Anlage B1d

der Vergabeunterlagen
zur Ausschreibung „Rahmenvereinbarung zur strategischen Beratung und IT-Dienstleistungen“ der AOK NordWest

Informationssicherheitsanforderungen

(nicht vom Bieter einzureichen)

Stand: 13.11.2026

Inhaltsverzeichnis

Rahmenteil ... 3
1 Gegenstand und Geltungsbereich ... 3
2 Begriffe ... 3
3 Zugang zu Systemen der Auftraggeberin und Remoteservice ... 4
4 Umgang mit Informationen der Auftraggeberin ... 4
5 Einsatz von KI-Systemen ... 5
6 Informationssicherheitsvorfälle ... 5
7 Unterauftragnehmer ... 6
8 Informationspflichten ... 6
9 Nachweise, Prüfrechte und Lieferantendialog ... 6
10 Pflichten bei Ende eines Einzelauftrags und der Rahmenvereinbarung ... 7
11 Änderungen dieser Anlage ... 8
Teil A: Organisatorische und technische Pflichten des Auftragnehmers ... 9
1 Organisation der Informationssicherheit ... 9
2 Personal ... 9
3 Sicherheit der Systeme des Auftragnehmers ... 9
4 Arbeitsumgebung ... 10
Teil B: Nutzung von Endgeräten und Zugängen der Auftraggeberin durch externe Personen ... 11
1 Geltung ... 11
2 Übergabe und Nutzung von Endgeräten der Auftraggeberin ... 11
3 Mobiles Arbeiten ... 11
4 Zugriff über die virtuelle Desktopumgebung mit Endgeräten des Auftragnehmers ... 12
5 Verlust, Diebstahl und Verdacht auf Schadsoftware ... 12
6 Arbeit in Räumen der Auftraggeberin ... 12
7 Rückgabe ... 12
Teil C: Sichere Softwareentwicklung ... 13
1 Eigene Vorgaben des Auftragnehmers ... 13
2 Entwicklungsumgebung und Quellcode ... 13
3 Sicherheitsanforderungen ... 13
4 Komponenten Dritter und Open Source ... 14
5 Tests, Code Review und Testdaten ... 14
6 KI-gestützte Entwicklung ... 14
7 Dokumentation und Produktivstellung ... 14
8 Schwachstellen ... 14
Teil D: Meldeweg für Informationssicherheitsvorfälle ... 15
1 Kontakt ... 15
2 Zu melden sind insbesondere ... 15
3 Inhalte der Meldungen ... 15

Rahmenteil

1 Gegenstand und Geltungsbereich

(1) Diese Anlage legt die Anforderungen an die Informationssicherheit fest, die der Auftragnehmer bei der Erbringung sämtlicher Leistungen aus der Rahmenvereinbarung und den Einzelaufträgen einhält.

(2) Die Anlage besteht aus diesem Rahmenteil und den folgenden Unteranlagen:

- Teil A Organisatorische und technische Pflichten des Auftragnehmers (alle Einzelaufträge)
- Teil B Nutzung von Endgeräten und Zugängen der Auftraggeberin durch externe Personen (alle Einzelaufträge)
- Teil C Sichere Softwareentwicklung (nur Einzelaufträge mit Unterstützung bei der Softwareentwicklung oder Erstellung beziehungsweise Anpassung von Software)
- Teil D Meldeweg für Informationssicherheitsvorfälle

(3) Die Ergänzenden Vertragsbedingungen (Anlage B1a) und die Datenschutzbestimmungen (Anlagen B1c1 und B1c2) bleiben unberührt. Diese Anlage wiederholt deren Regelungen nicht, sondern ergänzt sie um Anforderungen der Informationssicherheit. Soweit der Auftragnehmer Sozialdaten im Auftrag verarbeitet und Regelungen dieser Anlage den Regelungen der Anlage B1c2 widersprechen, gehen die Regelungen der Anlage B1c2 vor. Weitergehende Anforderungen dieser Anlage an die Informationssicherheit bleiben davon unberührt.

(4) Der Auftragnehmer stellt sicher, dass alle von ihm eingesetzten Personen die für ihre Tätigkeit maßgeblichen Inhalte dieser Anlage vor Aufnahme der Tätigkeit kennen und einhalten.

2 Begriffe

(1) Informationen der Auftraggeberin sind alle Informationen und Daten, die der Auftragnehmer im Zusammenhang mit der Rahmenvereinbarung erhält, einsehen kann oder für die Auftraggeberin erstellt, unabhängig von Form und Speicherort. Dazu gehören insbesondere Sozialdaten, sonstige personenbezogene Daten sowie Betriebs- und Geschäftsgeheimnisse.

(2) Informationssicherheitsvorfall ist jedes Ereignis, das die Vertraulichkeit, Integrität, Verfügbarkeit oder Authentizität von Informationen der Auftraggeberin oder von Systemen, über die Leistungen erbracht werden, beeinträchtigt oder beeinträchtigen kann. Ein begründeter Verdacht genügt.

(3) Systeme der Auftraggeberin sind IT-Systeme, Anwendungen, Zugänge und Endgeräte, die die Auftraggeberin oder ein von ihm beauftragter Dienstleister betreibt oder bereitstellt.

