BESONDERE VERTRAGSBESTIMMUNGEN

FÜR IT-BEZOGENE LEISTUNGEN UND DATENSCHUTZ

der

VAMED-KMB Krankenhausmanagement und Betriebsführungsges.m.b.H.
Spitalgasse 23, 1090 Wien,
(FN 33504x Handelsgericht Wien)

1. GELTUNGSBEREICH

Diese Besonderen Vertragsbestimmungen regeln die besonderen technischen, rechtlichen und organisatorischen Bedingungen für IT-bezogene Leistungen, um sicherzustellen, dass die VAMED-KMB IT-Sicherheitsrichtlinien und Regelungen zur Informationssicherheit eingehalten werden. Diese Bestimmungen umschließen auch die Lieferung von Soft- und Hardware, samt Lizenzierungen und Dienstleistungen, wie Beratungsleistungen, Programmierleistungen sowie Instandhaltungsleistungen vor Ort oder im Wege von „Fernwartungen".

Diese Bestimmungen legen für sämtliche Lieferungen und Leistungen, die VAMED-KMB zukauft, die Verpflichtungen der Auftragnehmer in Zusammenhang mit dem Datenschutz fest.

Diese Besonderen Vertragsbestimmungen gelten ergänzend zu den jeweils gültigen

- „Allgemeinen Vertragsbestimmungen für Leistungen" (0069).

Sollten in Ausnahmefällen überwiegend Bauleistungen zu erbringen sein, gelten die gegenständlichen Vertragsbestimmungen ergänzend zu den jeweils gültigen

- „Allgemeinen Vertragsbestimmungen für Bauleistungen" (0070).

In diesem Fall wird im Rahmen der Anfrage bzw. Bestellung gesondert darauf hingewiesen.

Die jeweils gültigen Versionen sind auf unserer Homepage unter: https://www.vamed.com/de/footer/wichtige-links/wichtige-unterlagen/ zu finden.

INHALTSVERZEICHNIS

Begriffsbestimmungen

ABGB	Allgemeines bürgerliches Gesetzbuch
AG	Auftraggeber
AKH-Wien	Stadt Wien, Wiener Krankenanstaltenverbund, Allgemeines Krankenhaus der Stadt Wien - Medizinischer Universitätscampus
AN	Auftragnehmer
Anfrage	Überbegriff für alle Formen der Angebotseinholung
bzw	beziehungsweise
dh	das heißt
DSG	Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG) gemäß BGBl 2017/120 (Datenschutz-Anpassungsgesetz 2018) in der jeweils geltenden Fassung
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG ("EU Datenschutz-Grundverordnung")
EU	Europäischen Union
etc.	et cetera
ges.m.b.H.	Gesellschaft mit beschränkter Haftung
IT	Informationstechnik
KAV	Stadt Wien, Wiener Krankenanstaltenverbund
MBit/S	Megabit pro Sekunde
Nr.	Nummer
Pkt.	Punkt
QM	Qualitätsmanagement
USt.	Umsatzsteuer
VKMB	VAMED-KMB
VAMED-KMB	VAMED Krankenhausmanagement und Betriebsführungsges.m.b.H.
zB	zum Beispiel

2. DATENVERARBEITUNG UND DATENSCHUTZ

Besteht die Leistungserbringung des AN (Vertragsgegenstand) auch in einer Datenverarbeitung, so ist verpflichtend ein „DATENSCHUTZVERTRAG“ unter Angabe folgender Informationen zu schließen:

a) Verarbeitete Datenkategorien, einschließlich der Information über die Verarbeitung besonderer Kategorien personenbezogener oder strafrechtlich relevante Daten

b) Zweck der Datenverarbeitung

c) Dauer der Datenverarbeitung

d) Gegebenenfalls: von AN genutzte IT-Systeme des AG (Punkt 4 unten)

Der AN ist im Zusammenhang mit jeder Verarbeitung von Daten des AG bzw. die dem AG zurechenbar sind, insbesondere verpflichtet,

a) die personenbezogenen Daten nur nach schriftlicher Weisung des AG zu verarbeiten und an Dritte zu übermitteln;

b) nur Personen zur Verarbeitung personenbezogener Daten einzusetzen, die zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

c) geeignete technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO zu ergreifen;

d) Subauftragnehmer nur nach vorheriger schriftlicher Genehmigung des AG hinzuzuziehen und diesem dieselben Datenschutzpflichten vertraglich aufzuerlegen, die auch den AN treffen. Der AN haftet gegenüber dem AG für die Einhaltung der Pflichten des Subauftragnehmers;

e) den AG bei der Beantwortung von Anfragen im Zusammenhang mit der Wahrnehmung der Rechte Betroffener mit geeigneten technischen und organisatorischen Maßnahmen zu unterstützen;

f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den AG bei der Einhaltung der Pflichten in Bezug auf die Meldung von Datenschutzverletzungen und die Datenschutzfolgeabschätzung nach den Artikeln 32 bis 36 DSGVO zu unterstützen. Dabei hat er den AG ehestmöglich, spätestens innerhalb von 24 Stunden, über (mögliche) Datenschutzverletzungen zu informieren;

g) nach Beendigung des Vertrages alle personenbezogenen Daten nach Wahl des AG entweder zu löschen oder zurückzugeben, sofern nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht;

h) dem AG alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Punkt niedergelegten Pflichten zur Verfügung zu stellen und Überprüfungen, inklusive Inspektionen vor Ort, die vom AG oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, zu ermöglichen und dabei zu unterstützen; sowie

i) alle sonstigen maßgeblichen Bestimmungen nach der DSGVO und nationaler Begleitgesetzgebung einzuhalten und den Schutz der Rechte der betroffenen Person sicherzustellen.

