TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Sofern nicht nachstehend etwas anderes definiert wird, haben alle hierin definierten Begriffe die ihnen jeweils im SDPA zugewiesene Bedeutung.

Die technischen und organisatorischen Maßnahmen des Dienstleisters sollten, ohne Einschränkung, insbesondere Folgendes umfassen:

(i) **Organisation der Informationssicherheit** - Festlegung, Umsetzung und Vorhaltung von Informationssicherheitsrichtlinien und eines Programms technischer und organisatorischer Sicherheitsmaßnahmen, die zweckdienlich für den Schutz von Kundeninformationen sind und der guten Industriepraxis entsprechen.

(ii) **Sichere Mindeststandards** - Maßnahmen, um sicherzustellen, dass für Informationssysteme sichere Konfigurationen entwickelt, dokumentiert und vorgehalten werden.

(iii) **Zugriffskontrollen** - Systemzugriff, Benutzerzugriff und Authentifizierungsmaßnahmen zur Verhinderung des Zugriffs auf Kundeninformationen auf jegliche, nicht durch den Kunden genehmigte Art und Weise oder für nicht durch den Kunden genehmigte Zwecke; die Maßnahmen sollten insbesondere die Verhinderung unbefugter Eingabe, des Lesens, Kopierens, Entfernens, Änderns oder Offenlegens von Kundeninformationen umfassen.

(iv) **Systemsicherheit** - Maßnahmen zur Stärkung von Informationssystemen und anderen Ressourcen gemäß der guten Industriepraxis.

(v) **Prüfung und Kontrolle -** Maßnahmen zur Vorhaltung eines automatisierten Prüfpfads, der Systemsicherheitsereignisse und jegliche Änderungsmanagementereignisse dokumentiert, die zu Zugriff, Änderung und/oder zur Löschung von Kundeninformationen führen.

(vi) **Netzwerksicherheit** - Maßnahmen zur Vorhaltung eines formalen Prozesses für Genehmigung, Prüfung und Dokumentation aller Netzwerkverbindungen und Änderungen an Netzwerkgerätekonfigurationen.

(vii) **Datenschutz** - Maßnahmen zur Verhinderung von unbefugtem Zugriff, Verfälschung oder Entfernung gespeicherter oder übermittelter Kundeninformationen.

(viii) **Sicherheitsbewusstsein und -schulung** - Maßnahmen zur regelmäßigen jährlichen Schulung des Sicherheitsbewusstseins der Mitarbeiter, die Sicherheitstrends, Bedrohungen und beste Praktiken berücksichtigen und diesbezüglich zweckdienlich sind.

(ix) **Sicherheitstests -** Maßnahmen zur regelmäßigen Erkennung und Behebung von Schwachstellen anhand der Richtlinien des Dienstleisters und Durchführung regelmäßiger Sicherheitstests für Systeme und Anwendungen oder bei wesentlichen Änderungen. Insbesondere die folgenden Maßnahmen sollten enthalten sein: (1) Beauftragung eines unabhängigen Dritten mit der Durchführung einer jährlichen Sicherheitsprüfung für alle Systeme des Dienstleisters, (2) Durchführung regelmäßiger Penetrationstests und wöchentlicher Schwachstellen-Scans für alle

Systeme des Dienstleisters, (3) Einführung und Vorhaltung eines Patch-Management-Programms, das mindestens der guten Industriepraxis entspricht, gemäß dem der Dienstleisters regelmäßig Aktualisierungen und Patches von Software durchführt, die sich direkt oder indirekt auf Kundeninformationen und/oder die Systeme des Dienstleisters auswirken kann, und (4) Benennung eines Sicherheitsbeauftragten für den Kunden, der zur Besprechung von Informationssicherheitsvorfällen, Sicherheitstests, Sicherheitsfeststellungen und anderen Sicherheitsbelangen in regelmäßigen Abständen zur Verfügung steht. Wird infolge einer der vorgenannten Maßnahmen oder der Sicherheitsbeurteilung des Kunden ein wesentlicher Mangel festgestellt, wird der Dienstleister diesen innerhalb von 30 Tagen beheben (der Kunde muss umgehend über jede kritische Feststellung informiert werden, die nicht innerhalb von 30 Tagen behoben wird; und auf Verlangen des Kunden wird der Dienstleister schriftlich die erfolgte Durchführung der vorstehen Sicherheitstests bescheinigen und wird eine detaillierte Liste der offenen Schwachstellen und der Pläne zu deren Behebung vorlegen).

(x) **Verfügbarkeitskontrollen -** Maßnahmen zu Entwicklung, Betrieb, Verwaltung und Überarbeitung von Geschäftsfortführungs- und Notfallplänen, einschließlich der technologischen Wiederherstellung.

(xi) **Behebung von Software-Sicherheitsproblemen -** Wenn der Dienstleister als Teil der Leistungen SaaS oder PaaS oder einen gehosteten Softwaredienst liefert und Dienstleister oder Kunde Schwachstellen oder andere Sicherheitsprobleme in der Software entdecken oder vermuten, sind in der Anwendung für den Kunden Maßnahmen zur Bereitstellung von Fehlerbehebungen, Updates, Patches, Überarbeitungen, Korrekturen, Upgrades und neuen Software-Versionen (jeweils mit Dokumentation) gemäß nachstehendem Zeitplan enthalten. Der Dienstleister wird dem Kunden den Nachweis erbringen, dass alle festgestellten Sicherheitsprobleme gemäß dem erstellten Plan für Abhilfemaßnahmen vollständig behoben worden sind.

chwere	**Beschreibung**	**Bestätigung**	**Updates**	**Lösung**	**Abschluss**
Notfall	Katastrophale Probleme ohne praktikable Umgehungslösung	1 Stunde während Geschäftszeiten nach Entdeckung einer Schwachstelle oder eines Sicherheitsproblems	Alle 3 Stunden während Geschäftszeiten	1 Tag	7 Tage
Kritisch	Probleme, die eine ernstzunehmende Gefahr für den Endnutzer und/oder Kunden darstellen	4 Stunden während Geschäftszeiten nach Entdeckung einer Schwachstelle oder eines Sicherheitsproblems	Täglich	5 Tage	14 Tage
Wichtig	Probleme, für die es eine praktikable Umgehungslösung gibt und die durch andere Sicherheitskontrollen eingegrenzt werden können	2 Arbeitstage nach Entdeckung einer Schwachstelle oder eines Sicherheitsproblems	5 Tage	10 Tage	45 Tage
Nicht kritisch	Alle anderen Probleme oder Umgehungslösungen	5 Arbeitstage nach Entdeckung einer Schwachstelle oder eines Sicherheitsproblems	5 Tage	15 Tage	Nächste Version