(4) Kritische Einzelaufträge sind Einzelaufträge, bei denen der Auftragnehmer in Prozesse eingebunden ist, die der Erbringung der kritischen Dienstleistung der Auftraggeberin als Betreiber einer kritischen Anlage im Sinne des BSI-Gesetzes dienen, oder administrative Berechtigungen auf Systemen erhält, die diese Prozesse unterstützen. Die Auftraggeberin kennzeichnet kritische Einzelaufträge im Einzelauftrag.

3 Zugang zu Systemen der Auftraggeberin und Remoteservice

(1) Der Auftragnehmer verarbeitet Informationen der Auftraggeberin ausschließlich auf Systemen der Auftraggeberin oder über die von der Auftraggeberin bereitgestellten Zugänge. Ausnahmen regelt Nr. 4 Abs. 3.

(2) Der Zugriff auf Systeme der Auftraggeberin erfolgt beim Remoteservice ausschließlich über von der Auftraggeberin bereitgestellte Zugänge, insbesondere eine virtuelle Desktopumgebung oder einen VPN-Zugang mit einem Endgerät der Auftraggeberin. Eigene Fernwartungs- oder Fernzugriffssoftware des Auftragnehmers ist nicht zulässig.

(3) Remoteservice und mobiles Arbeiten sind nur innerhalb der Mitgliedstaaten der Europäischen Union, der weiteren Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum, der Schweiz und des Vereinigten Königreichs zulässig. Die Datenschutzbestimmungen bleiben unberührt.

(4) Jede eingesetzte Person erhält eine persönliche Kennung. Sammel- und Gruppenkennungen sowie die Weitergabe von Zugangsdaten sind unzulässig. Die Anmeldung erfolgt mit Mehrfaktorauthentisierung, soweit die Auftraggeberin sie bereitstellt.

(5) Kennungen und Berechtigungen werden ausschließlich über den Berechtigungsprozess der Auftraggeberin beantragt. Sie werden auf die Dauer des Einzelauftrags befristet und nach dem Grundsatz der geringsten Berechtigung vergeben. Der Auftragnehmer teilt der Auftraggeberin hierzu für jede Person Name, Unternehmen, Tätigkeit und Einsatzzeitraum mit.

(6) Der Auftragnehmer teilt das Ausscheiden, den Austausch oder eine längere Abwesenheit einer eingesetzten Person der Auftraggeberin in Textform mit, möglichst vorab, spätestens am Arbeitstag des Ereignisses, damit Kennungen und Zutrittsberechtigungen gesperrt werden können.

(7) Endgeräte des Auftragnehmers dürfen nicht mit dem internen Netz der Auftraggeberin verbunden werden. Für Endgeräte des Auftragnehmers, mit denen auf eine virtuelle Desktopumgebung der Auftraggeberin zugegriffen wird, gilt Teil B Nr. 4.

(8) Die Auftraggeberin protokolliert Zugriffe auf ihre Systeme nach ihren Vorgaben. Der Auftragnehmer weist die eingesetzten Personen darauf hin.

4 Umgang mit Informationen der Auftraggeberin

(1) Der Auftragnehmer beachtet die Klassifizierung von Informationen der Auftraggeberin in den Stufen öffentlich, intern, vertraulich und streng vertraulich. Nicht gekennzeichnete Informationen behandelt er mindestens als intern, Sozialdaten mindestens als vertraulich.

(2) Informationen der Auftraggeberin werden nur den eingesetzten Personen zugänglich gemacht, die sie für die Erbringung des jeweiligen Einzelauftrags benötigen.

(3) Die Speicherung von Informationen der Auftraggeberin auf Systemen des Auftragnehmers oder seiner Unterauftragnehmer ist nur nach vorheriger Zustimmung der Auftraggeberin in Textform zulässig. In diesem Fall speichert der Auftragnehmer die Informationen verschlüsselt nach dem Stand der Technik, beschränkt den Zugriff auf die berechtigten Personen und löscht sie, sobald sie nicht mehr benötigt werden, spätestens nach Nr. 10 Abs. 3.

(4) Informationen der Auftraggeberin werden nur über von der Auftraggeberin freigegebene Kanäle übermittelt. Vertrauliche und streng vertrauliche Informationen werden außerhalb der

Systeme der Auftraggeberin nur verschlüsselt übermittelt, vorzugsweise über das von der Auftraggeberin bereitgestellte Verfahren zum sicheren Dateiaustausch. Private E-Mail-Konten, private Cloudspeicher, Messengerdienste und Wechseldatenträger sind nicht zulässig.

(5) Papierunterlagen ab der Stufe vertraulich bewahrt der Auftragnehmer verschlossen auf. Er vernichtet sie mindestens nach Sicherheitsstufe 4 der DIN EN ISO/IEC 21964.

(6) Verarbeitet der Auftragnehmer oder ein Unterauftragnehmer im Rahmen eines Einzelauftrags Sozialdaten oder Gesundheitsdaten der Auftraggeberin mittels eines Cloud-Computing-Dienstes, einschließlich KI-Diensten und Kollaborationsplattformen, müssen die Voraussetzungen des § 393 SGB V erfüllt sein. Der Auftragnehmer weist dies vor Beginn der Verarbeitung nach, insbesondere durch ein aktuelles C5-Testat des Cloudanbieters nach § 393 Abs. 3 und 4 SGB V oder ein dort zugelassenes gleichwertiges Testat oder Zertifikat.