Insgesamt ist der AN verpflichtet, das Datengeheimnis im Sinne des § 6 DSG zu wahren und den AG bei jeder Verletzung dieser Verpflichtung schad- und klaglos zu halten. Der AN stimmt seinerseits ausdrücklich zu, dass seine persönlichen Daten, wie insbesondere Name, Geburtsdatum- und Ort, Kontaktdaten, Funktionsbezeichnungen, die er dem AG bekannt gibt, zum Zweck der Umsetzung der jeweiligen Liefer- und/oder Leistungsvereinbarung, also etwa für Bestellungen bzw. Abrufe, deren Umsetzung und Verrechnung, für Abstimmungen über den Bestand der Vereinbarung und/oder der Bestellungen bzw. Abrufe oder der Bedeutung ihrer Regelungen und für Auskünfte an Mitarbeiter, Kunden, begleitende Prüfer, Berater des AG, Gerichte oder Behörden beim AG verarbeitet, auch an die genannten Personen und Institutionen weitergegeben werden. Der AN holt die entsprechende Zustimmung seiner Mitarbeiter und Subunternehmer dazu ein und stellt sicher, dass seine Mitarbeiter und Subunternehmer eine entsprechende ausdrückliche Zustimmung abgeben und dabei auch

insbesondere zustimmen, dass sämtliche persönlichen Daten, die der AN dem AG weitergibt oder die der AG vom Mitarbeiter oder Dritten erhält, wie insbesondere aber nicht nur Name, frühere Namen, Namensteile, Geburtsdatum, Adress- und Kontaktdaten, Berufliche Qualifikation und Referenzen samt Zeugnisse und Bestätigungen darüber sowie über Gewissenhaftigkeit und Verlässlichkeit, Lichtbild des Betroffenen (etwa für Ausweiskarten) zur Umsetzung der Vereinbarung des AN beim AG verarbeitet und/oder auch weitergegeben werden

3. NUTZUNG VON IT-SYSTEMEN DES AG

Sofern die Leistungserbringung durch den AN (Vertragsgegenstand) die Anmeldung zu den Kommunikations- und/oder sonstige IT-Netzwerken des AG (gemeinsam mit den entsprechenden Komponenten sowie der Infrastruktur „IT-Systeme des AG“ genannt) oder die Nutzung derselben erfordert, sind die von der Leistungserbringung betroffenen IT-Systeme in einem gesondert abzuschließenden Datenschutzvertrag detailliert festzuhalten.

Dafür hat der AN zumindest 14 Arbeitstage vor Leistungsbeginn mit dem genannten Ansprechpartner des AG und mit Bezug zum erteilten Auftrag (Bestellnummer) die betroffenen IT-Systeme des AG in folgender Struktur bekanntzugeben:

a) Systeme, auf die zugegriffen werden soll

b) Softwareprodukte, die der Wartung und Instandsetzung unterliegen

c) Softwareprodukte, die dabei eingesetzt werden

d) Umfang, Art und Zweck der Leistungen (Fehlerbehebung, Störfalldefinition, Updates, Patches)

e) Umfang der Zugriffe (Dateien, Verzeichnisse, schreibender oder lesender Zugriff)

f) personenbezogenen Daten oder aus den erhaltenen Daten gewonnene personenbezogene Daten (zusammen die "Auftraggeber-Daten"), die vom Zugriff betroffen sein können

g) Vom Zugriff ausgenommene Systeme und Softwareprodukte

h) Kreis der Betroffenen

Die Anmeldung zu den IT-Systemen des AG und die Nutzung derselben darf nur mit vom AG ausdrücklich genehmigter Hard- und Software erfolgen. Dabei sind sämtliche Sicherheitsvorgaben des AG (z.B. Beschränkung der Hardware, Passwort) einzuhalten.

Insofern mit dem Zugriff eine Verarbeitung von Daten des AG, insbesondere auch personenbezogener Daten von Mitarbeitern, Kunden oder anderen, umfasst ist, ist Punkt 3 anzuwenden.

3.1 Datenschutzvertrag mit dem Wiener Krankenanstaltenverbund

Voraussetzung für das Zustandekommen eines Vertrages für Leistungen, die im AKH Wien erbracht werden (auch als Subunternehmerleistungen), ist das Bestehen oder der Abschluss eines Datenschutzvertrages mit dem Wiener Krankenanstaltenverbund. Sollte bereits ein Datenschutzvertrag abgeschlossen sein, ist vom AN auch zu überprüfen, ob der gegenständliche Leistungsumfang vom bestehenden Datenschutzvertrag umschlossen ist und ist im Abweichungsfall ein erweiterter Neuabschluss durchzuführen.

