die Informationssicherheit zu verringern. Es werden nur Lieferanten ausgewählt, die alle Sicherheitsanforderungen erfüllen und die Sicherheitsbewertung bestehen. Diese Sicherheitsanforderungen entsprechen den branchenrelevanten Standards, regionalen und globalen Vorschriften und Verpflichtungen sowie den Erwartungen der SaaS-Kunden von BOC Group hinsichtlich Sicherheit und Datenschutz.

Die Prozesse des Lieferantenmanagements bestehen aus der Identifizierung und Bewertung von Lieferanten, bei der geeignete Lieferanten ausgewählt werden, nachdem ihre Fähigkeiten in Bezug auf Sicherheit, Compliance und Geschäftserwartungen bewertet wurden; dem Vertragsmanagement, bei dem Sicherheits- und Compliance-Anforderungen wie Geheimhaltungsvereinbarung, Datenverarbeitungsvereinbarung, technische und organisatorische Maßnahmen und andere Erwartungen wie SLA, Audit-Rechte, Zusammenarbeit bei der Behandlung von Zwischenfällen, Kontaktdaten, Konsequenzen bei Nichteinhaltung usw. ausgehandelt und vereinbart werden. Supplier Service Delivery Management beschreibt jenen Bereich, bei dem die Leistung der Lieferanten, die Einhaltung der vereinbarten Sicherheitsmaßnahmen und Änderungen an den erbrachten Leistungen überwacht und gesteuert werden. Darüber hinaus werden im Rahmen der Risikomanagementprozesse relevante Risikoszenarien, die vom jeweiligen Lieferanten und der erbrachten Leistung ausgehen, bewertet und überwacht.

Das SaaS-Angebot von BOC stützt sich auf die Public Cloud Infrastructure-as-a-Service (IaaS) von Amazon Web Services (AWS) und Cloudsigma AG, die in der EU und der Schweiz ansässig sind und die Datenhoheit innerhalb dieser Regionen gewährleisten. Beide Anbieter nutzen hochmoderne Rechenzentren, die die relevanten Sicherheits- und Compliance-Anforderungen erfüllen und nach den Standards ISO 27001, ISO 27018, ISO 27017, ISO 9001 zertifiziert sind und sich der DSGVO verpflichtet haben. Darüber hinaus bietet AWS ein noch stärkeres Sicherheitskonformitätsprogramm, indem es branchen- und länderspezifische Standards wie GxP, PCI DSS, FedRAMP, HIPAA, C5 und andere einhält und SOC 1-, SOC 2- und SOC 3-Berichte bereitstellt.

4.7. Geistiges Eigentum

Die BOC Group ist sich ihrer Verantwortung im Umgang mit vertraulichen Kundendaten bewusst und garantiert daher diese Daten ausschließlich im Auftrag des Kunden und nicht für eigene Zwecke zu verarbeiten. Alle in unseren Services gespeicherten Daten sind das alleinige geistige Eigentum des Kunden. Dennoch schützen wir diese Daten wie unsere eigenen. Die BOC Group hat modernste Maßnahmen ergriffen, um diese Daten vor dem unberechtigten Zugriff Dritter zu schützen, und stellt ihre ständige Verfügbarkeit durch kontinuierliche Datensicherungen sicher.

Es steht den Kunden frei, ihre im Service gespeicherten Daten jederzeit zu exportieren. Auch nach Beendigung des Services bewahren wir Ihre Daten für weitere 90 Tage auf und stellen sie dem jeweiligen Kunden in standardisierten Formaten zur weiteren Verwendung zur Verfügung (XML).

Auf der anderen Seite sind die bereitgestellten Produkte und Services geistiges Eigentum der BOC Group und werden auf der Grundlage eines benutzerbasierten Lizenzmodells an Kunden lizenziert. Unser benutzerbasiertes Lizenzierungsmodell bietet Kunden den Vorteil von transparenten Zugangsbeschränkungen und voller Kostenkontrolle. In diesem Modell werden nur die bestellten Benutzer verrechnet. Es gibt keine versteckten Kosten oder Überraschungen bei einer etwaigen Überschreitung von Transaktionen oder Ähnlichem. Darüber hinaus bietet die benutzerbasierte Lizenzierung Flexibilität, da die Nutzungsrechte jederzeit problemlos auf andere Personen in Ihrem Unternehmen übertragen werden können. Außerdem müssen sich Kunden keine Gedanken über geografische oder hardwarebedingte Einschränkungen machen. Insgesamt gewährleistet die benutzerbasierte Lizenzierung, dass die volle Kontrolle über die Kosten und den Zugang zu unseren Produkten und Dienstleistungen beim Kunden liegen.

Durch die Nutzung unserer Produkte und Services werden keine Rechte Dritter beeinträchtigt. Wir legen bei der Verwendung von Drittlizenzen großen Wert darauf, dass alle Lizenzbestimmungen eingehalten werden und es zu keiner Verletzung von geistigem Eigentum kommen kann. Damit schützen wir unsere Kunden vor möglichen Ansprüchen von Dritten.

