SICHERHEITSZUSATZ

Dieser Sicherheitszusatz ist Bestandteil der schriftlichen Vereinbarung zwischen insightsoftware und dem Kunden, in der auf dieses Dokument verwiesen wird (die „**Vereinbarung**“), und alle in Anführungszeichen geschriebenen Begriffe, die hier nicht definiert sind, haben die in der Vereinbarung festgelegte Bedeutung. Bei einem Widerspruch zwischen den Bedingungen der Vereinbarung und diesem Sicherheitszusatz gilt dieser Sicherheitszusatz. Dieser Sicherheitszusatz legt die Sicherheitskontrollen und -standards von insightsoftware fest („Sicherheitsprogramm“). insightsoftware testet und bewertet sein Sicherheitsprogramm regelmäßig und kann sein Sicherheitsprogramm sowie diesen Sicherheitszusatz überprüfen und aktualisieren, jedoch unter der Voraussetzung, dass das Sicherheitsprogramm durch solche Aktualisierungen verbessert und nicht wesentlich verschlechtert wird.

1. **Unternehmenssicherheitskontrollen von insightsoftware.**

   a. **Administrative Kontrollen.**
      i. **Dediziertes Informationssicherheitsteam**. Das Sicherheitsprogramm von insightsoftware wird von einem dedizierten Informationssicherheits-Expertenteam unter der Leitung des VP und des Chief Information Security Officer von insightsoftware verwaltet.
      ii. **Sicherheitsrichtlinie**. insightsoftware unterhält eine schriftliche Sicherheitsrichtlinie, die auf Branchenstandards basiert und den geltenden Datenschutzgesetzen („Datenschutzgesetze“) entspricht; diese Richtlinie wird jährlich überprüft und aktualisiert und allen insightsoftware-Mitarbeitern zur Verfügung gestellt.
      iii. **Hintergrundüberprüfungen**. insightsoftware führt im Rahmen des Einstellungsverfahrens in Übereinstimmung mit den geltenden Gesetzen Überprüfungen in Bezug auf mögliche kriminelle Hintergründe seiner Mitarbeiter durch. In einigen Ländern werden Hintergrundüberprüfungen für alle Mitarbeiter durchgeführt, in anderen Ländern können sie auf Anfrage durchgeführt werden.
      iv. **Sicherheitsbewusstseinsschulung.** insightsoftware unterhält ein dokumentiertes Programm zur Schulung des Sicherheitsbewusstseins für seine Mitarbeiter; dies schließt Schulungen für neu eingestellte Mitarbeiter sowie fortlaufende Schulungen ein.
      v. **Verhaltenskodex; Vertraulichkeitsvereinbarungen; Informationssicherheitsrichtlinien**. insightsoftware-Mitarbeiter müssen mehrere Richtlinien und Vereinbarungen, die von ihnen verlangen, die Vertraulichkeit von Kundendaten zu wahren und Sicherheitsprozesse im Zusammenhang mit Kundendaten zu befolgen, anerkennen und ihnen zustimmen; darunter der Verhaltenskodex von insightsoftware, die Vertraulichkeitsvereinbarungen für Mitarbeiter und die Informationssicherheitsrichtlinien von insightsoftware.
      vi. **Risikomanagement und Bedrohungsbewertung bei insightsoftware.** insightsoftware verfügt über einen dokumentierten Risikomanagementprozess. Das Informationssicherheitskomitee von insightsoftware trifft sich regelmäßig, um Berichte und wesentliche Änderungen im Bedrohungsumfeld zu prüfen, mögliche Kontrollmängel zu identifizieren und Empfehlungen für neue oder verbesserte Kontrollen und Strategien zur Bedrohungsabwehr zu geben.
      vii. **Überwachung externer Gefahren.** insightsoftware prüft Hinweise zu externen Gefahren, einschließlich US-Cert-Schwachstellenmeldungen, kritische Sicherheitshinweise von Herstellern und anderen vertrauenswürdigen Quellen für Schwachstellen- und Gefahreninformationen.
      viii. **Lieferantenrisikomanagement.** insightsoftware bewertet Anbieter, die Kundendaten verarbeiten oder Teil einer insightsoftware-Lösung sind, um sicherzustellen, dass sie Sicherheitsmaßnahmen einhalten, die den Verpflichtungen von insightsoftware in diesem Sicherheitszusatz und den Datenschutzgesetzen entsprechen.