Als Ansprechpartner für den Abschluss von Datenschutzverträgen steht

AKH/DTI - Technologie und Informatik - Sicherheit, Datenschutz und Qualitätsmanagement

Herr Mag. Neumann

Tel. Nr.: +43 1 40400 50170

Fax. Nr.: +43 1 40495 11605

E-Mail: markus.neumann@akhwien.at

zur Verfügung.

4. NUTZUNGSRECHTE / LIZENZREGELUNGEN

Der AG erhält das ausschließliche, unwiderrufliche, zeitlich, örtlich und inhaltlich unbeschränkte und übertragbare Nutzungsrecht an sämtlichen im Rahmen der Leistungserbringung erfolgten Arbeitsergebnissen. Dieses umfasst jedenfalls auch das Recht zur Bearbeitung und zur vollständigen oder teilweisen Veröffentlichung, Vervielfältigung und sonstigen Verwertung der Arbeitsergebnisse. für Individualsoftware

Für individuell für den AG entwickelte/customized Software räumt der AN dem AG ein ausschließliches, unwiderrufliches, zeitlich, örtlich und inhaltlich unbeschränktes sowie übertragbares (Sublizenz) Lizenz-/Nutzungsrecht ein. Dieses umfasst jedenfalls auch das Recht zur Bearbeitung, zur vollständigen oder teilweisen Veröffentlichung, Vervielfältigung und sonstigen Verwertung einschließlich der Weiterübertragung an Dritte ein.

Der AN räumt dem AG und Unternehmen der VAMED-Gruppe für die Anzahl bzw. den Umfang der erworbenen Standardsoftwarelizenzen ein nicht ausschließliches, unbefristetes und räumlich unbeschränktes Nutzungsrecht ein.

Wird Software zur Verfügung gestellt bzw. lizensiert, deren Lizenzinhaber ein Dritter ist (z.B. Standardsoftware von Microsoft), so erlangen diese Lizenzbestimmungen nur dann Gültigkeit, wenn diese vom AG im Rahmen der Beauftragung ausdrücklich akzeptiert werden. Sofern die Lizenzbestimmungen des Lizenzinhabers vom AG nicht ausdrücklich schriftlich akzeptiert wurden, kommen die Regelungen dieses Punktes 5 zur Anwendung.

Der AN wird beim Einsatz von Subunternehmern sicherstellen, dass der AG auch an allfälligen Leistungen des Subunternehmers die vorstehend genannten Rechte exklusiv erwirbt.

Die Gewährung der vor genannten Rechte ist mit dem Entgelt, das der AN für seine Leistungen erhält, abgegolten.

5. QUALIFIKATION, DOKUMENTATION, TRAINING, BERICHTERSTATTUNG

Der AN setzt für die Vertragserfüllung nur sorgfältig ausgewählte und nachweislich qualifizierte Mitarbeiter ein. Auf Verlangen gibt der AN schriftlich Name und Funktion der verantwortlichen Mitarbeiter bekannt. Der AN ist verpflichtet, auf Verlangen des AG unverzüglich Mitarbeiter, welche nicht über die erforderlichen Fachkenntnisse verfügen oder die Vertragserfüllung beeinträchtigen, von der Leistungserbringung abzuziehen und durch geeignet qualifizierte Mitarbeiter zu ersetzen.

Der AN liefert eine für den Betrieb vollständige, kopierbare Dokumentation in elektronischer Form (z.B. Handbuch, Manual), auf Wunsch auch in ausgedruckter bzw. gebundener Form. Der AG ist berechtigt, die Dokumentation für den vertragsgemäßen, beauftragten Gebrauch zu vervielfältigen und zu verwenden.

Der AN verpflichtet sich, über seine Arbeit, die seiner Mitarbeiter und von ihm beauftragter Dritter, dem Arbeitsfortschritt entsprechend dem AG regelmäßig, zumindest monatlich bzw. sofern von gewünscht auch in kürzeren Intervallen, Bericht zu erstatten. Nach Beendigung der Leistungserbringung wird der AN im Falle der Erbringung von Beratungsleistungen jedenfalls, bei jeder anderen Leistungserbringung auf unseren ausdrücklichen Wunsch hin, einen Abschlussbericht übergeben.

6. SOFTWARE- UND LÖSUNGSIMPLEMENTIERUNG

Software- bzw. Lösungsimplementierungen sowie die zugehörigen Leistungen gelten als Werk im Sinne der §§ 1165 ABGB ff.

7. WARTUNG

7.1 Standardsoftware

Der AG hat das Recht auf eigenen Wunsch einen gesonderten Wartungsvertrag abzuschließen, der innerhalb einer Frist von zwei Jahren ab Übernahme der Gesamtleistung auch die kostenlose Zurverfügungstellung aller nachfolgenden Programmversionen, welche eine Fehlerkorrektur enthalten (Updates), beinhaltet.

Sofern kein gesonderter Wartungsvertrag mit dem AN abgeschlossen wird, gelten die Bestimmungen in Punkt 9. auch für Standardsoftware.

7.2 Individualsoftware

Der AN verpflichtet sich eine Softwarewartung anzubieten, welche neben Punkt 8.2.2, die Behebung von Fehlern der Software die - sofern im Einzelfall nicht anders festgelegt - innerhalb einer Frist von zwei Jahren ab Übernahme der Gesamtleistung auftreten, umfasst. Sofern nicht ausdrücklich anders vereinbart (Position Leistungsverzeichnis), sind die Kosten für die Wartung bereits mit dem im Vertrag vereinbarten Entgelt, abgegolten.

