

Bestimmungen zum Datenschutz

Der Auftragnehmer verpflichtet sich zur ordnungsgemäßen und datenschutzgerechten Ausführung der vertraglich vereinbarten Arbeiten und dazu, die ordnungsgemäße Auftragsausführung zu überwachen und zu kontrollieren.

Die Parteien treffen gesonderte Bestimmungen zum Datenschutz in der Anlage B10 bis B10a.

ISO/IEC 27001 konformes ISMS

Der Auftragnehmer hält für die Dauer der Vertragslaufzeit ein nach ISO/IEC 27001 zertifiziertes ISMS (Informationssicherheits-Managementsystem) oder ein ISO/IEC 27001 konformes ISMS vor.

Nutzung sicherer Datenaustauschkanäle

- (1) Der Auftragnehmer verpflichtet sich, für den Austausch von vertraulichen oder personenbezogenen Daten im Rahmen der Vertragsdurchführung ausschließlich sichere und verschlüsselte Datenaustauschkanäle zu verwenden. Hierzu zählen insbesondere, aber nicht ausschließlich, die Nutzung eines gesicherten Datenaustauschportals sowie die Verwendung von E-Mail-Verschlüsselung gemäß aktuellen Sicherheitsstandards.
- (2) Der Auftragnehmer stellt sicher, dass alle Datenübertragungen, die im Rahmen der Vertragserfüllung erfolgen, gemäß den einschlägigen gesetzlichen und regulatorischen Anforderungen zum Schutz von Daten (insbesondere der Datenschutz-Grundverordnung (DSGVO)) erfolgen und vor unbefugtem Zugriff oder Verlust geschützt sind.

Mitwirkungspflicht bei Audits

- (1) Der Auftragnehmer verpflichtet sich, im Falle einer durch den Auftraggeber durchgeführten Auditierung der vertraglichen Leistungen oder Prozesse mit allen notwendigen Informationen und Unterstützung zur Durchführung zu kooperieren. Eine Auditierung erfolgt mindestens einmal jährlich; hiervon erfolgt die Auditierung in Form einer vor Ort Auditierung mindestens vor der Beauftragung sowie einmal in drei Jahren, sofern nichts Abweichendes vereinbart wird. Diese Mitwirkungspflicht des Auftragnehmers gilt unabhängig davon, ob die Auditierung durch den Auftraggeber selbst oder durch einen externen Auditor durchgeführt wird. Dies umfasst insbesondere folgende Mitwirkungsleistungen:
 - (a) Der Auftragnehmer stellt auf Anforderung des Auftraggebers alle erforderlichen Unterlagen, Aufzeichnungen und Daten zur Verfügung, die für die Auditierung relevant sind.
 - (b) Der Auftragnehmer gewährt den Auditierenden Zugang zu den relevanten Betriebsstätten und steht für Interviews mit Schlüsselpersonal zur Verfügung, soweit dies für die Auditierung erforderlich ist.
 - (c) Der Auftragnehmer verpflichtet sich, innerhalb einer angemessenen Frist auf Anfragen im Rahmen der Auditierung zu reagieren und notwendige Maßnahmen zur Sicherstellung der Kooperation zu ergreifen.
- (2) Der Auftragnehmer trägt die Kosten für die Bereitstellung der Informationen und seine vertragsgemäße Mitwirkung im Rahmen von Audits.

Qualitätssicherung (QS)

- (1) Der Auftragnehmer verpflichtet sich, für die Dauer des Vertrages eine systematische Qualitätssicherung zu entwickeln, zu implementieren und kontinuierlich zu überwachen.
- (2) Das Qualitätssicherungsprogramm muss mindestens folgende Elemente umfassen:
 - (a) Der Auftragnehmer stellt ein Qualitätsmanagementsystem (QMS) auf, das die Qualitätsanforderungen für die erbrachten Leistungen definiert und überwacht.

- (b) Der Auftragnehmer führt regelmäßige Kontrollen und Tests durch, um sicherzustellen, dass alle erbrachten Leistungen die festgelegten Qualitätsstandards erfüllen.
- (c) Der Auftragnehmer verpflichtet sich, ein Verfahren zur Identifikation, Dokumentation und Behebung von Abweichungen und Qualitätsmängeln zu implementieren.
- (d) Der Auftragnehmer stellt sicher, dass alle Mitarbeiter, die an der Erbringung der Leistungen beteiligt sind, regelmäßig geschult werden und über die notwendigen Qualifikationen verfügen, um die Qualitätsanforderungen zu erfüllen.