4.8. Ethische und ökologische Erwägungen

Bei der BOC Group nehmen wir unsere Verpflichtung zu ethischen, umweltfreundlichen und korruptionsfreien Praktiken sehr ernst. Unser Team ist sich seiner Verantwortung in dieser Hinsicht voll bewusst und wir haben eine Reihe von Maßnahmen ergriffen, um sicherzustellen, dass wir in all diesen Bereichen die höchsten Standards erfüllen. Wir sind bestrebt, unseren Kunden den bestmöglichen Service zu bieten, und wir sind der Meinung, dass dies auch die Einhaltung der höchsten ethischen und rechtlichen Standards erfordert.

Die BOC Group verpflichtet ihre Mitarbeiter, ihre hohen ethischen und ökologischen Standards in ihrem täglichen Verhalten gegenüber anderen anzuwenden. Dazu gehören unter anderem die Grundsätze der Menschenrechte, der Gleichberechtigung, der Gesundheit und Sicherheit sowie der Korruptions- und Bestechungsbekämpfung. Die BOC Group fördert die respektvolle Zusammenarbeit, die Kooperation und den Umweltschutz innerhalb des Unternehmens. Darüber hinaus ist die BOC Group bestrebt, bei der Auswahl ihrer Zulieferer und Subunternehmer das gleiche Niveau an ethischen und ökologischen Standards einzuhalten. BOC stellt sicher, dass alle potenziellen Auftragnehmer und Lieferanten entlang der Lieferkette vor deren Auswahl sorgfältig geprüft werden.

4.9. Branchenspezifische Compliance-Anforderungen

Die BOC Group verpflichtet sich zur Einhaltung der höchsten Compliance-Standards und ist sich ihrer Verantwortung für die Einhaltung branchenspezifischer Vorschriften bewusst. Wir wissen, dass Branchen wie das Bankwesen, die Pharmaindustrie oder die Versicherungsbranche strenge Compliance-Anforderungen haben, und wir verpflichten uns, diese Anforderungen zu erfüllen. Das Engagement von BOC zeigt sich darin, dass wir bereits eine Vielzahl an Kunden aus diesen Branchen mit strengen Compliance-Vorschriften bedienen.

Zu den getroffenen Maßnahmen gehören regelmäßiger Überprüfungen unserer Outsourcing-Vereinbarungen und der Aufrechterhaltung eines soliden Rahmens für Governance und Risikomanagement. Zudem führen wir regelmäßige Audits und Überprüfungen unserer Prozesse und Systeme durch, um sicherzustellen, dass wir alle erforderlichen Vorschriften einhalten.

Von unseren Zulieferern, einschließlich der IaaS-Anbietern, verlangen wir, dass sich diese ebenfalls an diese branchenspezifischen Compliance-Standards halten. Wir verfügen über robuste Prozesse für das Lieferantenmanagement, um sicherzustellen, dass alle unsere Lieferanten diese Anforderungen erfüllen.

4.9.1. Finanzinstitutionen

Wenn es um die Auslagerung an einen Cloud-Anbieter im Finanzsektor geht, gelten je nach Standort des Finanzinstituts unterschiedliche Vorschriften. Für europäische Finanzinstitute gelten in der Regel die EBA Leitlinien

zu Auslagerunen. Für deutsche Institute können auch die MaRisk AT 9 und § 25a KWG anwendbar sein. Österreichische Finanzinstitute müssen sich an § 25 BWG halten. All diese Leitlinien und Normen sollen sicherstellen, dass Auslagerungsgeschäfte auf sichere und solide Art und Weise durchgeführt werden, mit geeigneten Risikomanagementmaßnahmen und definierten rechtlichen Regelungen.

Als Cloud Service-Anbieter für die Finanzbranche nehmen wir die Einhaltung der einschlägigen Vorschriften sehr ernst. Wir stellen sicher, dass unsere Dienstleistungen den hohen Standards entsprechen, die von der Europäischen Bankenaufsichtsbehörde (EBA) in ihren Leitlinien für Outsourcing-Vereinbarungen oder anderen nationalen Behörden festgelegt wurden.

Zu diesem Zweck haben wir mehrere Maßnahmen ergriffen, um die Einhaltung dieser Leitlinien zu gewährleisten. Diese Maßnahmen umfassen:

- Durchführung regelmäßiger Risikobewertungen unserer Betriebe und Lieferanten
- Festlegung klarer vertraglicher Vereinbarungen mit unseren Kunden und Lieferanten
- Umsetzung von Outsourcing-Zusatzvereinbarungen mit unseren Infrastructure-as-a-Service-Anbietern, einschließlich der Einführung eines Rechts auf Zugang und Prüfung
- Umsetzung solider Governance-Regelungen, um sicherzustellen, dass wir in der Lage sind, unsere Outsourcing-Beziehungen effektiv zu verwalten
- Umfassende Pläne zur Aufrechterhaltung des Geschäftsbetriebs, um sicherzustellen, dass wir im Falle einer Störung in der Lage sind, den Betrieb fortzusetzen
- Umsetzung geeigneter Maßnahmen zum Schutz von Daten und zur Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit unserer Systeme

Zusätzlich zu diesen Maßnahmen haben wir auch eine Erfolgsbilanz bei der Betreuung von Kunden aus der Finanzbranche vorzuweisen. Wir haben eine Vielzahl an positiven Kundenprojekten im Finanzsektor vorzuweisen, wodurch wir unser Engagement zur Einhaltung der einschlägigen Vorschriften und Standards unter Beweis gestellt haben. Wir sind stolz darauf unseren Kunden aus der Finanzbranche zuverlässige, sichere und gesetzeskonforme Cloud-Services bieten zu können.

