



VERGABEUNTERLAGEN

20261023

Security Managed Services

Verhandlungsverfahren mit Teilnahmewettbewerb (EU) (VgV)

Teilnahmewettbewerb (Korrektur)

AUFTRAGGEBER

Universitätsklinikum Frankfurt

Theodor-Stern-Kai 7, 60590 Frankfurt am Main, Deutschland

22.09.2026

Inhaltsverzeichnis

Teilnahmeunterlagen.....	1
Veröffentlichungstexte Teilnahmewettbewerb.....	1
.....	4
Anlage-Bewerbungsbedingungen EU.pdf	4
Anlage-D Datenschutzerklärung.pdf	6
Anlage-D1_ Leistungsverzeichnis final	9
1. Einleitung.....	13
1.1 Auftraggeber und KRITIS-Kontext.....	13
1.2 Ziel der Beschaffung	13
2. Ist-Zustand	15
2.1 Mengengerüst	15
2.2 Bestehende Komponenten je Leistungsbereich.....	16
2.3 Datengrundlage und Kalkulationsbasis	16
3. Allgemeine Anforderungen.....	18
3.1 Datenhoheit und Datenhaltung.....	18
3.2 Lizenzhoheit (BYOL)	19
3.3 Klinischer Sonderkontext und Patientensicherheit	19
3.4 Anonymisierung klinischer Protokolldaten.....	19
3.5 Flexibles Onboarding und Erweiterbarkeit	20
3.6 Herstelleroffenheit	20
3.7 Bidirektionale ServiceNow-Integration als gemeinsam getragene Leistung	20
3.8 Sprache und Service Delivery	20
4. Leistungsbereich SOC / SIEM.....	21
4.1 Geltungsbereich und Datenquellen	21
4.2 Datenaufnahme, Parsing und Anreicherung	21
4.3 Use Cases, Detection Engineering und Threat Intelligence.....	22
4.4 Alarmierung und Analysetiefe	23
4.5 Plattformbetrieb, Plattformensicherheit und Zugriff	23
4.6 Integration mit den übrigen Leistungsbereichen	24
4.7 Beitrag zum SzA-Nachweis.....	24
5. Leistungsbereich NDR	25
5.1 Geltungsbereich und Zielbild.....	25
5.2 Sensorik und Erfassung	25
5.3 Detektion und Analysefähigkeiten	25
5.4 Datenhaltung und Investigation-Fähigkeit	26
5.5 Plattform- und Lizenzmodell.....	26
5.6 Integration in SIEM und Reaktionsfähigkeit	26
6. Leistungsbereich Vulnerability Management.....	28
6.1 Geltungsbereich und Zielbild.....	28

6.2 Plattform- und Lizenzmodell	28
6.3 Scanning, Discovery und Datenerhebung	28
6.4 Triage, Kontextpriorisierung und Handlungsempfehlungen	29
6.5 Remediation-Tracking, Validierung und Risikoakzeptanz	29
6.6 Integration und Reporting	30
7. Leistungsbereich EDR-Management	31
7.1 Geltungsbereich	31
7.2 Plattform- und Lizenzmodell	31
7.3 Anforderungen an den Betrieb und die Serviceintegration	32
7.4 Agentenbetrieb und Health Monitoring	33
7.5 Policy- und Konfigurationsmanagement	33
7.6 Response- und Containment-Maßnahmen	33
7.7 Integration in SIEM und XDR-Optionen	34
8. Leistungsbereich IoMT-Security	35
8.1 Geltungsbereich und Grundprinzipien	35
8.2 Passive Erkennung und Asset Discovery	35
8.3 Kommunikationsanalyse und Anomalieerkennung	35
8.4 Risiko- und Schwachstellenbewertung	36
8.5 Reaktion und Eskalation	36
8.6 Datenschutz klinischer Protokolldaten	36
8.7 Integration in SIEM und Abgrenzung zu NDR	36
9. Implementierung und Transition	37
9.1 Vorgehensmodell und Phasen	37
9.2 Asset- und Kritikalitätsklassifizierung	38
9.3 Logquellen-, Sensorik- und Integrationskatalog	38
9.4 Plattform-Übernahmen oder -Migrationen	38
9.5 Übergang der Serviceverantwortung und Ramp-up-Betrieb	39
9.6 Test, Validierung und Abnahme	40
9.7 Schulung, Wissenstransfer und Betriebshandbuch	40
9.8 Hypercare	41
10. Managed Service / Betriebsmodell	42
10.1 Betriebsorganisation und Serviceverantwortung	42
10.2 Eigenständige Bearbeitung und Begrenzung von Rückfragen	42
10.3 Security Monitoring und Triage	42
10.4 Methodik (MITRE ATT&CK)	43
10.5 Incident Handling	43
10.6 Investigation und forensische Analyse	43
10.7 Reaktion: Stufenmodell	44
10.8 Threat Hunting	44
10.9 SOAR und Playbooks	45
10.10 Use-Case-, Detection- und Regelpflege	45
10.11 Schwachstellen-Service im laufenden Betrieb	45

10.12 Incident- und Request-Klassen	46
10.13 Service Requests	46
10.14 Change-Management.....	47
10.15 Major Incident und Krisenmodus.....	48
10.16 Threat Intelligence.....	49
10.17 Service Health Monitoring und Datenqualitätskontrolle.....	49
10.18 Reporting und Service Reviews	49
10.19 Problem Management und kontinuierliche Verbesserung.....	49
10.20 Business Continuity und Notbetrieb des Auftragnehmers.....	50
11. Prozess- und Ticketintegration (ServiceNow)	51
11.1 Integration als gemeinsam getragene Leistung	51
11.2 Vorgangsarten und Mindestinformationen	51
11.3 Statussynchronisation und Übergabe an Gruppen	52
11.4 Eskalation und Sofortkommunikation	52
11.5 Ersatzverfahren	52
12. SLA, Reporting und Eskalation	53
12.1 Prioritätsmodell.....	53
12.2 SLA-Kennzahlen	53
12.3 Plattformverfügbarkeit	54
12.4 Status-Updates.....	54
12.5 Eskalationsmodell	55
12.6 Reportingpflichten	55
13. Rollen und Verantwortlichkeiten.....	56
13.1 Rollen des Auftragnehmers.....	56
13.2 Rollen des Auftraggebers.....	56
13.3 RACI-Übersicht (Auszug)	57
14. Exit Management	58
14.1 Auslöser und Grundsätze.....	58
14.2 Exit-Konzept.....	58
14.3 Übergabeobjekte	58
14.4 Datenexport und Löschung	59
14.5 Lizenz- und Übergaberechte	59
14.6 Abnahme des Exit-Prozesses	59
14.7 Unterstützung bei der Transition auf einen Nachfolgedienstleister	59
Anlage-D3_Zuschlagskriterien Bewertungsmatrix 20260826	61
Anlage-D4_Anforderungen Lösungsansätze 20260826	71
Bietergemeinschaft und Nachunternehmer.....	77
Anlage-EN1 Eigenerklärung Nachunternehmer.pdf	77
Anlage-EN2 Verpflichtungserklärung Nachunternehmer.pdf.....	78
Anlage-EBG Erklärung Bietergemeinschaft.pdf	79
Anlage-BMWK Eigenerklärung Bezug Russland.pdf	80
Anlage-VT Verpflichtungserklärung Tariftreue und Mindestlohn.pdf.....	82

Vertragsbedingungen UKF	84
EVB_IT_Systemvertrag blanco	84
1 Gegenstand, Vergütung und Bestandteile des Vertrages	88
1.1 Vertragsgegenstand	88
1.2 Vergütung	88
1.3 Vertragsbestandteile*	89
2 Übersicht über die vereinbarten Leistungen	89
2.1 Leistungen bis zur Abnahme	89
2.2 Leistungen nach der Abnahme	90
2.3 Vorgehensmodell	90
3 Systemumgebung* des Gesamtsystems und beizustellende Systemkomponenten*	90
4 Leistungen des Auftragnehmers zur Erstellung des Gesamtsystems	90
4.1 Verkauf von Hardware	90
4.2 Vermietung von Hardware	91
4.3 Überlassung von Standardsoftware* gegen Einmalvergütung auf Dauer (Verkauf)	91
4.3.1 Leistungsumfang und Vergütung	91
4.3.2 Mitteilung über Anpassungen der Standardsoftware* auf Quellcodeebene	92
4.3.3 Abweichende Lizenzbedingungen	93
4.3.3.1 Bezüglich der Nutzungsrechte an der jeweiligen Standardsoftware* oder ..	93
4.3.3.2 Regelungen für Open Source Software*	93
4.3.4 Bereitstellung der Standardsoftware*	93
4.4 Überlassung von Standardsoftware* auf Zeit (Vermietung)	93
4.4.1 Leistungsumfang und Vergütung	93
4.4.2 Mitteilung über Anpassungen der Standardsoftware* auf Quellcodeebene	94
4.4.3 Abweichende Lizenzbedingungen	95
4.4.3.1 Bezüglich der Nutzungsrechte an der jeweiligen Standardsoftware* oder ..	95
4.4.3.2 Regelungen für Open Source Software*	95
4.4.4 Bereitstellung der Standardsoftware*	95
4.5 Erstellung und Überlassung von Individualsoftware* auf Dauer	95
4.5.1 Leistungsumfang	95
4.5.2 Vergütung	96
4.5.3 Abweichende Nutzungsrechte an der Individualsoftware*	96
4.5.3.1 Open Source Software*	96
4.5.3.2 Keine Bereitstellung als Open Source Software*	96
4.5.3.3 Werkzeuge*	97
4.5.4 Sonderregelung: Lizenzrückvergütung (nur möglich bei nicht ausschließlicher Nu	97
4.5.5 Einräumung von Rechten an Erfindungen	97
4.5.6 Bereitstellung der Individualsoftware*	97
4.6 Übernahme von Altdaten und andere Migrationsleistungen	98
4.6.1 Leistungsumfang	98
4.6.2 Vergütung	98
4.7 Erstellung des Gesamtsystems und Herbeiführung der Betriebsbereitschaft*	98