- (3) Der Auftragnehmer verpflichtet sich, alle relevanten Qualitätssicherungsmaßnahmen, Prüfberichte und Abweichungsanalysen zu dokumentieren und dem Auftraggeber auf Verlangen zur Verfügung zu stellen. Diese Unterlagen müssen nach Abschluss der jeweiligen Leistung aufbewahrt werden, sofern nichts Abweichendes vereinbart wird.
- (4) Der Auftragnehmer gestattet dem Auftraggeber, regelmäßig die Qualitätssicherungsmaßnahmen zu überprüfen und erforderliche Audits durchzuführen, um die Wirksamkeit der Qualitätssicherungsmaßnahmen zu gewährleisten.
- (5) Im Falle von festgestellten Mängeln oder Abweichungen ist der Auftragnehmer verpflichtet, unverzüglich angemessene Korrektur- und Präventivmaßnahmen zu ergreifen, um eine wiederholte Nichteinhaltung der Qualitätsanforderungen zu vermeiden.
- (6) Der Auftragnehmer verpflichtet sich, die Qualitätssicherungsmaßnahmen basierend auf den Ergebnissen von Audits, Feedback des Auftraggebers und internen Qualitätsanalysen fortlaufend zu verbessern.

**Kontrolle und Dokumentation der Identität des Personals des Auftragnehmers;
Aktivitätsprotokollierung**

- (1) Der Auftragnehmer verpflichtet sich, sicherzustellen, dass alle Mitarbeiter und sonstigen von ihm beauftragte Dritte, die Zutritt zu den Räumlichkeiten des Auftraggebers erhalten oder dort tätig werden, vor dem Zugang einer Identitätsprüfung unterzogen werden. Dies gilt für alle Zutritte zu gesicherten Bereichen und für alle Zugriffe auf vertrauliche Informationen oder Systeme des Auftraggebers.
- (2) Der Auftragnehmer ist verpflichtet, die erforderlichen Maßnahmen zu treffen, um die Identität des eingesetzten Personals zu überprüfen und zu dokumentieren. Hierzu zählen:
- (a) Die Erhebung und Verifizierung der Identitätsdaten (z. B. Ausweiskontrolle) der betreffenden Personen.
- (b) Die Dokumentation dieser Identitätsprüfung in einer dauerhaften, nachvollziehbaren und prüfbar Form.
- (c) Die Ausstellung von Identifikationsnachweisen (z. B. Zutrittsausweise) für alle Mitarbeiter, die regelmäßig Zutritt zu den Räumlichkeiten des Auftraggebers benötigen.
- (3) Der Auftragnehmer stellt sicher, dass alle seinerseits eingesetzten Personen den Vorgaben des Auftraggebers zur Zutrittskontrolle und Identitätsdokumentation nachkommen. Insbesondere verpflichtet sich der Auftragnehmer, auf Verlangen des Auftraggebers die Identität des jeweiligen Personals bei Eintritt in gesicherte Bereiche oder bei Zugriff auf sensible Informationen zu bestätigen.
- (4) Der Auftragnehmer akzeptiert die Zutritts- und Sicherheitsvorgaben des Auftraggebers, die für den Zugang zu den Räumlichkeiten, IT-Systemen und anderen sensiblen Bereichen gelten. Diese Vorgaben können regelmäßige Identitätskontrollen, Sicherheitsprüfungen und die Ausstellung von Zutrittsberechtigungen umfassen. Der Auftragnehmer wird sicherstellen, dass sein Personal diese Vorgaben jederzeit einhält.
- (5) Sofern der Auftraggeber spezielle Zugangskontrollsysteme (z. B. elektronische Zutrittskontrollen, biometrische Systeme oder ähnliches) verwendet, verpflichtet sich der Auftragnehmer, sicherzustellen, dass das Personal des Auftragnehmers ordnungsgemäß in das System eingetragen und seine Identität überprüft wird, bevor ein Zugang gewährt wird.

- (6) Der Auftragnehmer verpflichtet sich, den Auftraggeber unverzüglich zu informieren, falls es zu Änderungen im Personalbestand kommt, das Zutritt zu den Räumlichkeiten oder Systemen des Auftraggebers hat. Hierzu gehören insbesondere Änderungen in der Identität, der Zuordnung von Zutrittsberechtigungen oder der Beendigung des Beschäftigungsverhältnisses von Mitarbeitern.
- (7) Der Auftragnehmer verpflichtet sich, der Protokollierung seiner Aktivitäten, die im Rahmen der Vertragserfüllung durch den Auftraggeber durchgeführt wird, zuzustimmen. Diese Protokollierung dient der Überwachung, Dokumentation und Verbesserung der Vertragserfüllung sowie der Sicherheit und Qualität der erbrachten Leistungen.
- (8) Die Protokollierung umfasst, ohne darauf beschränkt zu sein, die Erfassung von Arbeitszeiten, Zugriffen auf Systeme, Nutzung von Ressourcen und/oder anderen relevanten Aktivitäten, die zur Erfüllung der vertraglichen Verpflichtungen erforderlich sind. Der Auftraggeber verpflichtet sich, dabei die geltenden Datenschutzbestimmungen zu wahren.
- (9) Der Auftragnehmer wird den Auftraggeber bei der Aktivitätsprotokollierung unterstützen, insbesondere durch die Bereitstellung von Informationen und Daten, die zur Erfüllung der Protokollierungsanforderungen notwendig sind. Der Auftragnehmer stellt sicher, dass alle erforderlichen technischen und organisatorischen Vorkehrungen getroffen werden, um die ordnungsgemäße Durchführung der Protokollierung zu ermöglichen.
- (10) Alle Kosten, die durch Identitätsprüfung und -nachweis, Zugangskontrollen und Aktivitätsprotokollierung entstehen, trägt der Auftragnehmer.