   b. **Erkennung von Vorfällen und Reaktion auf Vorfälle.**
      i. **Plan zur Reaktion auf Vorfälle.** insightsoftware unterhält einen dokumentierten Plan zur Reaktion auf Vorfälle, der die Meldung von Vorfällen, Reaktion, Rollen und Verantwortlichkeiten, Priorisierung, Eskalation und Abhilfe beinhaltet. Der Plan wird in regelmäßigen Abständen getestet und aktualisiert.
      ii. **Meldung von Sicherheitsvorfällen.** Erlangt insightsoftware Kenntnis von einer Sicherheitsverletzung, die zur versehentlichen oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung von oder zum Zugriff auf Kundendaten führt (ein „Sicherheitsvorfall“), benachrichtigt insightsoftware den Kunden unverzüglich, in jedem Fall aber innerhalb von 48 Stunden, nachdem insightsoftware festgestellt hat, dass ein Sicherheitsvorfall die Kundendaten beeinträchtigt hat oder beeinträchtigen wird.
      iii. **Untersuchung.** Im Falle eines Sicherheitsvorfalls ergreift insightsoftware unverzüglich angemessene Maßnahmen zur Eindämmung, Untersuchung und Abmilderung des Sicherheitsvorfalls. Alle für einen Sicherheitsvorfall relevanten Protokolle sind mindestens ein Jahr lang aufzubewahren.

iv. **Kommunikation und Zusammenarbeit.** insightsoftware wird den Kunden rechtzeitig und in dem Umfang, in dem insightsoftware Kenntnis über den Sicherheitsvorfall hat, über diesen informieren, unter anderem über die Art und die Folgen des Sicherheitsvorfalls, die von insightsoftware ergriffenen und/oder vorgeschlagenen Maßnahmen zur Abmilderung oder Eindämmung des Sicherheitsvorfalls, den Stand der Ermittlungen von insightsoftware und mit Angabe einer Kontaktstelle, unter der zusätzliche Informationen verfügbar sind.

v. **Cyber-Versicherung.** insightsoftware unterhält eine Cyber-/Technologiefehler- und Unterlassungs-Haftpflichtversicherung mit einer Versicherungsnehmerbewertung von nicht weniger als „A-“ und einer Finanzgrößenklassenbewertung von nicht weniger als „VII“ gemäß der neuesten Ausgabe des A.M. Best's Key Rating Guide.

c. **Physische und Umgebungskontrollen der Unternehmenseinrichtungen von insightsoftware.** Die technischen, administrativen und physischen Kontrollen für die Unternehmensniederlassungen von insightsoftware, die von der ISO 27001-Zertifizierung abgedeckt werden, umfassen unter anderem Folgendes:

i. Kontrolle des physischen Zugangs zum Firmengebäude an den Eingängen;
ii. Erfordernis eines Zugangsausweises für alle Mitarbeiter; die entsprechenden Berechtigungen werden regelmäßig überprüft;
iii. Anmeldepflicht für Besucher;
iv. Videoüberwachung der Gebäudeeingänge;
v. Feuermelde- und Brandschutzsysteme; und
vi. Klimatisierungskontrollsysteme.

d. **insightsoftware Systemsicherheit.**

i. **Schutz vor Malware und Schwachstellen.** Laptopcomputer, Desktopcomputer und Produktionsserver von insightsoftware sind durch automatisch aktualisierten Anti-Malware-Schutz und Schwachstellenüberwachung geschützt. E-Mails, einschließlich Links und Anhänge in E-Mails, werden vor der Zustellung auf Malware gescannt.
ii. **Festplattenverschlüsselung.** Die Festplatten der insightsoftware-Laptops sind verschlüsselt.
iii. **Patching.** Mindestens einmal im Monat werden Sicherheits-Patches überprüft und installiert.
iv. **Sichere Entsorgung.** insightsoftware folgt einem dokumentierten Prozess für die sichere Entsorgung von Datenspeichern.
v. **Mehrstufige Authentifizierung**. Der Fernzugriff auf insightsoftware-Netzwerke erfordert eine mehrstufige Authentifizierung.