4.7.1 Leistungsumfang	98
4.7.2 Abweichende Nutzungsrechtsvereinbarungen	98
4.7.3 Vergütung	98
4.8 Schulung	98
4.8.1 Art und Umfang der Schulungen	98
4.8.2 Schulungsunterlagen	99
4.8.3 Vergütung für Schulungen inkl. Schulungsunterlagen	100
4.9 Dokumentation	100
4.10 Software Bill of Materials (SBOM)*	100
4.11 Sonstige Leistungen zur Systemerstellung	100
4.11.1 Leistungsumfang	100
4.11.2 Vergütung	100
5 Systemservice	101
5.1 Arten von Systemserviceleistungen	101
5.1.1 Wiederherstellung der Betriebsbereitschaft* des Gesamtsystems (Störungsbesei	101
5.1.1.1 Störungsmeldung	101
5.1.1.2 Reaktions-* und Wiederherstellungszeiten*, Mängelklassen	101
5.1.1.3 Servicezeiten	102
5.1.1.4 Hotline	102
5.1.2 Aufrechterhaltung der Betriebsbereitschaft* (vorbeugende Maßnahmen)	102
5.1.3 Überlassung von verfügbaren Programmständen* (Standardsoftware*)	103
5.2 Beginn / Dauer der Systemserviceleistungen	103
5.3 Kündigung von Systemserviceleistungen	103
5.4 Vergütung/Zahlungsfristen für Systemserviceleistungen	103
5.4.1 Vergütung	103
5.4.2 Zahlungsfristen für Systemserviceleistungen	104
5.5 Sonstige Regelungen zu Systemserviceleistungen	104
5.5.1 Teleservice*	104
5.5.2 Abnahme der Systemserviceleistungen	104
5.5.3 Dokumentation der Systemserviceleistungen	104
6 Zusätzliche Regelungen für Open Source Software*	104
7 Weitere Leistungen nach der Abnahme	105
7.1 Weiterentwicklung und Anpassung des Gesamtsystems nach der Abnahme	105
7.2 Sonstige Leistungen nach der Abnahme	105
7.2.1 Leistungsumfang	105
7.2.2 Vergütung	105
8 Ergänzende Vereinbarungen bei Vergütung nach Aufwand	106
8.1 Vereinbarung der Preiskategorien bei Vergütung nach Aufwand	106
8.2 Zeiten der Leistungserbringung bei Vergütung nach Aufwand	106
8.2.1 Während der Geschäftszeiten an Werktagen (außer an Samstagen und Feiertag	106
8.2.2 Außerhalb der Geschäftszeiten an Werktagen (außer an Samstagen und Feiertag	106
8.2.3 Während sonstiger Zeiten	106

8.3 Abweichende Regelungen für die Bestimmung und Vergütung von Personentagesätze	106
8.4 Reisekosten, Nebenkosten*, Materialkosten und Reisezeiten	106
8.4.1 Reisekosten, Nebenkosten* und Materialkosten	106
8.4.2 Reisezeiten	107
8.5 Besondere Bestimmungen zur Vergütung nach Aufwand	107
8.6 Preisanpassung für Systemserviceleistungen, die nicht im Pauschalpreis* enthalten	107
9 Termin- und Leistungsplan	107
10 Zahlungsplan, Rechnungen	108
11 Projektmanagement	108
11.1 Projektmanager/Projektleiter	108
11.2 Weitere Schlüsselpositionen des Auftragnehmers	109
11.3 Projektsteuerung/Projektkoordinierung	109
11.4 Behandlung von Änderungsverlangen (Change Requests)	109
12 Weitere Pflichten des Auftragnehmers	109
12.1 Besondere Anforderungen an Mitarbeiter des Auftragnehmers	109
12.2 Allgemeine Sicherheitsanforderungen	110
12.3 Kopier- oder Nutzungssperre*	110
12.4 Mitteilungspflicht bezüglich der zur Vertragserfüllung eingesetzten Werkzeuge*	110
12.5 Entsorgung der Hardware (ergänzend zu Ziffer 2.1 EVB-IT System-AGB)	110
12.6 Entsorgung der Verpackung	110
13 Mitwirkung des Auftraggebers	110
14 Abnahme	111
14.1 Gegenstand der Abnahme	111
14.2 Testdaten	111
14.3 Dauer, Ort und Systemumgebung* der Funktionsprüfung	111
14.4 Vereinbarungen zur Durchführung der Funktionsprüfung und zur Erklärung der Abnah.	111
14.5 Vereinbarungen zu Mängelklassen im Rahmen der Funktionsprüfung	111
15 Mängelhaftung (Gewährleistung)	111
15.1 Verjährungsfrist (Gewährleistungsfrist) für Mängel des Gesamtsystems	111
15.2 Verjährungsfrist (Gewährleistungsfrist) für Mängel an Teilleistungen	112
15.3 Mängelmeldungen	112
15.3.1 Form der Mängelmeldung	112
15.3.2 Adresse für Mängelmeldungen	112
15.4 Reaktions-* und Wiederherstellungszeiten*, Servicezeiten, Hotline	112
15.4.1 Reaktions-* und Wiederherstellungszeiten*, Mängelklassen	112
15.4.2 Servicezeiten	113
15.4.3 Hotline	113
15.5 Teleservice*	113
15.6 Weitere Vereinbarungen zur Mängelhaftung	113
16 Haftungsregelungen	113
16.1 Haftungsobergrenze bei leicht fahrlässiger Pflichtverletzung	113
16.2 Haftung bei Verzug	114

16.3 Haftung für den Systemservice	114
16.4 Haftung für entgangenen Gewinn	114
17 Vertragsstrafen bei Verzug.....	114
17.1 Verzug bei Erstellung des Gesamtsystems.....	114
17.2 Verzug bei Reaktions-* und Wiederherstellungszeiten*	114
18 Weitere Vereinbarungen	114
18.1 Garantien.....	114
18.1.1 Auftragnehmergarantien.....	114
18.1.2 Herstellergarantien	115
18.2 Übergabe bzw. Hinterlegung des Quellcodes*	115
18.2.1 Übergabe des Quellcodes*	115
18.2.2 Hinterlegung des Quellcodes	115
18.3 Haftpflichtversicherung	116
18.4 Sicherheiten	116
18.4.1 Vorauszahlungsbürgschaft.....	116
18.4.2 Vertragserfüllungs- oder Mängelhaftungssicherheit.....	116
18.4.3 Kombinierte Vertragserfüllungs- oder Mängelhaftungssicherheit.....	116
18.5 Datenschutz, Geheimhaltung und Sicherheit	117
18.6 Vereinbarungen zur Korruptionsprävention.....	117
18.7 Kündigungsrecht des Auftraggebers	117
18.8 Sonstige Vereinbarungen.....	117
Anlage EVB-IT Exit SLA Vergütung SOC-SIEM	118
EVB_IT_System_AGB	127
1 Gegenstand des EVB-IT Systemvertrages	128
2 Art und Umfang der Leistungen zur Erstellung des Gesamtsystems.....	129
3 Mängelklassifizierung	135
4 Systemservice nach Abnahme.....	135
5 Dokumentation und Software Bill of Materials (SBOM)*	138
6 Mitteilungspflichten des Auftragnehmers	139
7 Personal des Auftragnehmers, Subunternehmer	140
8 Vergütung.....	140
9 Verzug	141
10 Projektmanagement	141
11 Mitwirkung des Auftraggebers.....	142
12 Abnahme	143
13 Rechte des Auftraggebers bei Mängeln des Gesamtsystems (Gewährleistung)	144
14 Schutzrechte Dritter.....	145
15 Haftungsbeschränkung	146
16 Laufzeit und Kündigung.....	146
17 Änderung der Leistung nach Vertragsschluss.....	147
18 Quellcodeübergabe und Quellcodehinterlegung	148
19 Haftpflichtversicherung.....	149

20 Vorauszahlungsbürgschaft, Vertragserfüllungs... und Mängelhaftungssicherheit	149
21 Datenschutz, Geheimhaltung und Sicherheit	150
22 Zurückbehaltungsrechte	151
23 Schlichtungsverfahren	151
24 Textform	151
25 Anwendbares Recht	151
Anlage- AVV.pdf	158
Lieferanten Code of ConductDE.pdf	174
Eignungskriterien.....	182
Anlagen	191

13.10.2026 12:00:00



Universitätsklinikum Frankfurt
Theodor-Stern-Kai 7, 60590 Frankfurt am Main, Deutschland

22.09.2026

{Bieterdaten: Name | Supplier.Name}
{Bieterdaten: Straße | Supplier.AddressStreet}
{Bieterdaten: PLZ und Ort | Supplier.AddressZipCodeCity}

Unser Zeichen: 20261023

Betreff: Aufforderung zur Abgabe eines Teilnahmeantrags

Sehr geehrte Damen und Herren,

das Universitätsklinikum Frankfurt – Anstalt des öffentlichen Rechts – schreibt im Namen und auf Rechnung von Universitätsklinikum Frankfurt 60590 Frankfurt am Main folgende Leistung aus:

Security Managed Services

Verhandlungsverfahren mit Teilnahmewettbewerb (EU) (VgV)

Anmerkungen: Vertragsbeginn: schnellstmöglich; Leistungsbeginn: 01.06.2027 Laufzeit 60 Monate

Der Umfang der Leistung ergibt sich aus der Leistungsbeschreibung. Der Zuschlag wird auf das wirtschaftlichste Angebot erteilt.

Hinweise:

In der Phase des Teilnahmewettbewerbs sind keine Lösungskonzepte (vgl. Anlagen D3 + D4) einzureichen und keine Preise (vgl. Anlage D5) zu kalkulieren. Dies ist erst erforderlich, wenn die zugelassenen Teilnehmer zur Abgabe eines Angebotes aufgefordert werden. Gleiches gilt für den beiliegenden EVB-IT System sowie für die Anlage-AVV (Auftragsdatenverarbeitung) [jeweils blanko]. Sind mehr als 4 (vier) Teilnehmer geeignet, dann entscheidet die Summe der Punkte aus den Bewertungskriterien über die weitere Teilnahme. Das Verfahren wird mit den Rängen 1 – 4 (höchste Punktzahl absteigend) fortgesetzt. Haben mehrere Teilnehmer die gleiche Punktzahl erreicht, dann entscheidet das Los.