Der AN verpflichtet sich dem AG innerhalb einer Frist von zwei Jahren ab Übernahme der Gesamtleistung alle nachfolgenden Programmversionen, welche eine Fehlerkorrektur enthalten (Updates), kostenlos zur Verfügung zu stellen.

AG und AN vereinbaren die unten angeführten Fehlerklassen für die Klassifikation von Fehlern der Software und der Programmierungen:

Klasse 1 – Kritisch

Die Nutzung der Softwarelösung ist nicht möglich oder unzumutbar eingeschränkt. Der Fehler hat schwerwiegenden Einfluss auf wesentliche Funktionen und/oder die Sicherheit der Softwarelösung bzw. sonstiger Systeme des AG; die Softwarelösung kann nicht weiterverwendet werden.

Klasse 2 – Schwer

Die zweckmäßige Nutzung der Softwarelösung ist ernstlich eingeschränkt. Der Fehler hat wesentlichen Einfluss auf die Funktion und/oder die Sicherheit der Softwarelösung bzw. der IT-Systeme des AG, lässt aber eine Weiterverwendung der Softwarelösung mit größeren Einschränkungen zu.

Klasse 3 – Leicht

Die zweckmäßige Nutzung der Softwarelösung ist leicht eingeschränkt. Der Fehler hat unwesentlichen Einfluss auf die Funktionalität und/oder die Sicherheit der Softwarelösung bzw. der IT-Systeme des AG und lässt eine weitere Verwendung der Softwarelösung mit nur geringen Einschränkungen zu.

Klasse 4 – Unerheblich

Die zweckmäßige Nutzung der Softwarelösung ist ohne Einschränkung möglich. Der Fehler hat keinen oder nur unerheblichen Einfluss auf die Funktionalität und/oder die Sicherheit der Softwarelösung bzw. der IT-Systeme des AG. Die Nutzung der Softwarelösung bleibt uneingeschränkt möglich.

Die Zuordnung zu den Fehlerklassen erfolgt einvernehmlich. Im Zweifelsfall hat der AN auch davor zunächst Maßnahmen auf Basis der Klassifizierung des AG zu setzen, um allfällige Nachteile für den AG zu vermeiden.

Der AN verpflichtet sich, eine Telefonnummer (Hotline) und Support-E-Mail-Adresse bereitzustellen, bei der die Störungen und Probleme mit der Software gemeldet und Auskünfte eingeholt werden können.

Der AN verpflichtet sich die Behebung von Fehlern der Klasse 3 und Klasse 4 in angemessener Zeit zu beginnen. Im Falle von Fehlern der Klasse 1 und Klasse 2 verpflichtet sich der AN unverzüglich mit der Behebung des Fehlers zu beginnen und diese erst nach erfolgreicher Behebung zu beenden.

8. INSTANDHALTUNGSLEISTUNGEN AN IT-SYSTEMEN DES AG

Der AN hat alle erforderlichen Wartungs- und Instandsetzungsarbeiten an IT-Systemen des AG - die auch Teil einer (übergeordneten) Gesamtanlage (zB Steuerung einer Aufzugsanlage) sein können - durchzuführen, um die Funktionsfähigkeit der IT-Systeme und Anlagen in der Verantwortung des AG sicher zu stellen.

Sofern nicht ausdrücklich anders vereinbart, erfolgen die Wartungs- und Instandsetzungsleistungen grundsätzlich im Zeitraum von Montag bis Freitag,7:00–17:00 Uhr. Bei kritischen und/oder schweren Fehlern – Klasse 1 und Klasse 2 – erfolgt die Wartung binnen 2 Stunden ab Kenntnis oder Verständigung durch den AG. Der AN wird den AG vom Beginn der Instandsetzungsarbeiten verständigen und diese schnellst möglich durchführen. Sofern die Fehlerbehebung, unabhängig von der Fehlerklasse, nicht innerhalb von 12 Stunden möglich sein sollte, wird der AN dem AG dies binnen 24 Stunden unter Angabe von Gründen sowie des Zeitraums, der für die Fehlerbeseitigung voraussichtlich zu veranschlagen ist, schriftlich mitteilen. Der AN wird alle Mittel einsetzen, um dem AG eine Interimslösung bereitzustellen.

Der AN hat sicherzustellen, dass eine (Wieder-) Inbetriebnahme der IT-Systeme und Anlagen (z.B. nach einem Stromausfall) jederzeit und ohne spezielle Hilfsmittel wie Passwort, Zutrittscode uneingeschränkt möglich ist.

Der AN muss die laufende Soft- und Hardwarewartung im Sinne von erforderlichen Softwareupdates und Hardwareanpassungen durchführen. Insbesondere muss der AN das zugrundeliegende Betriebssystem bzw. die IT-Systeme des AG vor Sicherheitslücken schützen und dieses regelmäßig und unaufgefordert patchen. Der AG scannt seine IT-Systeme laufend auf Sicherheitslücken. Sollten im Zuge dieser Sicherheitsscans Systemlücken an Systemen in der Verantwortung des AN festgestellt werden, so hat der AN auf erste Aufforderung des AG diese Lücken unverzüglich zu schließen.