e. **Sichere Softwareentwicklung.**

i. Sicherheit ist Teil des gesamten Lebenszyklus der Softwareentwicklung.
ii. Die Entwicklungssysteme sind von den Produktionssystemen getrennt.
iii. Kundendaten werden nicht an Entwicklungssysteme übertragen oder dort gespeichert.
iv. Anwendungssicherheitstests sind in die Software-Entwicklungspipeline integriert.
v. Es wird ein Quellcode-Kontrollsystem verwendet, das Personen, die mit allen Änderungen an der Software oder der benutzerdefinierten Code-Basislinie und allen zugehörigen Konfigurations- und Build-Dateien verbunden sind, authentifiziert und protokolliert.
vi. Der Quellcode wird gesichert und geschützt.

2. **Sicherheitskontrollen und Schutzmaßnahmen für die Cloud.**

a. **Sicherheitsverantwortung.** insightsoftware stellt seine Software entweder (i) vor Ort zur Verfügung, wobei die Software auf den Computern des Kunden installiert wird, oder (ii) als gehosteten Service zur Verfügung, wobei insightsoftware Infrastructure-as-a-Service-Cloud-Anbieter und/oder sichere Colocation-Einrichtungen nutzt, um dem Kunden Zugriff auf die insightsoftware-Software zu gewähren (die „Cloud-Umgebung“). In Bezug auf die vor Ort zur Verfügung gestellte Software (On-Premise-Software) von insightsoftware, die auf den Computern des Kunden installiert wird, ist der Kunde für die Aufrechterhaltung der Sicherheit der Computer des Kunden verantwortlich; dies schließt Patches, Zugangskontrollen, Firewalls, physische Sicherheit, Backups und Verschlüsselung ein. Wenn die Software von insightsoftware über eine Cloud-Umgebung bereitgestellt wird, ist insightsoftware für die Aufrechterhaltung der unten beschriebenen Sicherheitskontrollen und Schutzmaßnahmen verantwortlich. insightsoftware verfügt über ein umfassendes dokumentiertes Sicherheitsprogramm, in dessen Rahmen insightsoftware physische, administrative und technische Schutzmaßnahmen implementiert und aufrechterhält, die die Vertraulichkeit, Integrität, Verfügbarkeit und Sicherheit der Software und der Kundendaten schützen sollen.

b. **Audits und Zertifizierungen von insightsoftware.**

i. insightsoftware führt die unter https://legal.insightsoftware.com/contracts/ISO&SOC-certifications.pdf beschriebenen Audits und Zertifizierungen durch.
ii. Berichte von unabhängigen Dritt-Auditoren werden dem Kunden auf Anfrage zur Verfügung gestellt.

c. **Hosting-Standort der Kundendaten.** insightsoftware setzt Unterauftragnehmer ein, deren Kontrollen durch SOC 2-Audits bewertet werden, um sicherzustellen, dass sie angemessen konzipiert sind und umgesetzt werden, um die Sicherheitsanforderungen von insightsoftware zu erfüllen.

d. **Verschlüsselung.**
i. **Verschlüsselung im Speicherungszustand**. In der Cloud-Umgebung befindliche Kundendaten werden im Speicherungszustand verschlüsselt.
ii. **Verwaltung des Verschlüsselungsschlüssels.** Alle kryptografischen Schlüssel sind vor unbefugter Offenlegung oder Verwendung geschützt.
1. Die Verschlüsselungsschlüssel werden in Übereinstimmung mit den aktuellen Stärkeempfehlungen nach Branchenstandard erstellt.
2. Jeder Schlüssel, der aufgrund veralteter Algorithmen schwach wird oder bei dem der Verdacht besteht, dass er kompromittiert ist, wird außer Dienst gestellt und/oder mit einem aktualisierten Schlüssel ausgetauscht.
3. Zur Verschlüsselung von Schlüsseln, die zur Verschlüsselung von Daten verwendet werden, werden Zertifikate verwendet.
iii. **Verschlüsselung bei der Übertragung.** Um vertrauliche Daten bei der Übertragung über öffentliche Netzwerke zu verschlüsseln, werden sichere Datenübertragungsprotokolle verwendet.

