

Vergabeverfahren

„IT-Service für Workload Automation“ Aktenzeichen BW 05/25

Vergabeunterlagen

Teil C.

Anlage 4 zum Vertrag zu BW 05/25 (Anlage A12)

„Informationssicherheitsregelung für IT-Dienstleistungen (Stand November 2023)“

Informationssicherheitsregelung für IT-Dienstleistungen

Stand: November 2023

- (1) Der Auftragnehmer hat die Methoden für die Bereitstellung und den Zugriff auf die zur Vertragsausführung erforderlichen Informationen mit den ihm genannten Ansprechpartnern des Auftraggebers im Vorfeld der Leistungserbringung abzustimmen.
- (2) Die Informationen des Auftraggebers werden intern wie folgt klassifiziert: „Streng Vertraulich“, „Vertraulich“, „Intern/Dienstgebrauch“ und „Öffentlich“. Der Auftragnehmer ist verpflichtet, die in der Datenschutzregelung getroffene Geheimhaltungsvereinbarung einzuhalten. Darüber hinaus kann er die vertragsgegenständlichen Informationen entsprechend seiner unternehmenseigenen Klassifizierungen eingruppieren.
- (3) Der Auftragnehmer räumt dem Auftraggeber ein Prüfungsrecht insofern ein, dass besonders zur Verschwiegenheit verpflichtete Mitarbeiter/-innen des Auftraggebers oder ein besonders zur Verschwiegenheit verpflichteter und beauftragter Dritter die Einhaltung der vertraglichen Verpflichtungen durch Prüfung von Dokumenten, Inaugenscheinnahmen, Einholung von Auskünften und/oder Vorlage anderer Nachweise nachprüfen kann/können. Zu diesen Mitarbeitern/-innen des Auftraggebers zählen in der Regel die/der Leiter/in der internen Revision und/oder seine/ihre Mitarbeiter/innen.
- (4) Sofern und soweit die Parteien im Hauptvertrag vereinbart haben, dass die Leistungserbringung (auch) mittels Remote-Zugriff erfolgt, gewährleistet der Auftragnehmer die Einhaltung der nachfolgenden Vorgaben zur Nutzung eines (24 Stunden) Remote-Zugriffs über eine sichere Verbindung auf sämtliche wartungsrelevanten Komponenten. Dies beinhaltet, dass
 - a) die Nutzung des Remote-Zugriffs ausschließlich zur Erfüllung der vertragsgegenständlichen Leistungen zulässig ist;
 - b) der Remote-Zugriff ausschließlich über eine vom Auftraggeber zugelassene Zugriffsmethode (bspw. VPN) erfolgen darf;
 - c) jeder Benutzer über einen eigenen, eindeutig identifizierbaren und angemessen geschützten (bspw. Passwort, Zertifikat) Zugang verfügen muss;
 - d) der Auftragnehmer beim Auftraggeber eine individuelle Zulassung für den Remote-Zugriff des jeweiligen Benutzers und die damit verbundenen Rechte beantragt;
 - e) der Auftragnehmer verpflichtet ist, eine aktuell gepflegte Liste der Personen und deren Aufgaben, in deren Rahmen der Remote-Zugriff gewährt wird, zu führen und diese bei Bedarf dem Auftraggeber zur Verfügung stellt;
 - f) der Auftragnehmer dem Auftraggeber jedwede Änderung der Benutzer unverzüglich mitteilt (Austritt eines Benutzers oder Neuanmeldung eines anderen Benutzers);
 - g) der Auftraggeber jederzeit berechtigt ist, einzelne Remote-Zugriffe und/oder den gesamten Remote-Zugriff des Auftragnehmers zu sperren. In einem solchen Fall sind jedoch negative Auswirkungen auf die Services zu erwarten. Für diese haftet der Auftragnehmer nicht, es sei denn, es liegen schwerwiegende Gründe für die Sperrung des Remote-Zugriffs vor, die der Auftragnehmer verursacht hat;
 - h) das Prinzip gilt, dass alles, was nicht ausdrücklich erlaubt ist, verboten ist, es sei denn, es liegt in der Natur des Auftrages, dass eine Handlung notwendig ist.
- (5) Sofern und soweit die Parteien im Hauptvertrag vereinbart haben, dass der Auftragnehmer zur Erbringung der vertragsgegenständlichen Leistungen Zugriff auf die Systeme des Auftraggebers benötigt, ist der Auftragnehmer verpflichtet,
 - a) beim Auftraggeber eine individuelle Zulassung für den Zugriff des jeweiligen Benutzers und die damit verbundenen Rechte zu beantragen;
 - b) eine aktuell gepflegte Liste der Personen und deren Aufgaben, in deren Rahmen der Zugriff gewährt wird, zu führen und diese bei Bedarf dem Auftraggeber zur Verfügung zu stellen;
 - c) dem Auftraggeber jedwede Änderung der Benutzer unverzüglich mitzuteilen (Austritt eines Benutzers oder Neuanmeldung eines anderen Benutzers).
- (6) Der Auftragnehmer ist verpflichtet, den Auftraggeber unverzüglich bei begründetem Verdacht einer Kompromittierung der für den vorliegenden Auftrag genutzten IT-Systeme und/oder Daten des Auftraggebers zu informieren.
- (7) Der Auftragnehmer stellt sicher, dass das für die Auftragsausführung eingesetzte Personal und das Personal, das Einblick in die IT-Systeme und/oder Daten des Auftraggebers erhalten kann, in den für die Auftragsausführung erforderlichen Methoden und Verfahren sowie in der IT-Sicherheit geschult und sich seiner Verantwortung für die Informationssicherheit bewusst ist.
- (8) Der Auftragnehmer hat sämtliche von ihm eingesetzten und/oder in den entsprechenden Vertrags- bzw. Vergabeunterlagen benannten Unterauftragnehmer in gleicher Weise zur Einhaltung dieser Regelungen zur Informationssicherheit zu verpflichten. Dies gilt auch für solche Unterauftragnehmer, deren Einsatz der Auftraggeber während der Vertragslaufzeit nachträglich zugestimmt hat.

Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte beim Unterauftragnehmer entsprechend dieser Vereinbarung einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der für die Informationssicherheit relevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Vorlage einer Kopie, zu erhalten.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung der Informationssicherheit des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.
- (9) Der Auftragnehmer wird dem Informationssicherheitsbeauftragten des Auftraggebers auf Verlangen einen Ansprechpartner/in für Fragen der Informationssicherheit namentlich benennen. Diese/r Ansprechpartner/in steht dem Auftraggeber während der üblichen Geschäftszeiten zur Verfügung.
- (10) Sofern und soweit Informationssicherheitsmängel beim Auftragnehmer auftreten sollten, werden die Parteien eine einvernehmliche Lösung zur Beseitigung dieser Informationssicherheitsmängel treffen. Sollte eine einvernehmliche Regelung scheitern, ist der Auftraggeber in Abhängigkeit von der Schwere der vorliegenden Informationssicherheitsmängel berechtigt, den Vertrag außerordentlich zu kündigen.
- (11) Sofern und soweit sich nach Vertragsschluss eine vom Auftraggeber zwingend geforderte Zertifizierung des Auftragnehmers ändern sollte (bspw. Feststellung von Mängeln oder vollständiger Entzug der Zertifizierung), ist der Auftragnehmer verpflichtet, den Auftraggeber unverzüglich zu informieren. Auf Anforderung hat der Auftragnehmer entsprechende Nachweise vorzulegen.
- (12) Sofern und soweit der mit dem Auftragnehmer geschlossene Vertrag Einsätze seiner Mitarbeiter/innen in den Räumlichkeiten des Auftraggebers beinhaltet, stellt der Auftragnehmer sicher, dass seine beim Auftraggeber eingesetzten Mitarbeiter/innen sich im

Rahmen ihres Einsatzes beim Auftraggeber über die für ihr jeweiliges Aufgabengebiet geltenden relevanten, internen Regelungen des Auftraggebers bei ihrem Ansprechpartner informieren (bspw. diejenigen zur Informationssicherheit) und diese während des gesamten Einsatzes einhalten.