5 Einsatz von KI-Systemen

(1) Der Auftragnehmer setzt KI-Systeme zur Leistungserbringung nur nach vorheriger Zustimmung des Auftraggebers in Textform ein. Vor dem Einsatz benennt er Produkt, Anbieter, Ort der Datenverarbeitung und Zweck des Einsatzes und erklärt, ob Eingaben zum Training des Modells verwendet werden. Sozialdaten, sonstige personenbezogene Daten und als vertraulich eingestufte Informationen des Auftraggebers dürfen nur in vom Auftraggeber freigegebene KI-Systeme eingegeben werden. Der Auftraggeber kann den Einsatz bestimmter KI-Systeme jederzeit untersagen. Die Zustimmung kann für einen Einzelauftrag im Einzelauftrag erteilt werden.

(2) Der Auftragnehmer prüft Ergebnisse von KI-Systemen fachlich, bevor er sie der Auftraggeberin übergibt. Die Verantwortung für die Leistung bleibt beim Auftragnehmer.

(3) Für KI-Systeme, die als Cloud-Computing-Dienst betrieben werden, gilt zusätzlich Nr. 4 Abs. 6. Ziffer 14.4 der Ergänzenden Vertragsbedingungen (Anlage B1a) bleibt unberührt. Für mit Unterstützung von KI-Systemen erstellten Quellcode gilt Teil C Nr. 6.

6 Informationssicherheitsvorfälle

(1) Der Auftragnehmer meldet der Auftraggeberin jeden Informationssicherheitsvorfall, der Informationen oder Systeme der Auftraggeberin betrifft oder betreffen kann. Dazu gehören auch Vorfälle beim Auftragnehmer oder bei Unterauftragnehmern, insbesondere die Kompromittierung von Konten, Endgeräten oder Systemen, über die Leistungen erbracht werden, der Verlust oder Diebstahl von Endgeräten, Datenträgern und Zugangsmitteln, Phishingangriffe mit Bezug zur Auftraggeberin sowie bekannt gewordene Schwachstellen in vom Auftragnehmer gelieferten Komponenten.

(2) Es gelten folgende Fristen:

a) Erstmeldung unverzüglich, spätestens 24 Stunden nach Kenntnis,

b) Folgemeldung mit Bewertung von Schweregrad und Auswirkungen, vorhandenen Kompromittierungsindikatoren und ergriffenen Maßnahmen spätestens 72 Stunden nach Kenntnis,

c) Abschlussbericht mit Ursache, Auswirkungen, ergriffenen Abhilfemaßnahmen und Maßnahmen gegen eine Wiederholung spätestens einen Monat nach der Folgemeldung.

Auf Verlangen der Auftraggeberin erstattet der Auftragnehmer Zwischenmeldungen. Die Fristen ermöglichen der Auftraggeberin die Erfüllung seiner Meldepflichten nach § 32 BSI-Gesetz.

(3) Meldungen erfolgen über den Meldeweg nach Teil D. Eine Meldung allein an einzelne Beschäftigte der Auftraggeberin genügt nicht.

(4) Meldepflichten nach Art. 33 DSGVO und nach den Datenschutzbestimmungen (Anlagen B1c1 und B1c2) bleiben unberührt. Eine Meldung kann beide Pflichten erfüllen, wenn sie die jeweils erforderlichen Angaben enthält.

(5) Der Auftragnehmer wirkt bei der Bewältigung des Vorfalls mit. Er stimmt Sofortmaßnahmen mit der Auftraggeberin ab, sichert Beweismittel wie Protokolle und betroffene Datenträger unverändert, erteilt die erforderlichen Auskünfte und nimmt an Abstimmungen teil. Informationen über Vorfälle bei der Auftraggeberin gibt er ohne Zustimmung der Auftraggeberin nicht an Dritte weiter, soweit keine gesetzliche Pflicht besteht.

7 Unterauftragnehmer

(1) Ergänzend zu Ziffer 3 der Ergänzenden Vertragsbedingungen verpflichtet der Auftragnehmer jeden Unterauftragnehmer vor dessen Einsatz in Textform auf sämtliche Pflichten dieser Anlage einschließlich der Melde-, Mitwirkungs- und Prüfpflichten.

(2) Mit dem Antrag auf Zustimmung zum Einsatz eines Unterauftragnehmers benennt der Auftragnehmer dessen Sitz, die Orte der Leistungserbringung und der Datenverarbeitung, den Leistungsumfang sowie den vorgesehenen Zugriff auf Informationen und Systeme der Auftraggeberin.

(3) Die Weitergabe an weitere Unterauftragnehmer bedarf ebenfalls der vorherigen Zustimmung der Auftraggeberin.

8 Informationspflichten

Der Auftragnehmer informiert die Auftraggeberin unverzüglich in Textform über Entwicklungen, die die Informationssicherheit der Leistungserbringung beeinträchtigen oder gefährden können, insbesondere über

a) wesentliche Änderungen seines Informationssicherheitsmanagements, etwa den Wegfall einer Zertifizierung,

b) Wechsel von Unterauftragnehmern oder von Orten der Datenverarbeitung,

c) Änderungen, die eine Offenbarungspflicht im Sinne von Ziffer 14.5 der Ergänzenden Vertragsbedingungen (Anlage B1a) begründen können,

d) behördliche Anordnungen mit Bezug zu Informationen der Auftraggeberin, soweit eine Mitteilung rechtlich zulässig ist.