e. **System- und Netzwerksicherheit.**
i. **Zugriffskontrollen.** Alle insightsoftware-Mitarbeiter erhalten über eine eindeutige Benutzer-ID mit einem komplexen Passwort und einer mehrstufigen Authentifizierung Zugang zur Cloud-Umgebung. Der Zugang zu Systemen und Daten wird Mitarbeitern nur gewährt, wenn dies für die Erfüllung ihrer Aufgaben erforderlich ist und dem Prinzip der geringsten Privilegien entspricht.
ii. **Trennung der Umgebungen.** insightsoftware trennt die Produktionsumgebung logisch von der Entwicklungs- und Testumgebung. Die Cloud-Umgebung ist sowohl logisch als auch physisch von den Unternehmensniederlassungen und -netzwerken von insightsoftware getrennt.
iii. **Änderungsmanagement.** insightsoftware unterhält ein dokumentiertes Änderungsmanagementprogramm für seine Software.
iv. **Firewalls/Sicherheitsgruppen.** Die Cloud-Umgebung von insightsoftware verwendet branchenübliche Firewall- oder Sicherheitsgruppentechnologien mit „Deny-All"-Standardrichtlinien, um nur die für das Unternehmen erforderlichen Netzwerkprotokolle zuzulassen und die Systeme vor nicht vertrauenswürdigen Netzwerken zu schützen.
v. **Überprüfung und Abtrennung des Zugriffs durch Personen.** insightsoftware überprüft die Zugriffsrechte seiner Mitarbeiter auf die Cloud-Umgebung mindestens vierteljährlich und entfernt unverzüglich den Zugriff für ausgeschlossene Mitarbeiter.
vi. **Härtung.** Die Cloud-Umgebung wird durch branchenübliche Praktiken gehärtet, um sie vor Schwachstellen zu schützen, u. a. durch das Ändern von Standardpasswörtern, das Entfernen unnötiger Software, das Deaktivieren oder Entfernen unnötiger Dienste, und durch regelmäßiges Patching, wie in diesem Sicherheitszusatz beschrieben.
vii. **Patching.** Sicherheitspatches werden regelmäßig überprüft und gemäß den festgelegten Richtlinien und Standards auf die Systeme aufgespielt.
viii. **Überwachung und Protokollierung.** Zur Protokollierung bestimmter Aktivitäten und Änderungen innerhalb der Cloud-Umgebung werden Überwachungstools und -dienste eingesetzt. Diese Protokolle werden bei Bedarf weiter überwacht und auf Anomalien analysiert. Die Protokolle werden sicher gespeichert, um Manipulationen zu verhindern.
ix. **Endpunktschutz**. Die Cloud-Umgebung nutzt sich automatisch aktualisierende Tools zur Erkennung von Bedrohungen, um verdächtige Aktivitäten und Malware (zusammenfassend „bösartige Aktivitäten") auf den Endpunkten im Geltungsbereich zu überwachen und diese davor zu schützen. insightsoftware überwacht Kundendaten nicht auf bösartige Aktivitäten.
x. **Schwachstellenmanagement.** Systeme in der Cloud-Umgebung werden automatisch auf Schwachstellen untersucht, die dann auf der Grundlage ihrer potenziellen Auswirkungen auf die Software von insightsoftware zur Behebung priorisiert werden.
xi. **Penetrationstests**. insightsoftware beauftragt einen oder mehrere unabhängige Dritte, mindestens einmal jährlich Penetrationstests an ausgewählter Software durchzuführen. Auf schriftliche Anfrage des Kunden

stellt insightsoftware dem Kunden eine Zusammenfassung des betreffendendes be Penetrationstests zur Verfügung.

f. **Physikalische und umgebungsbezogene Kontrollen des Cloud-Rechenzentrums.** Um sicherzustellen, dass die Cloud-Umgebung über angemessene physische und umgebungsbezogene Kontrollen für die Rechenzentren verfügt, in denen die Software gehostet wird, überprüft insightsoftware regelmäßig die Sicherheitskontrollen der Cloud-Umgebung, die von unabhängigen Dritten bei Audits zur Prüfung und Zertifizierung verwendet werden. Jeder Provider der Cloud-Umgebung durchläuft jährlich ein SOC 2 Typ II-Audit sowie eine ISO 27001-Zertifizierung oder ein gleichwertiges, von der Branche anerkanntes Rahmenwerk. Diese Kontrollen umfassen unter anderem Folgendes:
   i. Kontrolle des physischen Zugangs zu den Einrichtungen und physischen Systemen;
   ii. Regelmäßige Überprüfungen der physischen Zugangsberechtigungen;
   iii. Ausweis- und Anmeldepflicht für Besucher;
   iv. Videoüberwachung aller Gebäudeeingänge;
   v. Brandmelde- und Brandschutzsysteme;
   vi. Notstromversorgung und Redundanzsysteme;
   vii. Klimatisierungskontrollsysteme; und
   viii. Etablierte NIST 800-88-konforme Prozesse für die Außerbetriebnahme von Hardwareressourcen.