Kapazitätsplanung und -überwachung

- (1) Der Auftragnehmer verpflichtet sich, im Rahmen der Vertragserfüllung jederzeit über ausreichende Kapazitäten in personeller, technischer und organisatorischer Hinsicht zu verfügen, um die vertraglich vereinbarten Leistungen fristgerecht und in der vertraglich geschuldeten Qualität zu erbringen.
- (2) Der Auftragnehmer erstellt und pflegt einen detaillierten Kapazitätsplan, der insbesondere folgende Aspekte umfasst:
 - (a) Personelle Ressourcen: Die Anzahl und Qualifikation der benötigten Mitarbeiter zur Erbringung der vereinbarten Leistungen.
 - (b) Technische Ressourcen: Die Verfügbarkeit und Kapazität der technischen Infrastruktur (z. B. Software, Hardware, IT-Systeme).
 - (c) Zeitliche Planung: Die zeitliche Planung der Ressourcennutzung unter Berücksichtigung der vertraglich vereinbarten Termine und Meilensteine.
- (3) Der Kapazitätsplan muss dem Auftraggeber auf dessen Anforderung zur Verfügung gestellt werden.
- (4) Der Auftragnehmer verpflichtet sich, die eingesetzten Kapazitäten fortlaufend zu überwachen, um sicherzustellen, dass Ressourcen stets ausreichend zur Verfügung stehen. Im Falle von Engpässen oder Risiken, die geeignet sind, die fristgerechte oder ordnungsgemäße Erbringung der Leistungen zu gefährden, hat der Auftragnehmer den Auftraggeber unverzüglich hierüber zu informieren und nach Aufforderung des Auftraggebers unverzüglich Maßnahmen zur Behebung des Engpasses zu ergreifen.
- (5) Der Auftragnehmer ist verpflichtet, dem Auftraggeber regelmäßig über die aktuelle Kapazitätslage zu berichten. Auf Wunsch des Auftraggebers sind detaillierte Berichte und Prognosen zur Kapazitätsentwicklung vorzulegen. Der Auftraggeber kann bei Bedarf entsprechende feste Intervalle festlegen.
- (6) Der Auftragnehmer verpflichtet sich, bei unvorhergesehenen Änderungen oder Schwankungen im Bedarf (z. B. durch Änderungen der Projektanforderungen oder unvorhergesehene Kapazitätsengpässe) situationsangemessen zu agieren. Der Auftragnehmer hat dem Auftraggeber jegliche Risiken im Zusammenhang mit der

Kapazitätsplanung frühzeitig zu melden und ggf. ein Eskalationsverfahren einzuleiten, um die notwendige Leistungserbringung sicherzustellen.

- (7) Der Auftragnehmer verpflichtet sich, das Kapazitätsmanagement regelmäßig zu evaluieren und kontinuierlich zu verbessern, insbesondere im Hinblick auf die Effizienz und Anpassungsfähigkeit an sich ändernde Anforderungen oder Ressourcenverfügbarkeiten.

Service Level Agreements (SLAs)