Softwareänderungen sind dem AG zeitgerecht anzukündigen. Vor Durchführung der Änderungen der Software ist jedenfalls das Einvernehmen mit den AG über Inhalt und Zeitpunkt jeder Änderung herzustellen. Der AG erhält vom AN die gesamte geänderte Technische Dokumentation (Schnittstellen, Beschreibungen, Serviceunterlagen, falls erforderlich, Parametrierungen und Servicecodes von AG-spezifischen Änderungen). Darüber hinaus ist das technische Personal des AG vom AN so einzuweisen, dass sie ihre Aufgaben im Rahmen der Technischen Betriebsführung vollständig erfüllen können.

Bei einer dadurch notwendigen Änderung in der Softwarelandschaft des AG (Anpassung von Schnittstellen etc), hat der AN zeitgerecht (spätestens 6 Monate vor dem geplanten Update) die erforderlichen Adaptierungen bekanntzugeben. Der notwendige Aufwand für eine Softwareanpassung im Bereich des AG ist vom AN zu tragen. Der AN dokumentiert nach Abschluss der Adaptierung den

jeweiligen Softwarestatus im Detail (Übermittlung Änderungsversionen zur Bedienungsanleitungen, zur Technischen Dokumentation etc) und garantiert eine gegebenenfalls geforderte Netzwerkfähigkeit der gewarteten Anlagen, soweit diese Anlagen in ein Netzwerk eingebunden sind. Der dafür notwendige Aufwand ist vom AN zu tragen.

Aus Sicht des AN erforderliche IT-bezogene Hardwareänderungen sind dem AG zeitgerecht anzukündigen. Vor Änderungen der Hardware ist das Einvernehmen mit dem AG über Inhalt und Zeitpunkt jeder Änderung herzustellen. Der AG erhält vom AN die gesamte geänderte Dokumentation (Schnittstellen, Beschreibungen, Serviceunterlagen). Darüber hinaus ist das technische Personal des AG vom AN so einzuweisen, dass sie ihre Aufgaben im Rahmen der Technischen Betriebsführung vollständig erfüllen können. Der AN dokumentiert nach Leistungsabschluss den jeweiligen Hardwarestatus im Detail (Übermittlung Änderungsversionen zur Bedienungsanleitungen, zur Technischen Dokumentation etc). Der dafür notwendige Aufwand ist vom AN zu tragen.

9. TECHNISCHE UND ORGANISATORISCHE SICHERHEITSMASSNAHMEN

Der AN sichert zu, dass er angemessene technische und organisatorische Maßnahmen getroffen hat, sodass die Verarbeitung im Einklang mit den in dem Vertrag, den Weisungen, den gesetzlichen Bestimmungen (insbesondere des Unionsrechts und nationalen Rechts) genannten Sicherheitsanforderungen und sonstigen Anforderungen erfolgt. Insbesondere sind nachfolgende Maßnahmen zu setzen. Diese sind anzupassen, sofern sich die üblichen oder technischen oder organisatorischen Maßnahmen während der Laufzeit des Vertrages ändern.

Der AN muss sicherstellen, dass der technische Arbeitsplatz, über den der (Fern-)Zugriff stattfindet, regelmäßig und anlassbezogen Sicherheitsupdates unterzogen wird.

Vor jedem Zugriff durch den AN hat dieser eigenständig eine Daten- und Systemsicherung vorzunehmen damit im Fall einer nicht funktionierenden Lösung ein Fallback jederzeit möglich ist.

Der AN darf keine Auftraggeber-Daten in Privathäusern verarbeiten. Auch die Bereitstellung von Zugangsberechtigungen für seine Mitarbeiter, die die Verarbeitung von Auftraggeber-Daten in Privathäusern (zB Telearbeit) ermöglichen, sowie die Verarbeitung auf privaten Geräten der Mitarbeiter ist untersagt.

Benötigt der AN Zutritt zu entsprechend gesicherten und exponierten Räumlichkeiten, so wird der AN hinsichtlich der für den spezifischen räumlichen Bereich geltenden Verhaltensregeln unterwiesen. Die erfolgte Unterweisung ist zu dokumentieren. Der AN nimmt mit dieser Vereinbarung zur Kenntnis, dass verschiedene Bereiche durch eine Videoüberwachung gesichert sein können und erkennt dies im Sinne des Datenschutzgesetzes an.

9.1 Zugangskontrolle für Fernwartung

Der Zugang zu den Anlagen mittels Fernwartungsverbindung darf nur in Abstimmung mit dem AG erfolgen. Erfolgt der technische Zugang über das VAMED-KMB IT Netzwerk, so hat der Ansprechpartner des AG eine entsprechende Useranforderung bzw. Freischaltung über die VAMED-KMB IT zu beantragen. Der Zugangspunkt bzw. die technische Lösung des Zugangs wird von der VAMED-KMB IT bereitgestellt und ist zeitgerecht im Wege des genannten Ansprechpartners des AG anzufordern. Der AG muss die Fernwartungsarbeiten jederzeit abbrechen können. Soweit der AN daran mitwirken muss, gewährleistet er, dass dies möglich ist.

Nach Abschluss der Fernwartungsarbeiten ist die Fernwartungsverbindung unverzüglich abzubauen.