9 Nachweise, Prüfrechte und Lieferantendialog

(1) Der Auftragnehmer weist der Auftraggeberin auf Verlangen, höchstens einmal je Vertragsjahr, die Umsetzung dieser Anlage durch geeignete Unterlagen nach, etwa Zertifikate, Richtlinien oder Schulungsnachweise.

(2) Die Auftraggeberin ist berechtigt, die Einhaltung dieser Anlage beim Auftragnehmer und bei dessen Unterauftragnehmern selbst oder durch einen zur Verschwiegenheit verpflichteten Dritten zu prüfen. Der Dritte darf kein Wettbewerber des Auftragnehmers sein.

(3) Regelfall sind Auskunftsersuchen, Dokumentenprüfungen und Prüfungen per Videokonferenz. Prüfungen vor Ort finden bei kritischen Einzelaufträgen sowie anlassbezogen statt, insbesondere nach einem Informationssicherheitsvorfall oder bei Anhaltspunkten für Verstöße gegen diese Anlage.

(4) Prüfungen werden mit einer Frist von mindestens vier Wochen angekündigt, anlassbezogene Prüfungen mit einer Frist von mindestens fünf Arbeitstagen. Sie finden während der üblichen Geschäftszeiten statt und berücksichtigen den Schutz der Informationen anderer Kunden des Auftragnehmers.

(5) Jede Partei trägt ihre Kosten der Prüfung selbst. Ergibt eine Prüfung wesentliche Abweichungen, trägt der Auftragnehmer die Kosten einer erforderlichen Nachprüfung.

(6) Zu festgestellten Abweichungen legt der Auftragnehmer innerhalb von vier Wochen einen Maßnahmenplan vor und setzt die Maßnahmen in der mit der Auftraggeberin vereinbarten Frist um.

(7) Der Auftragnehmer wirkt bei Nachweisprüfungen der Auftraggeberin nach § 39 BSI-Gesetz sowie bei Prüfungen durch das Bundesamt für Sicherheit in der Informationstechnik, durch Aufsichtsbehörden und durch von der Auftraggeberin beauftragte Prüfer mit, soweit seine Leistungen betroffen sind. Ziffer 15 der Ergänzenden Vertragsbedingungen (Anlage B1a) bleibt unberührt.

(8) Im Lieferantendialog nach Teil A Nr. 14 der EVB-IT-Rahmenvereinbarung (Anlage B1) ist Informationssicherheit fester Tagesordnungspunkt mit den Inhalten Vorfälle, Abweichungen und offene Maßnahmen, Änderungen bei Unterauftragnehmern sowie geplante Änderungen mit Bezug zur Informationssicherheit. Das Protokoll dient zugleich als Grundlage der Bewertung des Auftragnehmers durch die Auftraggeberin.

10 Pflichten bei Ende eines Einzelauftrags und der Rahmenvereinbarung

Bei Ende eines Einzelauftrags, bei Ende der Rahmenvereinbarung und für einzelne Personen bei deren Ausscheiden aus der Leistungserbringung gilt:

(1) Rückgabe. Der Auftragnehmer gibt spätestens am letzten Leistungstag sämtliche von der Auftraggeberin überlassenen Endgeräte, Datenträger und Zugangsmittel wie Token, Smartcards, Ausweise und Schlüssel vollständig zurück. Die Rückgabe wird in einem Übergabeprotokoll bestätigt. Ein Zurückbehaltungsrecht besteht nicht. Nicht zurückgegebene Gegenstände meldet der Auftragnehmer unverzüglich nach Teil D.

(2) Entzug von Kennungen. Der Auftragnehmer teilt der Auftraggeberin spätestens fünf Arbeitstage vor dem letzten Leistungstag alle Personen mit, für die Kennungen, Zugänge oder Zutrittsberechtigungen bestehen. Er wirkt daran mit, dass diese mit Ablauf des letzten Leistungstags gesperrt werden. Von ihm angelegte technische Zugänge wie Schnittstellenschlüssel, Token oder Zugänge zu Repositories und Kollaborationsräumen widerruft er oder übergibt sie zur Änderung an die Auftraggeberin. Er bestätigt in Textform, dass keine weiteren Zugänge seiner Personen bestehen.

(3) Löschung. Der Auftragnehmer löscht innerhalb von 30 Kalendertagen nach dem letzten Leistungstag sämtliche Informationen der Auftraggeberin auf seinen Systemen und auf Systemen seiner Unterauftragnehmer einschließlich Kopien und Inhalten in KI-Systemen so, dass eine Wiederherstellung nach dem Stand der Technik ausgeschlossen ist. Informationen in Datensicherungen, die nicht gezielt gelöscht werden können, werden bis zu ihrem Überschreiben gesperrt und spätestens drei Monate nach dem letzten Leistungstag

überschrieben. Unterliegen Informationen einer gesetzlichen Aufbewahrungspflicht, werden sie bis zum Fristablauf gesperrt und danach gelöscht. Die Löschung bestätigt eine vertretungsberechtigte Person des Auftragnehmers in Textform unter Angabe von Umfang, Systemen, Verfahren und Datum, einschließlich der Bestätigungen der Unterauftragnehmer. Ziffer 14.2 letzter Satz der Ergänzenden Vertragsbedingungen (Anlage B1a) bleibt unberührt. Für Sozialdaten im Auftrag gehen die Regelungen der Anlage B1c2 vor.