- (1) Der Auftragnehmer verpflichtet sich, soweit SLAs festgelegt sind, die spezifischen Anforderungen hinsichtlich der Leistungserbringung definieren, diese einzuhalten. Die SLAs umfassen unter anderem, aber nicht ausschließlich, Kriterien zu Kapazitäten, Antwortzeiten, Wiederherstellungszeiten und Verfügbarkeiten einschl. spezifischer Eskalationsstufen.
- (2) Der Auftragnehmer ist verpflichtet, regelmäßig die Einhaltung der vereinbarten SLAs zu überwachen und zu messen. Der Auftragnehmer stellt dem Auftraggeber auf einen detaillierten Leistungsbericht zur Verfügung, der die erreichten SLAs und eventuelle Abweichungen dokumentiert. Der Bericht muss insbesondere Angaben zu den gemessenen Leistungskennzahlen (z. B. Antwortzeiten, Verfügbarkeiten, Ausfallzeiten) sowie die Gründe für etwaige Nichterfüllung enthalten.
- (3) Sollte der Auftragnehmer wiederholt oder in erheblichem Maße die vereinbarten SLAs nicht einhalten, ist der Auftraggeber berechtigt, die vertraglich festgelegte Vertragsstrafe geltend zu machen.
- (4) Im Falle von Nichteinhaltung eines oder mehrerer SLAs verpflichtet sich der Auftragnehmer, unverzüglich Korrekturmaßnahmen zu ergreifen, um die Ursache der Nichterfüllung zu beheben und zukünftig eine Einhaltung sicherzustellen. Diese Maßnahmen sind dem Auftraggeber innerhalb von fünf Werktagen nach Feststellung des Vorfalls mitzuteilen.
- (5) Eine Anpassung der SLAs aufgrund gesetzlichen Vorgaben oder technischen Erfordernisse ist nur durch schriftliche Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer zulässig.

Verfügbarkeit und Stand der Technik

- (1) Der Auftragnehmer verpflichtet sich, die vereinbarte Vertragsleistung mit der höchstmöglichen Verfügbarkeit zu erbringen.
- (2) Der Auftragnehmer stellt sicher, bei Erbringung der Dienstleistung stets die beste verfügbare Technik einzusetzen, die zum Zeitpunkt der Vertragserfüllung allgemein anerkannt und branchenüblich ist. Der Auftragnehmer stellt sicher, dass alle verwendeten Hard- und Softwarekomponenten, Infrastruktur, Systeme und Prozesse in Übereinstimmung auf dem aktuellen Stand der Technik entwickelt, betrieben und gewartet werden.
- (3) Der Auftragnehmer verpflichtet sich, alle eingesetzten Systeme und Technologien regelmäßig zu warten und notwendige Aktualisierungen vorzunehmen, um die Verfügbarkeit der Dienstleistung zu gewährleisten und sicherzustellen, dass die eingesetzte Technologie den aktuellsten sicherheitstechnischen, funktionalen und betrieblichen Anforderungen entspricht.
- (4) Der Auftragnehmer ist verpflichtet, die Verfügbarkeit der Dienstleistung sowie den Einsatz der verwendeten Technologien in geeigneter Weise zu dokumentieren. Auf Verlangen des Auftraggebers hat der Auftragnehmer nachzuweisen, dass die eingesetzte Technik dem Stand der Technik entspricht und die vereinbarte Verfügbarkeit eingehalten wird. Der Auftragnehmer informiert den Auftraggeber regelmäßig über wesentliche technologische Entwicklungen, Änderungen im Stand der Technik und mögliche Auswirkungen auf die Erbringung der Dienstleistung. Sollte eine technische Weiterentwicklung erforderlich sein, um die vereinbarte Verfügbarkeit aufrechtzuerhalten, wird der Auftragnehmer sich hierzu in Abstimmungen mit dem Auftraggeber begeben.

Verpflichtung zur Durchführung von und Mitwirkung an regelmäßigen Tests der gemeinsamen Funktionen

- (1) Der Auftragnehmer verpflichtet sich, an regelmäßigen Tests der gemeinsamen Funktionen, einschließlich, aber nicht beschränkt auf die Informationssicherheitsvorfallsbehandlung, das Change-Management und Notfallverfahren, aktiv mitzuwirken. Diese Tests dienen der Überprüfung der Effektivität und Effizienz der implementierten Sicherheitsmaßnahmen. Der Auftragnehmer stellt sicher, dass alle relevanten Mitarbeiter und Ressourcen zur Durchführung der Tests zur Verfügung stehen und dass die Tests unter realistischen Bedingungen durchgeführt werden.
- (2) Der Auftragnehmer stellt insbesondere die notwendige technische Infrastruktur und den Zugriff auf relevante Systeme zur Verfügung, leistet Unterstützung bei der Planung und Durchführung der Tests, einschließlich der Bereitstellung von Fachwissen und Personal.
- (3) Nach jedem Test hat der Auftragnehmer einen detaillierten Bericht zu erstellen, der die durchgeführten Tests, die Ergebnisse sowie etwaige identifizierte Mängel und geplante Maßnahmen zur Behebung derselben dokumentiert. Dieser Bericht ist dem Auftraggeber unverzüglich nach Abschluss des Tests in Textform zur Verfügung zu stellen.
- (4) Der Auftraggeber ist berechtigt, zusätzliche Tests anzuordnen, falls dies für die Sicherstellung der vereinbarten Sicherheitsstandards aus Sicht des Auftraggebers erforderlich ist.