I. Zuschlagskriterium

Wirtschaftlichstes Angebot
Berechnungsgrundlage ist die 'HVA-Bewertungsmethode'.
Gewichtung: 40%: 60%

II. Verfahren

Nebenangebote sind nicht zugelassen

Es ist nur die Abgabe eines Hauptangebots zugelassen.

A. Fristen

Frist Teilnahmeantrag: 13.10.2026 12:00:00Uhr

Frist für Bieterfragen: 29.09.2026 12:00 Uhr

B. Anlagen/Unterlagen, die im Vergabeverfahren zu beachten sind:

- Anlage-D Datenschutzerklärung
- Anlage-Bewerbungsbedingungen EU
- Anlage-D3_Zuschlagskriterien Bewertungsmatrix 20260826
- Anlage-D4_Anforderungen Lösungsansätze 20260826
- Lageplan (abzurufen unter: https://www.unimedizin-frankfurt.de/fileadmin/redakteure/Presse/Lageplan/lageplan_ukf.pdf)

C. Elektronische Teilnahme

Bitte melden Sie sich auf der Bekanntmachungsplattform unter <https://portal.deutsche-e-vergabe.de> mit Ihrem Benutzernamen und Ihrem Passwort an.

Sofern Sie im System noch nicht registriert sind, können Sie dies auf der Plattform vornehmen. Die Registrierung ist kostenfrei. Anschließend können Sie auf der Startseite bspw. nach dem Titel des Verfahrens über die Direksuche als Suchbegriff suchen. Folgen Sie anschließend der Anleitung im System, um an dem Verfahren

teilzunehmen.

D. Abgabe Teilnahmeunterlagen

Es werden nur elektronische Teilnahmeunterlagen in Schriftform akzeptiert!

Unterschriften: Durch Hochladen der Teilnahmeunterlagen und die in der eVergabe hinterlegte Signatur gelten die Teilnahmeunterlagen als signiert abgegeben.

E. Bieterfragen & Kommunikation

Bieterfragen müssen bis spätestens 29.09.2026 12:00 Uhr eingegangen sein. Für später eingehende Fragen wird keine Beantwortung zugesichert.

Bieterfragen müssen unter "Nachrichten" im eVergabe-Bieterassistenten gestellt und dort geprüft werden.

Den Assistenten erreichen Sie unter <https://portal.deutsche-e-vergabe.de>. Fragen auf anderen Kommunikationswegen, wie telefonisch, schriftlich oder per E-Mail, werden nicht beantwortet.

Bieterfragen müssen als eine Frage pro Nachricht über den Bieterassistenten eingereicht werden. Zudem sind angehängte Listen mit Fragen nicht zulässig.

Hinweis: Sie erhalten nach Beantwortung einer Bieterfrage eine Benachrichtigung per E-Mail. Alle Antworten müssen im Assistenten geprüft werden.

F. Vor-Ort-Besichtigung

Im Rahmen dieser Vergabe werden keine Objektbesichtigungen als erforderlich angesehen.

III. Bietergemeinschaft

Wird zur Leistungserbringung eine Bietergemeinschaft gebildet, ist die Anlage-EBG Eigenerklärung Bietergemeinschaft mit dem Angebot anzugeben und von jedem Mitglied der Bietergemeinschaft sind zusätzlich folgende Erklärung abzugeben:

- Anlage-BMWK Eigenerklärung Bezug zu Russland
- Anlage-VT Verpflichtungserklärung Tariftreue und Mindestlohn

Diese Dokumente sind gesondert von den dazu berechtigten Personen zu signieren.

IV. Nachunternehmer

Beabsichtigt der Bieter, Leistungen durch Nachunternehmer ausführen zu lassen, sind folgende Erklärungen und Nachweise abzugeben:

- Art und Umfang der Leistungen durch Nachunternehmer (Anlage-EN1, vom Bieter unterschrieben)
- Verpflichtungserklärung des Nachunternehmers (Anlage-EN2, vom Nachunternehmer unterschrieben).

Von allen Nachunternehmern sind nachfolgend aufgeführte Erklärungen und Nachweise mit dem Angebot einzureichen:

- Anlage-BMWK Eigenerklärung Bezug zu Russland
- Anlage-VT Verpflichtungserklärung Tariftreue und Mindestlohn

Die Einschaltung weiterer Nachunternehmer als der im Angebot benannten Nachunternehmer bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers. Der Bieter muss sicherstellen, dass ein Nachunternehmer die Leistungen nicht seinerseits ohne vorherige schriftliche Zustimmung des Auftraggebers weitervergibt.

Der Auftragnehmer ist verpflichtet,

- bei der Übertragung eines Unterauftrags nach wettbewerblichen Gesichtspunkten zu verfahren,
- dem Auftraggeber den Nachunternehmer zu benennen,
- dem Nachunternehmer insgesamt keine ungünstigeren Bedingungen – insbesondere hinsichtlich der Zahlungsweise und Sicherheitsleistungen – zu stellen, als zwischen ihm und dem Auftraggeber vereinbart sind.

Bei der Einholung von Angeboten für Unteraufträge sind regelmäßig kleine und mittlere Unternehmen angemessen zu beteiligen. Der Auftragnehmer hat sich ferner zu bemühen, Unteraufträge an kleine und mittlere Unternehmen in dem Umfang zu erteilen, wie er es mit der vertragsgemäßen Ausführung der Leistung vereinbaren kann.

V. Eignungsleihe

Sofern ein Bieter im Hinblick auf die erforderliche wirtschaftliche und finanzielle sowie die technische und berufliche Leistungsfähigkeit die Kapazitäten anderer Unternehmen in Anspruch nehmen will, wird im Rahmen der Eignungsprüfung überprüft, ob die Unternehmen, deren Kapazitäten der Bewerber oder Bieter für die Erfüllung bestimmter Eignungskriterien in Anspruch nehmen will, die entsprechenden Eignungskriterien erfüllen und ob Ausschlussgründe vorliegen.

Nimmt ein Bieter die Kapazitäten eines anderen Unternehmens im Hinblick auf die erforderliche wirtschaftliche und finanzielle Leistungsfähigkeit in Anspruch, so behält sich der Auftraggeber vor eine gemeinsame Haftung des Bieters und des anderen Unternehmens für die Auftragsausführung entsprechend dem Umfang der Eignungsleihe zu verlangen.

VI. Teilnahmeantrag

Mit der **Anlage-T Teilnahmeantrag** sind alle geforderten Anlagen und Nachweise abzugeben.

A. Unterlagen, die ggfs. ausgefüllt beigelegt / erstellt werden müssen:

- Anlage Kriterienkatalog (im Bietercockpit der eVergabe)
- Gültiges ISO 27001-Zertifikat
- Gültiges ISO 9001-Zertifikat
- BSI APT-Response-Listungsnachweis oder gleichwertiger Befähigungsnachweis...
- **bei Bietergemeinschaften:**
 - Anlage-EN 1 Eigenerklärung Nachunternehmereinsatz
 - Anlage-EN 2 Verpflichtungserklärung Nachunternehmer
 - Anlage-EBG Eigenerklärung Bietergemeinschaft
 - Anlage-BMWK bei Nachunternehmer + Bietergemeinschaft
 - Anlage-VT bei Nachunternehmer + Bietergemeinschaft

B. Unterlagen, die auf gesondertes Verlangen der Vergabestelle vorzulegen sind:

- weitergehende Referenznachweise

C. Anlagen des Bieters

Es wird ausdrücklich darauf hingewiesen, dass alle dem Angebot beigelegten Anlagen Angebotsbestandteil sind. Dies gilt auch für Prospekte und Technische Datenblätter.

Falls es nicht ausdrücklich gefordert wird, ist die Abgabe von Prospekten, Broschüren oder Datenblättern nicht erwünscht und kann zum Ausschluss des Bieters führen.

Sofern Prospekte oder Datenblätter beigelegt werden, muss aus dem Prospekt oder dem Datenblatt eindeutig hervorgehen und vom Bieter markiert werden, welches Produkt und welche Produktkonfiguration oder Leistung angeboten wird.

Wird vom Bieter in den von ihm mit dem Angebot abgegebenen Anlagen auf Zertifizierungen/Nachweise verwiesen, sind diese ebenfalls als Anlagen dem Angebot beizufügen.

Werden vom Bieter eigene Allgemeine-, Besondere-, Zusätzliche oder Ergänzende Geschäftsbedingungen mit dem Angebot abgegeben oder in Angebotsanlagen auf diese verwiesen, ist das Angebot nicht beauftragungsfähig, da es unter einem nicht vorgesehenen Vorbehalt steht.

VII. Vertragsunterlagen

Werden den geeigneten Bietern mit Aufforderung zur Angebotsabgabe zur Verfügung gestellt.

Unterlagen die beim Bieter verbleiben und bei Beauftragung Vertragsbestandteil werden:

- Anlagen/Unterlagen gemäß Abschnitt VI. A
- Anlage-D1 Leistungsverzeichnis 20260826
- EVB_IT_Systemvertrag blanco
- Anlage EVB-IT Exit SLA Vergütung SOC-SIEM
- EVB_IT_System_AGB
- Anlage -AVV Auftragsdatenverarbeitung (nach Zuschlag vom Auftragnehmer auszufüllen)
- Code of Conduct für Lieferanten (abzurufen unter: <https://www.unimedizin-ffm.de/ueber-uns/lieferkettensorgfaltspflichtengesetz>)

VIII. Schutzrechte

Der Auftragnehmer stellt den Auftraggeber auf eigene Kosten von allen Ansprüchen Dritter frei, die gegen den Auftraggeber wegen Verletzung von Schutzrechten an den angebotenen Geräten oder Dienstleistungen geltend gemacht werden.