9.2 Organisation der Datenträgerkontrolle

Der AN darf Daten des AG im Wege eines Filetransfers oder Downloads für Zwecke der Fehleranalyse und -behebung nur dann vom IT-System des AG abziehen und auf sein eigenes kopieren, wenn er dafür zuvor die schriftliche Zustimmung des AG erhalten hat. Der AG darf die Erlaubnis dazu nicht erteilen, wenn der Übertragung besondere Geheimhaltungsregelungen (zB ärztliche Schweigepflicht) entgegenstehen.

Alle Fernwartungsaktivitäten müssen an einem Kontrollbildschirm des AG zum Mitlesen sichtbar gemacht werden, sofern die technische Lösung dies vorsieht.

9.3 Speicherkontrolle

Der AG schützt alle ablauffähigen Programme in seinen IT-Systemen und Anlagen durch geeignete Zugriffsschutzmechanismen, so dass das Fernwartungspersonal nicht unkontrolliert auf Dateien zugreifen kann.

Vor Beginn der Fernwartungsarbeiten muss sich das Fernwartungspersonal mit Benutzerkennung und einer Authentifikation (Passwort) anmelden. Die entsprechenden Benutzerzugangsdaten werden vom AG in geeigneter Form kommuniziert. Die Fernbetreuung von Anwenderprogrammen ist unter einer Kennung ohne Administratorenrechte vorzunehmen.

Der AN darf von den ihm eingeräumten Zugriffsrechten nur in dem für die Durchführung der Fernwartungsarbeiten unbedingt notwendigen Umfang Gebrauch machen.

9.4 Zugriffskontrolle

Die dem AN zur Durchführung der Fernwartungsarbeiten mitgeteilten Passwörter sind regelmäßig zu ändern.

Bei Verlust oder Verdacht auf Kompromittierung des Passworts bzw. Sicherheitstokens ist die für die Freischaltung der Fernwartung zuständige Stelle des AG unverzüglich zu kontaktieren, damit Passwort bzw. Sicherheitstoken gesperrt werden können. Danach kann eine neue Berechtigung angefordert werden.

Für automatisierte Protokolle sind zumindest Angaben zu Usernamen, Zeitpunkt des Einloggens und Ausloggens und je nach Art der Applikation und gemäß dem technischen Stand weitere Inhaltsdaten zu protokollieren.

9.5 Transportkontrolle

Zur Sicherung von Vertraulichkeit, Integrität und Authentizität der übertragenen Auftraggeber-Daten sind die Auftraggeber-Daten auf dem Übertragungsweg zwischen IT-System des AG und Fernwartungszentrale zu verschlüsseln.

9.6 Organisationskontrolle

Die Auftraggeber-Daten, inklusive Vervielfältigungen der Auftraggeber-Daten im Besitz des AN, sind – nach Wahl des AG – unverzüglich datenschutzkonform zu löschen bzw. zu vernichten oder dem AG zurückzugeben, wenn sie für die Durchführung der Leistungen nicht mehr erforderlich sind, und sofern nicht nach Unionsrecht oder nationalem Recht anderes erforderlich ist. Die Rückstände der Datenvernichtung dürfen keine Rekonstruktion der ursprünglich gespeicherten Auftraggeber-Daten ermöglichen. Der AN hat die Löschung oder Zerstörung von Auftraggeber-Daten schriftlich zu dokumentieren und dem AG diese Dokumentation auf Verlangen vorzuweisen (Löschzertifikat). Dies

gilt auch für Vervielfältigungen von Auftraggeber-Daten in allen System des AN sowie für Test- und Ausschussdaten.

Der AG die Einhaltung der getroffenen Sicherheitsmaßnahmen jederzeit und unangekündigt überprüfen.

Der AG ist nach der ISO Norm 27001 zertifiziert und behält sich das Recht vor, entsprechende Audits beim AN durchzuführen.

9.7 Zertifizierung

Die AN belegen diese Maßnahmen durch entsprechende Zertifizierungen.

10. BESONDERE BESTIMMUNGEN FÜR CLOUD SERVICE PROVIDER

10.1 Erfüllung der Prüfkriterien für VAMED-fremde Cloud Services Provider (auch während der Vertragslaufzeit)

Der AN bestätigt, dass die auf dem aktuellen Stand der Technik freigegebenen Anforderungen betreffend „Physikalische Sicherheit“ und „Anforderungen hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität der Datenhaltung“ mit den angebotenen Leistungen erfüllt werden und dass die Anforderungen, die während der Vertragslaufzeit jeweils an den dann aktuellen Stand der Technik dynamisch angepasst werden, zumindest auf gleichbleibendem Standard (Niveau) für den AG erfüllt werden. Entsprechende Prüfungen durch „K-IRM“ der VAMED werden unterstützt und dabei etwaig erkannte Anpassungsmaßnahmen werden zeitnahe umgesetzt.

10.2 Servicezeiten, Reaktions- und Wiederherstellungszeiten

Dazu wird festgelegt, dass die Plattform ganzjährig jeweils Montag bis Sonntag von 0.00h – 24.00h betrieben wird. Als Wiederherstellungszeit (inkl. Reaktionszeit) für Funktion und Datenverfügbarkeit wird – wenn im Vertrag keine andere Festlegung getroffen wurde - ein verbindlicher Zeitraum von 2 Stunden zugesagt. Als Servicezeit, in der eine Abstimmung mit unserem Ansprechpartner erforderlich ist oder eine Bearbeitung vor Ort erforderlich ist wird Montag bis Freitag jeweils 7.00h – 16.00h festgelegt.