(4) Übergabe von Tätigkeitsergebnissen. Der Auftragnehmer übergibt ohne gesonderte Aufforderung sämtliche Tätigkeitsergebnisse im Sinne von Ziffer 6 der Ergänzenden Vertragsbedingungen (Anlage B1a) einschließlich Dokumentation, Konfigurationen und Quellcode vollständig und in bearbeitbarem Format, soweit sie sich nicht bereits im Quellcoderepository oder in Ablagen der Auftraggeberin befinden.

(5) Vertraulichkeit. Die Fortgeltung der Geheimhaltungspflichten richtet sich nach Ziffer 14.3 der Ergänzenden Vertragsbedingungen (Anlage B1a) und den Datenschutzbestimmungen (Anlage B1c1 bzw. B1c2).

11 Änderungen dieser Anlage

(1) Es gilt die Fassung dieser Anlage bei Bereitstellung der Vergabeunterlagen.

(2) Die Auftraggeberin kann die Anforderungen dieser Anlage anpassen, soweit dies aufgrund gesetzlicher oder behördlicher Vorgaben, aufgrund von Prüfungsfeststellungen oder aufgrund geänderter interner Vorgaben erforderlich ist. Er kündigt Änderungen in Textform mit einer Umsetzungsfrist von mindestens drei Monaten an. Eine kürzere Frist ist nur zulässig, wenn gesetzliche oder behördliche Vorgaben sie erfordern. Für Mehraufwand gilt Ziffer 12 der Ergänzenden Vertragsbedingungen (Anlage B1a).

(3) Als Ergänzung angekündigt sind die Programmierrichtlinien der Auftraggeberin je Programmiersprache. Nach ihrer Bereitstellung gelten sie mit einer Umsetzungsfrist von drei Monaten.

Teil A: Organisatorische und technische Pflichten des Auftragnehmers

Diese Unteranlage gibt die Pflichten für Auftragnehmer aus der Richtlinie Informationssicherheit in Lieferanten- und Dienstleisterbeziehungen der Auftraggeberin wieder, soweit sie nicht bereits im Rahmenteil geregelt sind. Sie gilt für alle Einzelaufträge.

1 Organisation der Informationssicherheit

(1) Der Auftragnehmer unterhält ein Informationssicherheitsmanagement, das der Größe seines Unternehmens und den angebotenen Leistungen angemessen ist. Es umfasst mindestens eine Leitlinie zur Informationssicherheit, festgelegte Verantwortlichkeiten, eine Betrachtung der Risiken, einen Prozess zur Behandlung von Informationssicherheitsvorfällen und regelmäßige interne Überprüfungen.

(2) Der Auftragnehmer benennt der Auftraggeberin bei Zuschlag eine Ansprechperson für Informationssicherheit und eine Vertretung. Änderungen teilt er unverzüglich mit.

(3) Der Auftragnehmer dokumentiert seine Maßnahmen so, dass sie bei einer Prüfung nach Nr. 9 des Rahmenteils nachvollziehbar sind.

2 Personal

(1) Der Auftragnehmer verpflichtet die eingesetzten Personen vor Aufnahme der Tätigkeit nach Ziffer 14.1 der Ergänzenden Vertragsbedingungen (Anlage B1a) und den Datenschutzbestimmungen (Anlage B1c1 bzw. B1c2). Die Verpflichtung umfasst die Wahrung des Sozialgeheimnisses.

(2) Die eingesetzten Personen haben innerhalb der letzten 24 Monate eine Sensibilisierung zur Informationssicherheit absolviert, die mindestens Phishing, Social Engineering, Umgang mit Informationen und das Melden von Vorfällen behandelt. Der Auftragnehmer weist dies auf Verlangen nach.

(3) Personen mit einer Kennung der Auftraggeberin nehmen auf Verlangen an den Pflichtschulungen der Auftraggeberin zu Informationssicherheit und Datenschutz teil. Der Aufwand hierfür ist in die Preise einzukalkulieren.

(4) Der Auftragnehmer stellt durch Vertretungsregelungen und Wissenssicherung sicher, dass der Ausfall einzelner Personen die Leistungserbringung nicht gefährdet. Ziffer 4.2 der Ergänzenden Vertragsbedingungen (Anlage B1a) bleibt unberührt.