IX. Verschwiegenheit

Der Bieter hat auch nach Beendigung des Vergabeverfahrens über die ihm bei seiner Tätigkeit bekannt gewordenen Informationen Verschwiegenheit zu bewahren. Er hat hierzu auch die mit der Erstellung des Angebotes beschäftigten Mitarbeiter und Nachunternehmer zu verpflichten. Der Auftraggeber behält sich vor, diesbezügliche Nachweise im Falle der beabsichtigten Auftragsvergabe zu verlangen.

X. Rechtsschutz

Behörde für Nachprüfung behaupteter Verstöße gegen Vergabebestimmungen (Vergabekammer gem. § 156 GWB): Vergabekammer des Landes Hessen beim Regierungspräsidium Darmstadt

Wilhelminenstraße 1–3 (Wilhelminenhaus)

64283 Darmstadt

Kontakt ist per E-Mail unter vergabekammer@rpd.hessen.de

Mit freundlichen Grüßen,
Vergabeabteilung

Aufsichtsrat
Christoph Degen
(Vorsitzender)

Postanschrift
Universitätsklinikum Frankfurt
Theodor-Stern-Kai 7
60590 Frankfurt a. M.

Frankfurter Sparkasse
IBAN: DE32 5005 0201 0000
3799 99
BIC: HELADEF1822

Postbank Frankfurt
IBAN: DE14 5001 0060 0000
7606 03
BIC: PBNKDEFF

Bewerbungsbedingungen für die Vergabe von Leistungen

Das Vergabeverfahren erfolgt nach der Vergabeverordnung (VgV).

1 Mitteilung von Unklarheiten in den Vergabeunterlagen

Enthalten die Vergabeunterlagen nach Auffassung des Unternehmens Unklarheiten, Unvollständigkeiten oder Fehler, so hat es unverzüglich die Vergabestelle vor Angebotsabgabe in Textform darauf hinzuweisen.

2 Unzulässige Wettbewerbsbeschränkungen

Angebote von Bietern, die sich im Zusammenhang mit diesem Vergabeverfahren an einer unzulässigen Wettbewerbsbeschränkung beteiligen, werden ausgeschlossen.

Zur Bekämpfung von Wettbewerbsbeschränkungen hat der Bieter auf Verlangen Auskünfte darüber zu geben, ob und auf welche Art er wirtschaftlich und rechtlich mit Unternehmen verbunden ist.

3 Angebot

3.1 Das Angebot ist in deutscher Sprache abzufassen.

3.2 Für das Angebot sind die von der Vergabestelle vorgegebenen Vordrucke zu verwenden. Das Angebot ist bis zu dem von der Vergabestelle angegebenen Ablauf der Angebotsfrist einzureichen. Ein nicht form- oder fristgerecht eingereichtes Angebot wird ausgeschlossen.

3.3 Eine selbst gefertigte Abschrift oder Kurzfassung des Leistungsverzeichnisses ist zulässig.

Die von der Vergabestelle vorgegebene Langfassung des Leistungsverzeichnisses ist allein verbindlich.

3.4 Unterlagen, die von der Vergabestelle nach Angebotsabgabe verlangt werden, sind zu dem von der Vergabestelle bestimmten Zeitpunkt einzureichen.

3.5 Alle Eintragungen müssen dokumentenecht sein.

3.6 Ein Bieter, der in seinem Angebot die von ihm tatsächlich für einzelne Leistungspositionen geforderten Einheitspreise auf verschiedene Einheitspreise anderer Leistungspositionen verteilt, benennt nicht die von ihm geforderten Preise. Deshalb werden Angebote, bei denen der Bieter die Einheitspreise einzelner Leistungspositionen in „Mischkalkulationen“ auf andere Leistungspositionen umlegt, von der Wertung ausgeschlossen.

3.7 Alle Preise sind in Euro mit höchstens drei Nachkommastellen anzugeben.

Die Preise (Einheitspreise, Pauschalpreise, Verrechnungssätze usw.) sind ohne Umsatzsteuer anzugeben. Der Umsatzsteuerbetrag ist unter Zugrundelegung des geltenden Steuersatzes am Schluss des Angebotes hinzuzufügen.

Es werden nur Preisnachlässe gewertet, die

- ohne Bedingungen als Vomhundertsatz auf die Abrechnungssumme gewährt werden und

- an der im Angebotsschreiben bezeichneten Stelle aufgeführt sind.

Nicht zu wertende Preisnachlässe bleiben Inhalt des Angebotes und werden im Fall der Auftragserteilung Vertragsinhalt.

4 Nebenangebote

4.1 Nebenangebote müssen die geforderten Mindestanforderungen erfüllen; dies ist mit Angebotsabgabe nachzuweisen.

4.2 Der Bieter hat die in Nebenangeboten enthaltenen Leistungen eindeutig und erschöpfend zu beschreiben; die Gliederung des Leistungsverzeichnisses ist, soweit möglich, beizubehalten.

Nebenangebote müssen alle Leistungen umfassen, die zu einer einwandfreien Ausführung der Leistung erforderlich sind.

Soweit der Bieter eine Leistung anbietet, deren Ausführung nicht in den Vergabeunterlagen geregelt ist, hat er im Angebot entsprechende Angaben über Ausführung und Beschaffenheit dieser Leistung zu machen.

- 4.3 Nebenangebote sind, soweit sie Teilleistungen (Positionen) des Leistungsverzeichnisses beeinflussen (ändern, ersetzen, entfallen lassen, zusätzlich erfordern), nach Mengenansätzen und Einzelpreisen aufzugliedern (auch bei Vergütung durch Pauschalsumme).
- 4.4 Nebenangebote, die den Nummern 4.1 bis 4.3 nicht entsprechen, werden von der Wertung ausgeschlossen.

5 Bietergemeinschaften

- 5.1 Die Bietergemeinschaft hat mit ihrem Angebot eine Erklärung aller Mitglieder in Textform abzugeben,
- in der die Bildung einer Arbeitsgemeinschaft im Auftragsfall erklärt ist,
 - in der alle Mitglieder aufgeführt sind und der für die Durchführung des Vertrags bevollmächtigte Vertreter bezeichnet ist,
 - dass der bevollmächtigte Vertreter die Mitglieder gegenüber dem Auftraggeber rechtsverbindlich vertritt,
 - dass alle Mitglieder als Gesamtschuldner haften.
- Auf Verlangen der Vergabestelle ist eine von allen Mitgliedern unterzeichnete bzw. fortgeschritten oder qualifiziert signierte Erklärung abzugeben.
- 5.2 Sofern nicht im offenen Verfahren ausgeschrieben wird, werden Angebote von Bietergemeinschaften, die sich erst nach der Aufforderung zur Angebotsabgabe aus aufgeforderten Unternehmen gebildet haben, nicht zugelassen.

6 Kapazitäten anderer Unternehmen (Unteraufträge, Eignungsleihe)

Beabsichtigt der Bieter, Teile der Leistung von anderen Unternehmen ausführen zu lassen oder sich bei der Erfüllung eines Auftrages im Hinblick auf die erforderliche wirtschaftliche, finanzielle, technische oder berufliche Leistungsfähigkeit anderer Unternehmen zu bedienen, so muss er die hierfür vorgesehenen Leistungen/Kapazitäten in seinem Angebot benennen. Der Bieter hat auf gesondertes Verlangen der Vergabestelle zu einem von ihr bestimmten Zeitpunkt nachzuweisen, dass ihm die erforderlichen Kapazitäten der anderen Unternehmen zur Verfügung stehen und diese Unternehmen geeignet sind. Er hat den Namen, den gesetzlichen Vertreter sowie die Kontaktdaten dieser Unternehmen anzugeben und entsprechende Verpflichtungserklärungen dieser Unternehmen vorzulegen.

Nimmt der Bieter in Hinblick auf die Kriterien für die wirtschaftliche und finanzielle Leistungsfähigkeit im Rahmen einer Eignungsleihe die Kapazitäten anderer Unternehmen in Anspruch, müssen diese gemeinsam für die Auftragsausführung haften; die Haftungserklärung ist gleichzeitig mit der Verpflichtungserklärung abzugeben.

Der Bieter hat andere Unternehmen, bei denen Ausschlussgründe vorliegen oder die das entsprechende Eignungskriterium nicht erfüllen, innerhalb einer von der Vergabestelle gesetzten Frist zu ersetzen.

7 Eignung

Unternehmen haben als Nachweis der Eignung für die zu vergebende Leistung mit dem Angebot

- **Entweder** die in der Auftragsbekanntmachung oder der Aufforderung zur Interessensbestätigung angegebenen Unterlagen (Eigenerklärungen, Angaben, Bescheinigungen und sonstige Nachweise)
- **Oder** eine Einheitliche Europäische Eigenerklärung (EEE) als vorläufigen Nachweis vorzulegen.

Bei Einsatz von anderen Unternehmen gemäß Nummer 6 sind auf gesondertes Verlangen die Unterlagen/die EEE auch für diese abzugeben.

Gelangt das Angebot in die engere Wahl, sind Eigenerklärungen (auch die der benannten anderen Unternehmen) auf gesondertes Verlangen durch Vorlage der genannten Bescheinigungen zuständiger Stellen zu bestätigen. Bescheinigungen, die nicht in deutscher Sprache abgefasst sind, ist eine Übersetzung in die deutsche Sprache beizufügen.

Die Verpflichtung zur Vorlage von Eigenerklärungen und Bescheinigungen entfällt, soweit die Eignung (Bieter und benannte andere Unternehmen) bereits im Teilnahmewettbewerb nachgewiesen ist.

Universitätsmedizin Frankfurt
Vergabenummer: 20261023
Vergabeverfahren: Security Managed Services

Information nach Art. 13 Datenschutz-Grundverordnung (DSGVO)

Information nach Art. 13 DSGVO

Vertrauen ist wichtig, besonders wenn es um Ihre Daten geht. Aus diesem Grund erachten wir es als unsere Verpflichtung, nur die Daten zu erheben, welche unbedingt erforderlich sind, sowie die Daten mit der gebotenen Sorgfalt zu verwalten und vor Missbräuchen zu schützen.

Die Universitätsmedizin Frankfurt hält sich strikt an die datenschutzrechtlichen Vorschriften bei der Erhebung und Verarbeitung Ihrer Daten.