g. **Löschung von Kundendaten durch insightsoftware.** Vorbehaltlich der anwendbaren Bestimmungen der Vereinbarung löscht insightsoftware unverzüglich alle verbleibenden Kundendaten, sobald (i) die Vereinbarung abläuft oder gekündigt wird oder (ii) eine in der Vereinbarung festgelegte „Abruffrist“ nach der Kündigung abgelaufen ist.

h. **Geschäftskontinuität und Notfallwiederherstellung.** Automatisierte Sicherungssysteme führen planmäßige Sicherungen der Produktionsdatenbanken durch. Für die Software, für die insightsoftware Audits durchführt, gibt es einen Geschäftskontinuitäts- und Notfallwiederherstellungsplan, der die Wiederaufnahme von zeitkritischen Operationen und Diensten im Falle eines katastrophalen Ereignisses, das eine erhebliche Geschäftsunterbrechung verursacht, sicherstellt. Der Geschäftskontinuitäts- und Notfallwiederherstellungsplan enthält detaillierte Zuständigkeiten und spezifische Notfalleinsatzmaßnahmen sowie Aktivitäten zur Wiederaufnahme des Betriebs auf der Grundlage vordefinierter Zeitrahmen. Der Plan wird jährlich überprüft und getestet, um zu validieren, ob die dokumentierten Verfahren angemessen sind, und um sicherzustellen, dass die Mitarbeiter den Plan und die Rolle, die sie bei der Ausführung des Plans spielen, verstehen.

3. **Rechte in Bezug auf Kunden-Audits.** Auf schriftliche Anfrage und ohne zusätzliche Kosten für den Kunden gewährt insightsoftware dem Kunden und/oder seinem angemessen qualifizierten Drittvertreter (zusammen der „Auditor“) Zugriff auf angemessen angeforderte Unterlagen, die die Einhaltung der Verpflichtungen von insightsoftware im Rahmen dieses Sicherheitszusatzes belegen, und zwar in Form (i) der ISO 27001-Zertifizierung von insightsoftware, (ii) des SOC 2 Typ II-Auditberichts von insightsoftware und/oder des SOC 1 Typ II-Auditberichts von insightsoftware, (iii) des zuletzt abgeschlossenen Standardisierten Fragebogens zur Informationserhebung zu gemeinsamen Bewertungen (SIG), und (iv) des letzten zusammenfassenden Berichts über Penetrationstests für die betreffende Software („Auditberichte“). Für den Fall, dass insightsoftware nicht in der Lage ist, einen Auditbericht vorzulegen, erklärt sich insightsoftware bereit, einen vom Kunden zur Verfügung gestellten Fragebogen zur Informationssicherheit jährlich innerhalb von sechs (6) Wochen nach schriftlicher Anforderung des Kunden auszufüllen. Handelt es sich bei dem Prüfer um eine Drittpartei, so kann von dieser verlangt werden, dass sie vor der Prüfung von Auditberichten eine gesonderte Vertraulichkeitsvereinbarung mit insightsoftware abschließt, und insightsoftware kann der betreffenden Drittpartei schriftlich widersprechen, wenn diese nach angemessener Einschätzung von insightsoftware nicht angemessen qualifiziert ist oder ein direkter Wettbewerber von insightsoftware ist. Ein solcher angemessener Einwand von insightsoftware erfordert vom Kunden die Beauftragung einer anderen Drittpartei. Alle Kosten, die einem Auditor im Zusammenhang mit der Überprüfung von Auditberichten oder einem vom Kunden zur Verfügung gestellten Fragebogen entstehen, sind ausschließlich vom Auditor zu tragen.