3 Sicherheit der Systeme des Auftragnehmers

Für Systeme des Auftragnehmers, die er für die Kommunikation mit der Auftraggeberin, für den Zugriff auf Systeme der Auftraggeberin oder nach Zustimmung für die Verarbeitung von Informationen der Auftraggeberin nutzt, gilt:

a) Betriebssysteme und Anwendungen werden in vom Hersteller unterstützten Versionen betrieben. Sicherheitsupdates werden zeitnah, kritische Sicherheitsupdates unverzüglich eingespielt.

b) Ein aktueller Schutz vor Schadsoftware ist aktiv.

c) Mobile Endgeräte und Datenträger sind vollständig verschlüsselt. Eine automatische Bildschirmsperre bei Inaktivität ist aktiviert.

d) Zugänge zu E-Mail, Kollaborationsplattformen und Fernzugängen sind mit Mehrfaktorauthentisierung geschützt.

e) Administrative Berechtigungen werden nur für administrative Tätigkeiten genutzt und nicht für die tägliche Arbeit.

f) Sicherheitsrelevante Ereignisse werden protokolliert, soweit dies zur Erkennung und Aufklärung von Vorfällen erforderlich ist.

g) Kryptografische Verfahren entsprechen dem Stand der Technik.

4 Arbeitsumgebung

(1) Unterlagen und Bildschirminhalte mit Informationen der Auftraggeberin werden vor Einsicht durch Unbefugte geschützt. Beim Verlassen des Arbeitsplatzes werden Unterlagen weggeschlossen und Bildschirme gesperrt.

(2) Vertrauliche Gespräche werden nicht in öffentlich zugänglichen Bereichen geführt. In öffentlichen Bereichen wird ein Sichtschutz für Bildschirme verwendet.

Teil B: Nutzung von Endgeräten und Zugängen der Auftraggeberin durch externe Personen

Diese Unteranlage gibt die Pflichten für externe Personen aus den Vorgaben der Auftraggeberin zur Nutzung von mobilen Endgeräten und zur Berechtigungsvergabe für externe Personen wieder. Sie gilt für alle Einzelaufträge, bei der Arbeit in Räumen der Auftraggeberin ebenso wie beim mobilen Arbeiten.

1 Geltung

Die Regelungen gelten für alle Personen des Auftragnehmers, denen die Auftraggeberin Endgeräte, Zugangsmittel, Zugänge oder Arbeitsplätze bereitstellt. Der Auftragnehmer stellt ihre Einhaltung durch die eingesetzten Personen sicher.

2 Übergabe und Nutzung von Endgeräten der Auftraggeberin

(1) Endgeräte und Zugangsmittel werden gegen Quittung übergeben. Sie dürfen ausschließlich für Leistungen aus dem jeweiligen Einzelauftrag genutzt werden. Eine private Nutzung und die Weitergabe an andere Personen sind unzulässig.

(2) Von der Auftraggeberin eingerichtete Sicherheitsmaßnahmen dürfen nicht deaktiviert oder umgangen werden. Software wird ausschließlich durch die Auftraggeberin bereitgestellt. Das Entfernen von Nutzungsbeschränkungen und das Zurücksetzen der Geräte sind unzulässig.

(3) Externe Speichermedien wie USB-Sticks, Speicherkarten, CDs und DVDs dürfen nicht genutzt werden. Für den Datenaustausch steht das von der Auftraggeberin bereitgestellte Verfahren zum sicheren Dateiaustausch zur Verfügung.

(4) Updates und Neustarts, zu denen die Auftraggeberin auffordert, werden unverzüglich, spätestens innerhalb von 14 Tagen durchgeführt. Andernfalls kann das Gerät gesperrt werden.

(5) Dokumente werden nicht lokal auf dem Endgerät gespeichert, sondern nur in den vom Auftraggeber vorgesehenen Ablagen.

(6) Drahtlose Schnittstellen wie Bluetooth werden nur wie von der Auftraggeberin konfiguriert genutzt und bei Nichtgebrauch deaktiviert. Es wird nur von der Auftraggeberin freigegebenes Zubehör angeschlossen.

3 Mobiles Arbeiten

(1) Mobiles Arbeiten ist nur in den in Nr. 3 Abs. 3 des Rahmenteils genannten Staaten zulässig.

(2) Öffentliche WLAN-Netze und Hotspots dürfen nur mit aktiver VPN-Verbindung zum Auftraggeber genutzt werden. Häusliche WLAN-Netze sind mindestens mit WPA2, vorzugsweise WPA3, verschlüsselt. Die Funktion WPS ist deaktiviert.

(3) Endgeräte werden nicht unbeaufsichtigt an öffentlich zugänglichen Orten und nicht sichtbar in Fahrzeugen zurückgelassen. Beim Verlassen des Geräts wird der Bildschirm gesperrt.

(4) Bildschirminhalte werden vor Einsicht geschützt, insbesondere durch eine Blickschutzfolie in Verkehrsmitteln und öffentlichen Bereichen.

4 Zugriff über die virtuelle Desktopumgebung mit Endgeräten des Auftragnehmers

Stellt die Auftraggeberin einen Zugriff über eine virtuelle Desktopumgebung bereit, dürfen hierfür Endgeräte des Auftragnehmers genutzt werden, wenn folgende Anforderungen erfüllt sind:

a) Das Endgerät wird vom Auftragnehmer verwaltet und ist einer Person zugeordnet. Private oder gemeinsam genutzte Geräte sowie öffentlich zugängliche Rechner sind ausgeschlossen.

b) Betriebssystem und Software werden in unterstützten Versionen mit aktuellen Sicherheitsupdates betrieben. Ein aktueller Schutz vor Schadsoftware ist aktiv.

c) Der Datenträger des Endgeräts ist vollständig verschlüsselt. Die Anmeldung erfolgt mit persönlicher Kennung. Eine automatische Bildschirmsperre ist aktiviert.

d) Es wird ausschließlich der von der Auftraggeberin vorgegebene Client verwendet.

e) Informationen der Auftraggeberin werden nicht aus der virtuellen Desktopumgebung heraus kopiert, heruntergeladen, gedruckt oder per Bildschirmfoto festgehalten, soweit die Auftraggeberin dies nicht ausdrücklich freigegeben hat.