Nachstehend finden Sie Informationen zur Verarbeitung Ihrer Daten und den Ihnen zukommenden Rechten:

1. Name und Kontaktdaten des/der Verantwortlichen

Universitätsmedizin Frankfurt
Theodor-Stern-Kai 7
60596 Frankfurt am Main
Telefon: +49 69 63 01-0
Fax: +49 69 6301-63 01

E-Mail: info@unimedizin-ffm.de
Internet: www.unimedizin-ffm.de

2. Kontaktdaten der/des Datenschutzbeauftragten (gemäß Art. 37 DSGVO)

Datenschutzbeauftragte(r) der Universitätsmedizin Frankfurt
Theodor-Stern-Kai 7
60596 Frankfurt am Main

Telefon: +49 69 63 01-7235
E-Mail: datenschutz@unimedizin-ffm.de

3. Kategorien der erhobenen personenbezogenen Daten, Zwecke und Rechtsgrundlagen der Verarbeitung

Im Vergabeverfahren sind personenbezogene Daten, insbesondere bei der Eignungsprüfung von Bedeutung, etwa wenn die Bieter aufgefordert werden, Referenzen mit Lebensläufen, Namen, Adressen und Fotos ihrer Mitarbeiter vorzulegen. Auch Studien- und Ausbildungsnachweise sind personenbezogene Daten, welche im Rahmen des Verfahrens verarbeitet werden können.

Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene einwilligt.

Nach Art. 6 Abs. 1 b) DSGVO ist die Datenverarbeitung zulässig, wenn sie zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist. Die Datenverarbeitung ist zudem nach Art. 6 Abs. 1 c) DSGVO zulässig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, welcher der Verantwortliche unterliegt. Gem. Art. 6 Abs. 1 a) DSGVO ist die Datenverarbeitung zulässig, wenn sie auf einer Einwilligung beruht.

Da wir als Vergabestelle nach dem Vergaberecht verpflichtet sind, die Eignung unter Verarbeitung von personenbezogenen Daten zu prüfen, ist dies nach den vorgenannten Regelungen zulässig.

Zudem kommt eine Verarbeitung aufgrund einer konkludenten Einwilligung in Betracht, wenn die Bieter und deren Beschäftigte personenbezogene Daten im Rahmen der Bewerbung selbst zur Verfügung stellen.

4. Dauer der Speicherung der personenbezogenen Daten

Ihre Daten werden nach der Erhebung so lange gespeichert, wie dies

- unter Beachtung der gesetzlichen Aufbewahrungsfristen gemäß §8 Abs 4 VgV bzw. §6 Abs. 2 UVgO erforderlich ist.

5. Betroffenenrechte

Nach der EU-Datenschutz-Grundverordnung stehen Ihnen folgende Rechte zu:

- (i) Auskunft zu erhalten über die verarbeiteten personenbezogenen Daten bzw. deren Kategorien, die Verarbeitungszwecke, die Kategorien von Empfängern, gegenüber denen Ihre Daten offengelegt wurden oder werden, die Absicht, Daten an ein Drittland oder eine internationale Organisation zu übermitteln einschliesslich dafür geeigneter Garan-

tien, die geplante Speicherdauer, das Bestehen eines Rechts auf Berichtigung, Löschung, Einschränkung der Verarbeitung oder Widerspruch, das Bestehen eines Beschwerderechts, die Herkunft Ihrer Daten, sofern diese nicht bei uns erhoben wurden, sowie über das Bestehen einer automatisierten Entscheidungsfindung einschliesslich Profiling und ggf. aussagekräftigen Informationen zu deren Einzelheiten,

- (ii) die Berichtigung, Ergänzung, oder das Löschen Ihrer personenbezogenen Daten, die falsch sind oder nicht rechtskonform verarbeitet werden, zu verlangen,
- (iii) von uns zu verlangen, die Verarbeitung Ihrer personenbezogenen Daten einzuschränken,
- (iv) unter bestimmten Umständen der Verarbeitung Ihrer personenbezogenen Daten zu widersprechen oder die für das Verarbeiten zuvor gegebene Einwilligung zu widerrufen,
- (v) Ihre personenbezogenen Daten, die Sie uns bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten oder die Übermittlung an einen anderen Verantwortlichen zu verlangen,
- (vi) bei der zuständigen Datenschutzaufsichtsbehörde Beschwerde zu erheben.

6. Widerrufsrecht bei Einwilligung

Wenn Sie in die Verarbeitung durch eine entsprechende Erklärung eingewilligt haben, können Sie die Einwilligung jederzeit für die Zukunft widerrufen. Die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Datenverarbeitung wird durch diesen nicht berührt.

Möchten Sie von Ihrem Widerrufsrecht Gebrauch machen, teilen Sie dies per E-Mail an datenschutz@unimedizin-ffm.de mit.

D1 – Technische Leistungsbeschreibung

Security Managed Services

SOC / SIEM, NDR, Vulnerability Management, EDR-Management und IoMT-Security

Inhaltsverzeichnis

1. EINLEITUNG.....	5
1.1 AUFTRAGGEBER UND KRITIS-KONTEXT	5
1.2 ZIEL DER BESCHAFFUNG	5
2. IST-ZUSTAND	7
2.1 MENGengerüst	7
2.2 BESTEHENDE KOMPONENTEN JE LEISTUNGSBEREICH	8
2.3 DATENGRUNDLAGE UND KALKULATIONSBASIS	8
3. ALLGEMEINE ANFORDERUNGEN	10
3.1 DATENHOHEIT UND DATENHALTUNG	10
3.2 LIZENZHOHEIT (BYOL)	11
3.3 KLINISCHER SONDERKONTEXT UND PATIENTENSICHERHEIT.....	11
3.4 ANONYMISIERUNG KLINISCHER PROTOKOLLDATEN	11
3.5 FLEXIBLES ONBOARDING UND ERWEITERBARKEIT	12
3.6 HERSTELLEROFFENHEIT	12
3.7 BIDIREKTIONALE SERVICENow-INTEGRATION ALS GEMEINSAM GETRAGENE LEISTUNG.....	12
3.8 SPRACHE UND SERVICE DELIVERY	12
4. LEISTUNGSBEREICH SOC / SIEM.....	13
4.1 GELTUNGSBEREICH UND DATENQUELLEN.....	13
4.2 DATENAUFNAHME, PARSING UND ANREICHERUNG	13
4.3 USE CASES, DETECTION ENGINEERING UND THREAT INTELLIGENCE	14
4.4 ALARMIERUNG UND ANALYSETIEFE.....	15
4.5 PLATTFORMBETRIEB, PLATTFORMSICHERHEIT UND ZUGRIFF	15
4.6 INTEGRATION MIT DEN ÜBRIGEN LEISTUNGSBEREICHEN.....	16
4.7 BEITRAG ZUM SZA-NACHWEIS	16
5. LEISTUNGSBEREICH NDR	17
5.1 GELTUNGSBEREICH UND ZIELBILD	17
5.2 SENSORIK UND ERFASSUNG	17
5.3 DETEKTION UND ANALYSEFÄHIGKEITEN	17
5.4 DATENHALTUNG UND INVESTIGATION-FÄHIGKEIT	18
5.5 PLATTFORM- UND LIZENZMODELL	18
5.6 INTEGRATION IN SIEM UND REAKTIONSFÄHIGKEIT	18
6. LEISTUNGSBEREICH VULNERABILITY MANAGEMENT	20
6.1 GELTUNGSBEREICH UND ZIELBILD	20
6.2 PLATTFORM- UND LIZENZMODELL	20
6.3 SCANNING, DISCOVERY UND DATENERHEBUNG	20
6.4 TRIAGE, KONTEXTPRIORISIERUNG UND HANDLUNGSEMPFEHLUNGEN.....	21

6.5 REMEDIATION-TRACKING, VALIDIERUNG UND RISIKOAKZEPTANZ	21
6.6 INTEGRATION UND REPORTING.....	22
 <u>7. LEISTUNGSBEREICH EDR-MANAGEMENT.....</u>	 <u>23</u>
7.1 GELTUNGSBEREICH.....	23
7.2 PLATTFORM- UND LIZENZMODELL	23
7.3 ANFORDERUNGEN AN DEN BETRIEB UND DIE SERVICEINTEGRATION.....	24
7.4 AGENTENBETRIEB UND HEALTH MONITORING.....	25
7.5 POLICY- UND KONFIGURATIONSMANAGEMENT	25
7.6 RESPONSE- UND CONTAINMENT-MAßNAHMEN	25
7.7 INTEGRATION IN SIEM UND XDR-OPTIONEN	26
 <u>8. LEISTUNGSBEREICH IOMT-SECURITY</u>	 <u>27</u>
8.1 GELTUNGSBEREICH UND GRUNDPRINZIPIEN	27
8.2 PASSIVE ERKENNUNG UND ASSET DISCOVERY	27
8.3 KOMMUNIKATIONSANALYSE UND ANOMALIEERKENNUNG.....	27
8.4 RISIKO- UND SCHWACHSTELLENBEWERTUNG	28
8.5 REAKTION UND ESKALATION.....	28
8.6 DATENSCHUTZ KLINISCHER PROTOKOLLDATEN	28
8.7 INTEGRATION IN SIEM UND ABGRENZUNG ZU NDR.....	28
 <u>9. IMPLEMENTIERUNG UND TRANSITION</u>	 <u>29</u>
9.1 VORGEHENSMODELL UND PHASEN	29
9.2 ASSET- UND KRITIKALITÄTSKLASSIFIZIERUNG.....	30
9.3 LOGQUELLEN-, SENSORIK- UND INTEGRATIONSKATALOG	30
9.4 PLATTFORM-ÜBERNAHMEN ODER -MIGRATIONEN	30
9.5 ÜBERGANG DER SERVICEVERANTWORTUNG UND RAMP-UP-BETRIEB.....	31
9.6 TEST, VALIDIERUNG UND ABNAHME	32
9.7 SCHULUNG, WISSENSTRANSFER UND BETRIEBSHANDBUCH	32
9.8 HYPERCARE.....	33
 <u>10. MANAGED SERVICE / BETRIEBSMODELL.....</u>	 <u>34</u>
10.1 BETRIEBSORGANISATION UND SERVICEVERANTWORTUNG.....	34
10.2 EIGENSTÄNDIGE BEARBEITUNG UND BEGRENZUNG VON RÜCKFRAGEN.....	34
10.3 SECURITY MONITORING UND TRIAGE	34
10.4 METHODIK (MITRE ATT&CK).....	35
10.5 INCIDENT HANDLING	35
10.6 INVESTIGATION UND FORENSISCHE ANALYSE	35
10.7 REAKTION: STUFENMODELL	36
10.8 THREAT HUNTING.....	36
10.9 SOAR UND PLAYBOOKS	37
10.10 USE-CASE-, DETECTION- UND REGELPFLEGE	37
10.11 SCHWACHSTELLEN-SERVICE IM LAUFENDEN BETRIEB.....	37
10.12 INCIDENT- UND REQUEST-KLASSEN.....	38
10.13 SERVICE REQUESTS	38
10.14 CHANGE-MANAGEMENT.....	39
10.15 MAJOR INCIDENT UND KRISENMODUS.....	40