4.9.2. Versicherungsanstalten

Als Cloud Service-Anbieter unterstützen wir regulierte Unternehmen im Versicherungssektor bei der Einhaltung der von der EIOPA aufgestellten Regeln für das Outsourcing in die Cloud. Laut EIOPA soll die Kontrolle der ausgelagerten Cloud Services in einem angemessenen Verhältnis zu Art, Umfang und Komplexität der mit den von uns erbrachten Leistungen verbundenen Risiken stehen. Auf Anfrage unterstützen wir Sie bei der in dieser Verordnung geforderten Risikobewertung, Dokumentation und Analyse der ausgelagerten Services.

Darüber hinaus sollten die Rechte und Pflichten des Kunden und die Rechte und Pflichten der BOC Group klar zugewiesen und in einer schriftlichen Vereinbarung festgehalten werden. Solche Vereinbarungen ermöglichen die tatsächliche Ausübung der Zugangs- und Prüfungsrechte des auslagernden Unternehmens. Die in diesem Dokument beschriebenen Maßnahmen bieten unseren Kunden die notwendigen Informationen, um festzustellen, dass wir als Cloud Service Anbieter die europäischen und nationalen Vorschriften sowie die entsprechenden IKT-Sicherheitsstandards einhalten.

Um unseren Outsourcing-Kunden die notwendige Kontrolle über unsere Dienstleistungen zu geben, haben wir entsprechende Outsourcing-Vereinbarungen abgeschlossen, insbesondere mit unseren IaaS-Anbietern. Diese Vereinbarungen ermöglichen es unseren Outsourcing-Kunden, ihre Kontrollrechte auch gegenüber unseren Dienstleistern geltend zu machen.

Wir sind nicht nur bereit, unseren Outsourcing-Kunden Kontrollrechte einzuräumen, sondern auch die Outsourcing-Vereinbarungen so zu erweitern, dass sie Kündigungsrechte und Ausstiegsstrategien vorsehen. Dies trägt dazu bei, dass unsere Kunden die nötige Flexibilität haben, um unsere Leistungen an ihre sich veränderten Bedürfnisse anzupassen und die Beziehung gegebenenfalls zu beenden. Unsere Verträge sehen dazu klare und faire

Bedingungen vor. Zudem verpflichten wir uns, mit unseren Kunden in diesem Bereich zusammenzuarbeiten, um für beide Seiten vorteilhafte Lösungen zu finden.

4.9.3. Pharmazeutische Industrie

Beim Outsourcing in die Cloud sind für Pharmaunternehmen insbesondere die spezifischen Branchenanforderungen im Hinblick auf GxP (Good Practices for the pharmaceutical industry) und FDA 21 CFR Part 11 relevant.

Bei GxP handelt es sich um eine Reihe von Leitlinien, mit denen sichergestellt werden soll, dass Produkte durchgängig nach den für ihren Verwendungszweck geeigneten Qualitätsstandards hergestellt und kontrolliert werden. Im Zusammenhang mit der Auslagerung in die Cloud müssen Pharmaunternehmen sicherstellen, dass ihr Cloud-Anbieter in der Lage ist, die GxP Anforderungen zu erfüllen sowie eine sichere und konforme Umgebung für die Speicherung und Verarbeitung von regulierten Daten bereitzustellen.

FDA 21 CFR Part 11 ist eine Reihe von Vorschriften der US-Food-and-Drug-Administration, in denen Kriterien festgelegt sind, wodurch elektronische Aufzeichnungen und elektronische Signaturen als vertrauenswürdig, zuverlässig und gleichwertig mit Papieraufzeichnungen gelten.

BOC ist ein zuverlässiger Partner für die Bereitstellung von Cloud Services für Pharmakunden. Wir können auf eine nachweisliche Erfolgsbilanz in der Zusammenarbeit mit vielen Pharmakunden zurückblicken und helfen ihnen bei der Einhaltung der GxP- und FDA 21 CFR Part 11-Anforderungen. Unser Team ist sehr erfahren in der Zusammenarbeit mit regulierten Branchen und verpflichtet sich, eine sichere und konforme Umgebung für die Speicherung und Verarbeitung von regulierten Daten bereitzustellen. Wir sind zuversichtlich, dass wir die Anforderungen Ihres Unternehmens als zuverlässiger Anbieter von Cloud Services in der pharmazeutischen Industrie erfüllen können.