Die Auftraggeberin kann die Einhaltung technisch prüfen und den Zugriff bei Abweichungen sperren.

5 Verlust, Diebstahl und Verdacht auf Schadsoftware

Verlust oder Diebstahl eines Endgeräts oder Zugangsmittels sowie der Verdacht auf Schadsoftware werden unverzüglich nach Teil D gemeldet. Zusätzlich wird die im Einzelauftrag benannte Ansprechperson der Auftraggeberin informiert.

6 Arbeit in Räumen der Auftraggeberin

(1) Der von der Auftraggeberin ausgegebene Ausweis wird sichtbar getragen. Zutritt besteht nur zu den freigegebenen Bereichen. Sicherheitsbereiche werden nur in Begleitung oder mit gesonderter Berechtigung betreten.

(2) Fotos und Aufnahmen von Räumen, Bildschirmen und Unterlagen sind ohne Zustimmung der Auftraggeberin unzulässig.

(3) Die Regelungen in § 3 Abs. 2 der Datenschutzbestimmungen (Anlage B1c1) bleiben unberührt.

7 Rückgabe

Für die Rückgabe von Endgeräten und Zugangsmitteln gilt Nr. 10 Abs. 1 des Rahmenteils.

Teil C: Sichere Softwareentwicklung

Diese Unteranlage gibt die Anforderungen der Richtlinie zur sicheren Entwicklung der Auftraggeberin für Auftragnehmer wieder. Sie gilt für Einzelaufträge mit Unterstützung bei der Softwareentwicklung (Teil B EVB-IT Dienstleistung) und für Einzelaufträge über die Erstellung oder Anpassung von Software (Teil B EVB-IT Erstellung). Sie umfasst Anwendungen, Schnittstellen, Skripte, Automatisierungen und Low-Code-Lösungen. Der Auftragnehmer kennt, akzeptiert und setzt diese Anforderungen um und verpflichtet alle entwickelnden Personen darauf.

1 Eigene Vorgaben des Auftragnehmers

Der Auftragnehmer unterhält eigene Vorgaben zur sicheren Entwicklung und schreibt sie fort. Sie berücksichtigen die Anforderungen dieser Unteranlage.

2 Entwicklungsumgebung und Quellcode

(1) Quellcode wird ausschließlich im Quellcoderepository der Auftraggeberin geführt. Kopien in Repositories des Auftragnehmers bedürfen der Zustimmung der Auftraggeberin.

(2) Entwicklungs-, Test- und Produktivumgebung sind voneinander getrennt. Software wird nicht auf Systemen entwickelt, auf denen sie produktiv genutzt wird. Nicht abgenommene Stände werden nur auf den dafür vorgesehenen Systemen getestet.

(3) Der Zugriff auf das Repository erfolgt mit persönlicher Kennung und Mehrfaktorauthentisierung. Berechtigungen werden nach dem Grundsatz der geringsten Berechtigung vergeben. Erweiterte Berechtigungen werden nur nach gesonderter Freigabe durch die Auftraggeberin und nur für die Dauer der Tätigkeit erteilt. Für den Entzug gilt Nr. 10 Abs. 2 des Rahmenteils.

(4) Jede Änderung ist über die Versionsverwaltung einer Person zuordenbar. Aktionen externer Personen sind über die Protokollierung nachvollziehbar.

(5) Zugangsdaten, Schlüssel und Token werden nicht im Quellcode oder im Repository gespeichert.

3 Sicherheitsanforderungen

(1) Bei der Konzeption werden die Risiken für Vertraulichkeit, Integrität und Verfügbarkeit betrachtet und mit den abgeleiteten Maßnahmen dokumentiert. Zu betrachten sind mindestens Authentisierung und Berechtigungskonzept, Protokollierung, Datensicherung und Wiederherstellung, Aktualisierung der Software, Einsatz von Kryptografie und Schlüsselmanagement, zulässige Netzkommunikation, Härtung, Eingabevalidierung, restriktive Schnittstellen und Tests vor produktiver Nutzung.

(2) Zu berücksichtigen sind die OWASP Top 10 bei Webanwendungen, die OWASP API Security Top 10 bei Schnittstellen, der OWASP MASVS bei mobilen Anwendungen und die CWE Top 25 bei jeder Softwareentwicklung. Mobile Anwendungen, die personenbezogene Daten verarbeiten, erfüllen OWASP MASVS Level 2.

(3) Webanwendungen verfügen über ein sicheres Sessionmanagement ohne Eigenimplementierung, prüfen alle Eingaben und sind gegen Cross-Site-Scripting, Cross-Site-Request-Forgery und Clickjacking geschützt. Die Kommunikation ist verschlüsselt. Ein Rückfall auf unverschlüsselte Kommunikation ist unterbunden. Backenddienste werden nur verschlüsselt und nach gegenseitiger Authentisierung angebunden.