10.16 THREAT INTELLIGENCE	41
10.17 SERVICE HEALTH MONITORING UND DATENQUALITÄTSKONTROLLE	41
10.18 REPORTING UND SERVICE REVIEWS	41
10.19 PROBLEM MANAGEMENT UND KONTINUIERLICHE VERBESSERUNG	41
10.20 BUSINESS CONTINUITY UND NOTBETRIEB DES AUFTRAGNEHMERS.....	42
 11. PROZESS- UND TICKETINTEGRATION (SERVICENOW)	 43
11.1 INTEGRATION ALS GEMEINSAM GETRAGENE LEISTUNG	43
11.2 VORGANGSARTEN UND MINDESTINFORMATIONEN	43
11.3 STATUSSYNCHRONISATION UND ÜBERGABE AN GRUPPEN.....	44
11.4 ESKALATION UND SOFORTKOMMUNIKATION.....	44
11.5 ERSATZVERFAHREN	44
 12. SLA, REPORTING UND ESKALATION	 45
12.1 PRIORITÄTSMODELL	45
12.2 SLA-KENNZAHLEN.....	45
12.3 PLATTFORMVERFÜGBARKEIT	46
12.4 STATUS-UPDATES.....	46
12.5 ESKALATIONSMODELL	47
12.6 REPORTINGPFLICHTEN	47
 13. ROLLEN UND VERANTWORTLICHKEITEN	 48
13.1 ROLLEN DES AUFTRAGNEHMERS	48
13.2 ROLLEN DES AUFTRAGGEBERS.....	48
13.3 RACI-ÜBERSICHT (AUSZUG)	49
 14. EXIT MANAGEMENT	 50
14.1 AUSLÖSER UND GRUNDSÄTZE	50
14.2 EXIT-KONZEPT	50
14.3 ÜBERGABEOBJEKTE.....	50
14.4 DATENEXPORT UND LÖSCHUNG	51
14.5 LIZENZ- UND ÜBERGABERECHTE.....	51
14.6 ABNAHME DES EXIT-PROZESSES	51
14.7 UNTERSTÜTZUNG BEI DER TRANSITION AUF EINEN NACHFOLGEDIENSTLEISTER	51

1. Einleitung

1.1 Auftraggeber und KRITIS-Kontext

Das Universitätsklinikum Frankfurt / die Universitätsmedizin Frankfurt (nachfolgend „Auftraggeber“) ist ein Maximalversorger und Universitätsklinikum. Das UKF ist Betreiber einer Kritischen Infrastruktur im Sektor Gesundheit (§ 8a BSIG bzw. § 31 BSIG in der Fassung des NIS-2-Umsetzungsgesetzes). Die Leistungserbringung steht in unmittelbarem Zusammenhang mit Verfügbarkeit, Integrität und Vertraulichkeit klinischer und administrativer Prozesse sowie mit der Patientensicherheit.

Maßgebliche Rahmenwerke und regulatorische Bezugspunkte sind insbesondere:

- § 8a / § 30 / § 31 BSIG (Risikomanagementmaßnahmen für Betreiber kritischer Anlagen, Systeme zur Angriffserkennung)
- NIS-2-Richtlinie (EU) 2022/2555 in der nationalen Umsetzung (NIS-2-Umsetzungsgesetz, NIS2UmsuCG)
- Branchenspezifischer Sicherheitsstandard B3S „Medizinische Versorgung im Krankenhaus“ in der jeweils aktuell gültigen Fassung (derzeit v1.3, Eignungsfeststellung 03.11.2025)
- BSI-Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung (OH SzA)
- BSI Mindeststandard zur Protokollierung und Detektion von Cyberangriffen (orientierende Referenz)
- Modell zur Reife- und Umsetzungsgradbewertung (RUN) für SzA-Nachweise
- BSI IT-Grundschutz, ISO/IEC 27001
- DSGVO; MDR (EU) 2017/745 für medizinisch geprägte Systeme

Die zu beschaffenden Leistungen sollen das UKF in die Lage versetzen, die Anforderungen aus den vorgenannten Rahmenwerken nachweislich umzusetzen, insbesondere die Nachweispflichten gemäß § 8a Abs. 3 BSIG bzw. § 39 BSIG (NIS-2-Fassung) sowie die Meldepflichten nach § 32 BSIG ohne Medienbruch zu bedienen.

1.2 Ziel der Beschaffung

Gegenstand der Beschaffung ist ein Cybersecurity Managed Service mit fünf Leistungsbereichen in einem Los:

- SOC / SIEM – zentrale Detektion, Korrelation und Analyse
- NDR – netzwerkbasierte Erkennung und Anomalieanalyse
- Vulnerability Management – Scanning, Triage, Priorisierung, Remediation-Tracking
- EDR-Management – Betrieb der EDR-Plattform für ca. 11.200 Endpunkte
- IoMT-Security – passive Überwachung von ca. 5.000 vernetzten Medizingeräten

Die Vertragslaufzeit beträgt 60 Monate und beginnt mit dem Cut-over gemäß Kapitel 9.5. Der Vertrags- und Projektbeginn erfolgt spätestens am 01.02.2027. Der bestehende Managed-Service-Vertrag des Auftraggebers für die Leistungsbereiche SOC/SIEM und EDR-Management endet am 31.05.2027. Der Auftragnehmer muss die Serviceverantwortung im Mindestschutzzumfang gemäß

Kapitel 9.5 spätestens zum 31.05.2027 übernehmen (Cut-over). Der Übergang in den vollständigen Regelbetrieb (Go-Live) erfolgt nach Maßgabe des Vorgehensmodells gemäß Kapitel 9.1.

Ziele der Beschaffung sind insbesondere:

- Datenhoheit und Lizenzhoheit beim UKF (eigener SIEM-Tenant; BYOL für alle einbezogenen Plattformen)
- Bidirektionale, gemeinsam getragene Integration in das ITSM-System ServiceNow des UKF
- Flexibles Log-Onboarding ohne Einzelfreigabe oder Zusatzkosten als Bestandteil des Regelbetriebs
- Geordnete Übergabe bei Dienstleisterwechsel ohne Verlust von Daten, Lizenzen, Konfigurationen oder Betriebsartefakten
- 24x7-SOC-Betrieb mit deutschsprachiger Service-Steuerung, klaren Eskalationswegen und konkreten Handlungsempfehlungen; Rückfragen an das UKF sind auf fachlich erforderliche Fälle zu begrenzen

2. Ist-Zustand

2.1 Mengengerüst

Das nachfolgende Mengengerüst dient als Planungs- und Kalkulationsgrundlage. Es ist im Rahmen der Feinkonzeption durch den Auftragnehmer zu validieren und bei wesentlichen Abweichungen transparent fortzuschreiben.

Komponente	Menge	Einordnung
Active Directory	7	Authentifizierungslogs, Gruppenrichtlinien
Identity Provider (ADFS, Entra ID)	2	SSO, Federation
Privileged Access Management (Beyond Trust)	1	Privilegierte Zugriffe
Exchange Server	4	Mail- und Kommunikationslogs
Mailsecurity-Gateways (FortiMail)	2	Mail-Security-Kontext
Aktive Mailkonten	ca. 11.500	Benutzerkontext
Windows Server	ca. 750	SIEM-Logquelle, EDR-Scope
UNIX/Linux Server	ca. 350	SIEM-Logquelle, EDR-Scope nach Eignung
Clients / Workstations	ca. 7.000	EDR-Scope
VDI-Desktops (VM-Ware, Nutanix)	ca. 5.095	EDR-Scope nach technischer Eignung
EDR-Scope gesamt	ca. 11.200	Clients, Server, VDI
Core- / Perimeter-Firewalls	ca. 4	SIEM-Logquelle
IDS/IPS	ca. 4	Security Events
WAF	ca. 2	Web- und Applikationsschutz
NAC	ca. 2	Netzzugang, Geräte-/Identitätskontext
Router, Switches, Wireless	ca. 878	Infrastrukturereignisse
Access Points	1.208 (Plan: bis 3.400)	WLAN-Infrastruktur
DNS / DHCP	7 / 4	Namensauflösung, Adressvergabe
Proxy / VPN / Loadbalancer	2 / 1 / 2	Kommunikationsereignisse
Backup-Systeme	ca. 10	Wiederherstellungsdienste
Cloud-Applikationen (SIEM-Scope)	ServiceNow, SAP S/4HANA, M365 / Entra ID	Cloud-Audit-Logs
Vernetzte Medizingeräte / IoMT	ca. 5.000	Eigenständige Sonderdomäne

Komponente	Menge	Einordnung
IP-Adressen	ca. 21.000	Planungsgröße
Mitarbeitende	ca. 7.500	Organisatorischer Kontext
Standorte	Hauptcampus + externes Rechenzentrum	–

2.2 Bestehende Komponenten je Leistungsbereich

Die nachfolgenden Angaben beschreiben den Ist-Zustand zur Information der Bieter. Soweit nachfolgend nicht ausdrücklich abweichend geregelt, begründen sie keine Vorgabe für das künftig anzubietende Zielmodell. Die Anforderungen an den künftigen Cybersecurity Managed Service sind in den Kapiteln 3 bis 14 geregelt.