Als garantierte Mindestverfügbarkeit wird – wenn im Vertrag keine andere Festlegung getroffen wurde - mit 99,5 % festgelegt.

10.3 Schadensersatzregelungen (Pönalen)

Für die eine Nichterreichung der vor angeführten Performance bzw. Service Levels wird – wenn im Vertrag keine andere Festlegung getroffen wurde - folgende Pönalregelung vorgesehen:

Pönale für Überschreitung der Wiederherstellungszeit (inkl. Reaktionszeit): EUR 500,00, exkl. USt. je angefangener Stunde, maximal jedoch EUR 5.000,00, exkl. USt. je Anlassfall.

Pönale für Unterschreitung der Verfügbarkeit: 10 % der Wartungsgebühr je [1] % der Unterschreitung der Mindestverfügbarkeit

10.4 Bandbreiten für Up- und Download

Dazu wird, abhängig von der Performance der Internetverbindung des AG – folgendes festgelegt:

Mindest-Upload-Rate: [10] MBit/S

Mindest-Download-Rate: [50] MBit/S

10.5 Migrationsregelungen bei Bestandsdaten

Für ein einfaches Hochladen von vorhandenen Bestandsdaten ist eine entsprechende Funktion vorzusehen. Dieser Upload kann entweder durch einen User seitens des AG selbst vorgenommen werden, der AN wird den AG dabei unterstützen; alternativ übernimmt das Service-Team des AN diese Aufgabe als Dienstleistung.

10.6 Regelungen für den Fall der Insolvenz des Service Providers

Im Falle der Einleitung eines Insolvenzverfahrens beim AN – auch bei eingeleiteten Sanierungsverfahren – hat der AN dem AG innerhalb einer Frist von zwei Kalenderwochen eine Kopie aller gespeicherten Daten in allgemein lesbaren Formaten, welche die referentielle Integrität erhalten, zu übergeben, sodass eine weitere lokale Bearbeitung mittels lokal installierbaren Versionen (Viewer) und eine einfache Migration der Daten auf andere Plattformen sichergestellt sind.

10.7 Exportmöglichkeit in allgemein lesbare Formate welche die referentielle Integrität erhalten / Möglichkeiten zum Umstieg auf lokal installierbare Versionen (Viewer)

Der AN hat dem AG nach Aufforderung – innerhalb einer Frist von zwei Kalenderwochen - eine Kopie aller gespeicherten Daten in allgemein lesbaren Formaten, welche die referentielle Integrität erhalten, zu übergeben, sodass eine weitere lokale Bearbeitung mittels lokal installierbaren Versionen (Viewer) und eine einfache Migration der Daten auf andere Plattformen sichergestellt sind.

10.8 Datenrückgabe und -bereitstellung nach Vertragsauflösung / Datenlöschung auf Anforderung

Nach Beendigung des Vertrages ist mit Vertragsende eine Kopie aller gespeicherten Daten an den AG in allgemein lesbaren Formaten, welche die referentielle Integrität erhalten, zu übergeben, sodass eine weitere lokale Bearbeitung mittels lokal installierbaren Versionen (Viewer) und eine einfache Migration der Daten auf andere Plattformen sichergestellt sind.

Alle Daten des AG sind nach Übernahmebestätigung gesichert zu löschen.

Über die erfolgte Löschung ist eine schriftliche Bestätigung (Zertifikat) zu erstellen mit der garantiert wird, dass alle Daten nach einem zum Zeitpunkt entsprechenden europäischen Standard restlos gelöscht wurden. Zu diesem Vorgang bzw. zur Nachweisführung ist im Anlassfall das Einvernehmen mit dem zuständigen IT-Verantwortlichen herzustellen.

10.9 Ort der Datenspeicherung bzw. Betriebsführung (Begrenzung auf EU Raum)

Die gegenseitig gesicherten Rechenzentren des AN befinden sich in an zwei räumlich getrennten und gesicherten Standorten innerhalb des EU-Raumes.

10.10 Kontrollrechte des AG bzw. Duldungs- und Mitwirkungspflichten des AN, Möglichkeit einer Rechenzentrumsbegehung, Recht auf Audits

Der AN sichert dem AG entsprechende Kontrollrechte zu. Dazu zählen insbesondere die Möglichkeit einer Rechenzentrumsbegehung und das Recht auf Audits – nach Terminvereinbarung. Der AN verpflichtet sich zur entsprechenden Mitwirkung.

10.11 Besondere Anforderungen an Subunternehmer

Die vom AN eingesetzten Subunternehmer sind zu nennen (siehe diesbezügliche allgemeine Bestimmungen). Darüber hinaus haben die vom AN zur Leistungserbringung eingesetzten Subunternehmen den Anforderungen ISO/IEC 27001 zu entsprechen.

10.12 Technische Anforderungen und Integrationsfähigkeit

Um die Cloud-Lösung zu nutzen, muss der AG keine Software installieren, der AG benötigt lediglich einen Internet-Browser.