(4) Anwendungen arbeiten mit den geringsten erforderlichen Berechtigungen. Zugriffe und Anwendungsfehler werden protokolliert.

(5) Abweichungen von diesen Anforderungen sind zu begründen, zu dokumentieren und vom Auftraggeber freizugeben.

4 Komponenten Dritter und Open Source

(1) Komponenten Dritter und Open Source Software werden nur aus vertrauenswürdigen Quellen und über die vom Auftraggeber vorgesehenen Repository-Manager bezogen. Komponenten mit bekannten kritischen Schwachstellen werden ohne Freigabe der Auftraggeberin nicht eingesetzt.

5 Tests, Code Review und Testdaten

(1) Modul- und Integrationstests und die Anforderungen an Testdaten werden vorab geplant.

(2) Eine statische Codeanalyse wird in der Entwicklungsumgebung und im Buildprozess eingesetzt. Vor Produktivstellung prüft eine unabhängige entwickelnde Person die Software auf Fehler und Schwachstellen. Feststellungen werden behoben oder dokumentiert und vom Auftraggeber akzeptiert.

(3) Für Tests werden vorzugsweise synthetische Daten verwendet. Produktivdaten und Sozialdaten werden nur nach Freigabe durch den Auftraggeber einschließlich dessen Datenschutzbeauftragten, nur in Testsystemen, auf das Erforderliche beschränkt und soweit möglich anonymisiert oder pseudonymisiert verwendet. Die Nutzung wird protokolliert.

6 KI-gestützte Entwicklung

(1) Quellcode der Auftraggeberin, Zugangsdaten und Konfigurationen dürfen nur in vom Auftraggeber freigegebene KI-Systeme eingegeben werden.

(2) Mit Unterstützung von KI-Systemen erstellter Quellcode unterliegt denselben Prüf-, Review- und Lizenzanforderungen wie sonstiger Quellcode.

7 Dokumentation und Produktivstellung

(1) Vor Produktivstellung dokumentiert der Auftragnehmer die für den sicheren Betrieb erforderlichen Angaben, mindestens Funktion und Aufbau der Software, bekannte Fehler und Einschränkungen, sicherheitsrelevante Konfiguration, Berechtigungskonzept, Protokollierung, Datensicherung und Wiederherstellung, Härtungsmöglichkeiten, eingesetzte kryptografische Verfahren, Abhängigkeiten und Rechte Dritter, Installation und Aktualisierung, Schlüsselmanagement sowie erforderliche Netzkommunikation und Schnittstellen.

(2) Der Auftragnehmer bestätigt vor Produktivstellung, dass die Software fertig entwickelt und dokumentiert ist, alle Entwicklertests bestanden hat und für den produktiven Einsatz geeignet ist.

8 Schwachstellen

Der Auftragnehmer meldet während der Leistungserbringung und während einer vereinbarten Pflege bekannt gewordene Schwachstellen in gelieferter Software und deren Komponenten unverzüglich nach Teil D. Die Meldung enthält eine Bewertung und einen Vorschlag zur Behebung. Fristen zur Behebung werden im Einzelauftrag festgelegt.

Teil D: Meldeweg für Informationssicherheitsvorfälle

1 Kontakt

Meldeweg	Kontakt
Funktionspostfach Informationssicherheit	IT-Sicherheit@nw.aok.de
Zusätzlich zu informieren	Die im Einzelauftrag benannte Ansprechperson der Auftraggeberin

Meldungen mit Einzelheiten zu Schwachstellen oder Kompromittierungsindikatoren werden verschlüsselt übermittelt. Ist dies nicht möglich, wird der Übermittlungsweg vorab mit dem Auftraggeber abgestimmt.

2 Zu melden sind insbesondere

a) Verlust oder Diebstahl von Endgeräten, Datenträgern oder Zugangsmitteln,

b) Verdacht auf Schadsoftware oder Kompromittierung von Konten und Systemen,

c) Preisgabe von Zugangsdaten, etwa durch Phishing,

d) Fehlversand oder unbefugte Weitergabe von Informationen der Auftraggeberin,

e) unbefugter Zugriff auf Informationen oder Räume der Auftraggeberin,

f) bekannt gewordene Schwachstellen in gelieferter Software oder genutzten Komponenten.

3 Inhalte der Meldungen

Meldung	Mindestinhalte
Erstmeldung (24 Stunden)	Meldende Person mit Erreichbarkeit Zeitpunkt der Feststellung und des Ereignisses, soweit bekannt Betroffener Einzelauftrag und betroffene Leistungen Beschreibung des Ereignisses Betroffene Informationen, Systeme, Konten oder Geräte Verdacht auf rechtswidrige oder böswillige Handlung Bereits ergriffene Sofortmaßnahmen
Folgemeldung (72 Stunden)	Aktualisierung der Erstmeldung Bewertung von Schweregrad und Auswirkungen Kompromittierungsindikatoren, soweit vorhanden Ergriffene und geplante Maßnahmen
Abschlussbericht (ein Monat nach Folgemeldung)	Ursache Tatsächliche Auswirkungen Ergriffene Abhilfemaßnahmen Maßnahmen gegen eine Wiederholung