Leistungsbereich	Bestehende Lösung	Vertragslage
SOC / SIEM	Externer Managed-SOC-Betrieb SIEM-Lösung von Hunters	Vertragsende 31.05.2027
NDR	Vectra AI (On-Prem-Sensorik, Traffic-Spiegelung)	Lizenzanschluss endet 30.09.2027
Vulnerability Management	Tenable Security Center Plus (On-Premises-Konsole, Subscription IP Bands 21.000)	Lizenzanschluss endet 30.09.2027
EDR-Management	SentinelOne Singularity (Cloud)	Vertragsende 31.05.2027
IoMT-Security	Keine dedizierte Lösung im Einsatz	Erstbeschaffung im Rahmen dieses Verfahrens
ITSM des UKF	ServiceNow	Bestandssystem, dauerhaft im Einsatz

Für die NDR- und Vulnerability-Management-Plattformen kann der Bieter wahlweise die Fortführung der bestehenden Lösung oder eine alternative Lösung anbieten.

Für den Leistungsbereich EDR-Management gibt der Auftraggeber die zu betreibende EDR-Plattform vor. In Betracht kommt ausschließlich die Fortführung von SentinelOne Singularity oder der Betrieb von Microsoft Defender for Endpoint im Rahmen der Microsoft-Umgebung des Auftraggebers. Eine eigene, zusätzliche oder abweichende EDR-Plattform des Auftragnehmers ist nicht Gegenstand dieser Ausschreibung und darf nicht angeboten werden. Die domänenspezifischen Regeln stehen in den Kapiteln 5, 6 und 7.

2.3 Datengrundlage und Kalkulationsbasis

Für die Auslegung und Kalkulation der SIEM-Leistungen ist ein sicherheitsrelevantes Logvolumen von 400 GB pro Tag zugrunde zu legen. Das tatsächliche Volumen ist im Rahmen der Feinkonzeption anhand der anzubindenden Quellen, Filterlogiken und Datenqualitätsanforderungen zu validieren. Der Auftragnehmer ist im Rahmen der Implementierung verantwortlich für die Optimierung von

Logquellen und Filtern, um das Zielvolumen zu erreichen. Wesentliche Abweichungen sind zu dokumentieren und mit Auswirkungen auf Betrieb, Speicherung und Kosten transparent darzustellen.

3. Allgemeine Anforderungen

Die folgenden Anforderungen gelten leistungsbereichsübergreifend für alle Komponenten des Cybersecurity Managed Service. Sie werden in den Fachkapiteln nicht erneut wiederholt.

3.1 Datenhoheit und Datenhaltung

Die Hoheit über sicherheitsrelevante Daten des Auftraggebers verbleibt während der gesamten Vertragslaufzeit sowie nach Vertragsende beim UKF. Der Auftragnehmer darf diese Daten ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen verarbeiten.

- Alle sicherheitsrelevanten Daten, die im Rahmen des Managed Service verarbeitet oder erzeugt werden, verbleiben in der Hoheit des UKF. Dies umfasst insbesondere Rohdaten, normalisierte Ereignisse, Logdaten, Telemetriedaten, Incident-Informationen, Reports, Nachweise und betriebliche Dokumentationen.
- Die SIEM-Plattform wird in einem UKF-eigenen Tenant bzw. einer UKF-eigenen Instanz betrieben. Der Auftragnehmer bindet sich operativ an diesen Tenant bzw. diese Instanz an. Ein Betrieb unter Eigentum, ausschließlicher Verfügung oder alleiniger administrativer Kontrolle des Auftragnehmers ist ausgeschlossen. Siehe Kapitel 4.5.
- Sicherheitsrelevante Log-, Event-, Telemetrie- und Incident-Daten sind für mindestens 12 Monate aufzubewahren. Davon müssen mindestens 90 Tage als Hot Storage direkt und ohne Wiederherstellungsaufwand durchsuchbar sein. Die verbleibende Aufbewahrungszeit kann als Warm- oder Cold Storage realisiert werden, sofern eine Wiederherstellung und Bereitstellung innerhalb von 24 Stunden gewährleistet ist.
- Verarbeitung und Speicherung sicherheitsrelevanter Daten erfolgen ausschließlich innerhalb der EU bzw. des EWR. Bei Einsatz von Cloud- oder SaaS-Komponenten sind Datenarten, Datenflüsse, Verarbeitungsorte, Speicherorte, Unterauftragnehmer und etwaige Herstellerzugriffe im Angebot nachvollziehbar darzustellen.
- Kundenspezifische Konfigurationen, Integrationen, Parser, Normalisierungen, Feldzuordnungen, Dashboards, Reports, Use Cases, Detection-Regeln, Playbooks und sonstige Betriebsartefakte, die im Rahmen der Leistungserbringung speziell für das UKF erstellt, angepasst oder parametrisiert werden, sind dem UKF in dokumentierter und weiterverwendbarer Form bereitzustellen.
- Standardmethoden, Standard-Playbooks, generische Detection-Regeln, proprietäre SOC-Prozesse und interne Werkzeuge des Auftragnehmers bleiben beim Auftragnehmer. Dies darf jedoch nicht dazu führen, dass UKF-bezogene Daten, Konfigurationen, Dokumentationen oder Betriebsartefakte bei Vertragsende nicht vollständig übergeben oder weiterverwendet werden können.
- Daten, kundenspezifische Konfigurationen, Dokumentationen und servicebezogene Betriebsartefakte müssen in dokumentierten, marktüblichen und weiterverarbeitbaren Formaten exportierbar sein. Der Auftragnehmer stellt sicher, dass das UKF zu keinem Zeitpunkt in eine faktische Abhängigkeit gerät, die eine geordnete Übergabe, einen Dienstleisterwechsel oder einen Weiterbetrieb wesentlich erschwert.

3.2 Lizenzhoheit (BYOL)

- Für alle kundenbezogenen Plattform- und Produktlizenzen, die zur technischen Erbringung, Fortführung oder Übergabe der ausgeschriebenen Leistung erforderlich sind, ist das UKF als Lizenznehmer bzw. nutzungsberechtigte Organisation zu führen. Dies betrifft insbesondere SIEM, NDR, EDR, Vulnerability Management, IoMT-Plattformen sowie vergleichbare kundenbezogene Sicherheitsplattformen.
- Lizenzmodelle, bei denen die vorgenannten kundenbezogenen Lizenzen ausschließlich Bestandteil eines MSP-Vertrags des Auftragnehmers sind und bei Vertragsende nicht auf das UKF übertragen oder durch das UKF weitergenutzt werden können, sind ausgeschlossen.
- Nicht hiervon umfasst sind rein interne Werkzeuge des Auftragnehmers zur eigenen Leistungserbringung, insbesondere interne SOC-Werkzeuge, Standard-Playbooks, generische Regelwerke, proprietäre Analysemethoden, Threat-Intelligence-Aufbereitungen oder interne Automatisierungsbausteine, sofern diese nicht als kundenbezogene Plattformbestandteile betrieben werden und hierdurch keine faktische Abhängigkeit des UKF entsteht.
- Lizenzkosten für kundenbezogene Plattform- und Produktlizenzen sind im Preisblatt separat und transparent vom Managed-Service-Anteil auszuweisen. Einmalige, laufende und nutzungsabhängige Lizenzkosten sind getrennt darzustellen.
- Auf Anforderung ist nachzuweisen, dass das UKF als Lizenznehmer bzw. nutzungsberechtigte Organisation geführt wird.

Für den Leistungsbereich EDR gilt ergänzend: Sofern der Auftraggeber Microsoft Defender for Endpoint im Rahmen bestehender oder künftig beschaffter Microsoft-Lizenzierung bereitstellt, sind hierfür keine EDR-Produktlizenzen durch den Auftragnehmer zu kalkulieren. Sofern der Auftraggeber die Fortführung von SentinelOne Singularity wählt und die Lizenzbereitstellung über den Auftragnehmer abrufen möchte, ist diese ausschließlich als optionale Position gemäß Preisblatt auszuweisen. In beiden Fällen verbleiben Lizenz-, Nutzungs- und Datenhoheit beim Auftraggeber.

3.3 Klinischer Sonderkontext und Patientensicherheit

- In medizinisch-kritischen Netzwerksegmenten sind ausschließlich passive, nicht-invasive Erfassungsmethoden zulässig. Aktive Scans sowie automatisierte Blocking-, Quarantäne- oder Isolationsmaßnahmen sind ausgeschlossen.
- Sicherheitsrelevante Reaktionen in medizinisch-kritischen Segmenten erfolgen ausschließlich nach dem Human-in-the-Loop-Prinzip mit Freigabe durch den Auftraggeber.
- Patientensicherheit hat Vorrang vor automatisierter technischer Reaktion.

3.4 Anonymisierung klinischer Protokolldaten

- Klinische Kommunikationsprotokolle (insbesondere DICOM, HL7 v2/v3, FHIR) enthalten regelmäßig Patientenidentifikationsinformationen nach Art. 9 Abs. 1 DSGVO. Eine Übertragung dieser Rohdaten in Cloud- oder Drittumgebungen ist technisch auszuschließen.
- Sofern eine Verarbeitung klinischer Protokolldaten erforderlich ist, sind diese vor jeder Übertragung in Cloud- oder Drittumgebungen lokal in der On-Premises-Komponente zu

anonymisieren oder zu pseudonymisieren. Eine Data-Flow-Dokumentation mit Feldliste ist im Angebot vorzulegen.

- Die Wirksamkeit der Anonymisierungsmechanismen ist im Rahmen der Abnahme technisch nachzuweisen.