10.13 Anpassungen des Cloud Services an die Veränderungen des Stands der Technik

Der AN wird seine Technologien stets auf dem aktuellsten Stand der Technik halten.

10.14 Backupzyklen und Datenaufbewahrungsfristen

Der AN sichert die komplette Datenbank durch tägliche inkrementelle Sicherungen, sowie – wenn im Vertrag keine andere Festlegung getroffen wurde - wöchentliche Vollbackups.

Sämtliche Backups werden komplett in beiden Rechenzentren abgelegt und dort jeweils bis zu – wenn im Vertrag keine andere Festlegung getroffen wurde - 6 Monate vorgehalten.

Ein Restore-Test pro Release-Zyklus (entspricht im Normalfall 14 Tage, im Ausnahmefall 21 Tage) stellt die Funktionsfähigkeit der Backups sicher.

Das verteilte Dateisystem der Produktivplattform wird – wenn im Vertrag keine andere Festlegung getroffen wurde - mit maximal 24 Stunden Nachlauf in ein logisch und physisch getrenntes, ebenfalls über beide Standorte verteilt arbeitendes, redundantes Speichersystem gesichert.

10.15 Schulungsmöglichkeiten und Betriebs- sowie Benutzerhandbücher

Der AG kann jederzeit Schulungen beim AN abrufen, die Konditionen hierzu sind vor Vertragsabschluss vom AN anzubieten und einvernehmlich festzulegen.

Benutzerhandbücher und Guides zur Nutzung der Plattform sind in aktueller Form zur Verfügung zu stellen.

Das Support-Team des AN steht jedenfalls innerhalb der üblichen Büroarbeitszeiten zur Verfügung und ist telefonisch oder über Email erreichbar.

10.16 Informationspflichten bei Versionsänderungen

Die aktuellen Informationen über die geplanten und durchgeführten Wartungsarbeiten und Releases finden sich auf der Startseite des AN.

11. BESONDERE BESTIMMUNGEN FÜR SUBUNTERNEHMER

Setzt der AN seinerseits Subunternehmer ein, ist er verpflichtet sicherzustellen, dass der Subunternehmer schriftlich zur Einhaltung zumindest der Bedingungen aus diesem Vertrag, dem Unionsrecht und nationalen Recht verpflichtet hat.

Der AN hat Überwachungspflichten gegenüber dem Subunternehmernehmer, die den Überwachungspflichten des Auftraggebers gleichen. Daher hat der AN regelmäßig (dh zumindest einmal im Jahr) die Einhaltung der vertraglichen Verpflichtungen durch den Subunternehmer zu überprüfen.

12. MELDUNG VON DATENSICHERHEITSVORFÄLLEN

Der AN informiert den AG unverzüglich, wenn er oder eine bei ihm beschäftigte Person gegen Vorschriften zum Schutz personenbezogener Daten, gegen Bestimmungen nach diesem Vertrag oder gegen eine vom AG erteilte Weisung verstoßen hat, wenn Anhaltspunkte dafür bestehen, dass ein Dritter – egal aus welchem Grund – unrechtmäßig Kenntnis von Auftraggeber-Daten erlangt haben könnte, oder wenn in sonstiger Weise eine Gefährdung für die Integrität oder Vertraulichkeit der Auftraggeber-Daten eingetreten ist ("Datensicherheitsvorfall").

Die Information über den Datensicherheitsvorfall hat Angaben über den Zeitpunkt und die Art des Vorfalls (einschließlich einer Information, welche Auftraggeber-Daten wie betroffen sind), das betroffene IT-System, die betroffenen Personen, den Zeitpunkt der Entdeckung, alle denkbaren nachteiligen Folgen des Datensicherheitsvorfalls sowie die vom AN daraufhin ergriffenen Maßnahmen zu enthalten.

Eine erste Information des AG hat unverzüglich, spätestens jedoch innerhalb von 2 Stunden nach Kenntniserlangung von dem Datensicherheitsvorfall, zu erfolgen. Eine weitere, detaillierte Unterrichtung des AG, die sämtliche Informationen gemäß Pkt 0 enthalten muss, hat innerhalb von sieben Kalendertagen nach Kenntniserlangung vom Datensicherheitsvorfall zu erfolgen.

Der AN ist verpflichtet, den AG im Falle eines Datensicherheitsvorfalls bei seinen diesbezüglichen Aufklärungs-, Abhilfe- und Informationsmaßnahmen, einschließlich aller Handlungen zur Erfüllung gesetzlicher Verpflichtungen (etwa nach § 24 DSG 2000 oder Unionsrecht) auf erstes Anfordern zu unterstützen. Der AN wird insbesondere unverzüglich sämtliche zumutbaren Maßnahmen ergreifen, um die entstandenen Gefährdungen für die Integrität oder Vertraulichkeit der Auftraggeber-Daten zu minimieren und zu beseitigen, die Auftraggeber-Daten zu sichern und mögliche nachteilige Folgen für Betroffene zu verhindern oder ihre Auswirkungen so weit wie möglich zu begrenzen.

Diese Bestimmungen stellen eine Vertragsgrundlage dar und sind vor Auftragserteilung rechtgültige zu unterfertigen, falls kein gesonderter Datenschutzvertrag abzuschließen ist.

Für den Auftragnehmer: NAME, Unterschrift

_____

Datum