3.5 Flexibles Onboarding und Erweiterbarkeit

- Die Anbindung neuer Logquellen, Datenquellen, Sensoren, Cloud-Dienste, Netzsegmente und Sicherheitskomponenten muss Bestandteil des Regelbetriebs sein. Sie löst keine Einzelbeauftragung und keine Zusatzkosten aus, soweit es sich um Standardquellen mit verfügbarem Parser handelt.
- Die angebotene Architektur muss steigende Datenmengen, neue Quellen und veränderte Infrastrukturen aufnehmen können, ohne dass der laufende Sicherheitsbetrieb strukturell gefährdet wird (z. B. Rechenzentrumswechsel, Firewall-Wechsel, Netzbauten).
- Die Aufnahme nicht-standardisierter Quellen, für die kein Parser verfügbar ist und die daher Parser-Engineering erfordern, wird nach den im Preisblatt ausgewiesenen Stundenverrechnungssätzen abgerechnet. Der Auftragnehmer weist den erforderlichen Aufwand vor Beginn aus und holt die Freigabe des Auftraggebers ein.

3.6 Herstelleroffenheit

- Anforderungen sind funktional und herstellerneutral formuliert; sie sind grundsätzlich durch funktional gleichwertige Lösungen erfüllbar, soweit in dieser Leistungsbeschreibung nicht ausdrücklich abweichend geregelt. Dies gilt nicht für ausdrücklich bezeichnete Bestandssysteme oder vom Auftraggeber vorgegebene Plattformen, insbesondere für die EDR-Plattform gemäß Kapitel 7.2.

3.7 Bidirektionale ServiceNow-Integration als gemeinsam getragene Leistung

Die bidirektionale Integration zwischen den Systemen des Auftragnehmers und dem ITSM-System ServiceNow des UKF wird von beiden Vertragsparteien getragen. Sie ist keine einseitige Leistung des Auftragnehmers, sondern setzt aktive Mitwirkung des UKF voraus.

- Der Auftragnehmer muss sein Vorgangsmanagement bidirektional in ServiceNow integrieren. Detailanforderungen siehe Kapitel 11.
- Die technischen, organisatorischen und prozessualen Detailanforderungen an Schnittstellen, Mapping, Tests, Inbetriebnahme, Ersatzverfahren und laufenden Betrieb der Integration sind in Kapitel 11 geregelt. Die Verantwortlichkeiten beider Seiten sind in der RACI-Matrix gemäß Kapitel 13 festgelegt.

3.8 Sprache und Service Delivery

- Die operative Service-Kommunikation, Eskalation, Regelkommunikation und Dokumentation gegenüber dem UKF erfolgen in deutscher Sprache. Ergänzende Anforderungen an Service Delivery Management, SOC-Betrieb und Hotline sind in Kapitel 10 geregelt

4. Leistungsbereich SOC / SIEM

4.1 Geltungsbereich und Datenquellen

Die SIEM-Plattform bildet die zentrale Detektions-, Korrelations- und Nachweisebene des gesamten Cybersecurity Managed Service. Sie nimmt sicherheitsrelevante Ereignisse aus den nachfolgend beschriebenen Quellen auf, normalisiert und reichert sie an, korreliert sie zu auswertbaren Sicherheitslagen und stellt die Basis für SOC-Betrieb, Reporting und KRITIS-Nachweisführung bereit.

In den SIEM-Scope einzubinden sind mindestens:

- Identitätsdienste: Active Directory, ADFS, Entra ID, Privileged Access Management
- Server: Windows-, UNIX- und Linux-Server
- Endpunkte: Clients, Workstations und VDI-Systeme
- E-Mail: Mailserver und Mailsecurity-Gateways
- Netzwerk- und Sicherheitskomponenten: Firewalls(Palo Alto, Juniper, FortiGate), IDS/IPS, WAF, NAC, Proxy, DNS, DHCP, VPN, Loadbalancer
- Sicherheitsrelevante Ereignisse aus Switching-, Routing- und WLAN-Komponenten
- Cloud-Dienste: M365 / Entra ID, ServiceNow, SAP S/4HANA
- Erkenntnisse der übrigen Leistungsbereiche: EDR, NDR, IoMT-Plattform, Vulnerability Management
- Weitere sicherheitsrelevante Fach- und Plattformsysteme nach Festlegung in der Feinkonzeption

Die konkrete Quellenliste, Anschlussart und Priorisierung wird im Integrationskatalog (Kap. 9.3) gepflegt.

- Die SIEM-Plattform muss alle vorgenannten Quellenarten aufnehmen, normalisieren und korrelieren können.
- Für Auslegung und Kalkulation ist ein sicherheitsrelevantes Logvolumen von 400 GB/Tag zugrunde zu legen. Der Auftragnehmer ist im Rahmen der Implementierung für die Optimierung von Logquellen und Filtern zur Erreichung dieses Zielvolumens verantwortlich.
- Die Aufnahme neuer Quellen über marktübliche Verfahren (Syslog, Webhooks, API, Agent, Forwarder, dateibasiert sowie native Cloud- und Storage Schnittstelle) ist Bestandteil des Regelbetriebs und löst keinen Sonderaufwand und keine Zusatzbeauftragung aus, soweit ein Standard-Parser verfügbar ist.
- Bei der Auswahl und Priorisierung der Logquellen orientiert sich der Auftragnehmer am BSI-Mindeststandard zur Protokollierung und Detektion von Cyberangriffen sowie an der BSI-Orientierungshilfe SzA. Abweichungen sind in der Feinkonzeption zu begründen.

4.2 Datenaufnahme, Parsing und Anreicherung

Eingehende Daten werden geparkt, in ein einheitliches Datenmodell normalisiert und anschließend mit Asset-, Identitäts-, Schwachstellen- und Bedrohungskontext angereichert. Datenqualität und Vollständigkeit der Anlieferung sind kontinuierlich zu überwachen.

-
- Die Plattform muss Syslog-, API-, agenten-, forwarder- und dateibasierte Verfahren der Datenaufnahme unterstützen.
 - Logs aus Individualsoftware und krankenhausspezifischen Anwendungen müssen einbindbar sein. Erforderliche Parser, Normalisierungen und Mappings setzt der Auftragnehmer in der Feinkonzeption um.
 - Unterbrechungen oder Qualitätsmängel kritischer Logquellen sind innerhalb von 30 Minuten nach Feststellung zu melden und im Service-Health-Bericht (Kap. 12.6) auszuweisen.

4.3 Use Cases, Detection Engineering und Threat Intelligence

Detection Engineering ist nicht eine einmalige Aufbauleistung, sondern ein kontinuierlicher Prozess. Der Auftragnehmer bringt einen Standard-Use-Case-Katalog ein. UKF-spezifische Anpassungen, neue Detection-Regeln und Tuning-Maßnahmen sind im Betrieb zu dokumentieren und fortzuschreiben.

- Use Cases müssen Identitäts-, Endpunkt-, Netzwerk-, Cloud- und Infrastrukturereignisse korrelieren und Vulnerability- sowie IoMT-Kontext einbeziehen.
- Detektionslogiken sind nachvollziehbar dem MITRE ATT&CK Framework zuzuordnen, soweit fachlich anwendbar. Der Auftragnehmer hat im Rahmen der Feinkonzeption und danach mindestens jährlich eine Abdeckungsanalyse der umgesetzten Detection-Use-Cases gegen MITRE ATT&CK oder ein fachlich gleichwertiges Framework vorzulegen. Die Analyse muss darstellen, welche Taktiken und Techniken durch vorhandene Logquellen, Telemetriedaten und Detection-Regeln abgedeckt werden, wo erkennbare Lücken bestehen und welche Maßnahmen zur Verbesserung der Detection-Abdeckung empfohlen werden. Reporting und Incident-Dokumentation enthalten entsprechende Verweise (siehe Kapitel 10 und 12).
- Healthcare- und KRITIS-spezifische Bedrohungslagen sowie aktiv ausgenutzte Schwachstellen sind regelmäßig in die Detektionslogik aufzunehmen.
- Der Auftragnehmer hat KI-gestützte bzw. hochautomatisierte Angriffsmuster im Detection Engineering, in der Threat-Intelligence-Verarbeitung und im Threat Hunting angemessen zu berücksichtigen. Die hierfür erforderlichen Erkennungs-, Analyse- und Reaktionsfähigkeiten müssen in den SOC-/SIEM-Betrieb integriert oder über dokumentierte Schnittstellen integrierbar sein.
- Detection-Regeln, Korrelationen und Schwellwerte werden mindestens quartalsweise sowie anlassbezogen überprüft und fortgeschrieben.

Ergänzend zur regelbasierten Detektion erwartet das UKF verhaltensbasierte Auswertungen für Identitäten und Konten:

- Verhaltensbasierte Anomalieerkennung für Benutzer- und Dienstkonto (UEBA) muss verfügbar sein, insbesondere zur Erkennung kompromittierter Konten, untypischer Anmeldeuster, ungewöhnlicher Zugriffe auf sensitive Daten und Privilege-Escalation. Die Bewertung erfolgt risikobasiert und mit nachvollziehbarer Begründung.
- Der Auftragnehmer stellt einen Threat-Intelligence-Feed mit IoCs, TTPs und KRITIS-/Healthcare-relevanten Entwicklungen als Bestandteil des Managed Service bereit. Eine separate Lizenzierung durch das UKF ist nicht zulässig.

4.4 Alarmierung und Analysetiefe

Alarme verlassen die SIEM-Plattform nicht als technische Rohmeldung, sondern erst nach fachlicher Bewertung durch das SOC. Sie enthalten mindestens die folgenden Inhalte, damit eine Bearbeitung durch das UKF ohne Rückfrage möglich ist:

Inhalt	Beschreibung
Auslösender Use Case	Detektionslogik, betroffene Datenquelle, Konfidenz, MITRE-Bezug soweit anwendbar
Betroffenes Asset / Identität	System, Benutzer, Konto, Dienst, Kommunikationsbeziehung
Zeitlicher Verlauf	Erkennungszeitpunkt, Eskalation, relevante Ereigniskette
Bewertung	Priorität, fachliche Einschätzung, Begründung
Kontext	Erkannte IoCs, bekannte Schwachstellen, NDR- bzw. EDR-Bezug
Empfehlung	Konkreter nächster Bearbeitungsschritt, ggf. Freigabebedarf

- Eine technische Alarmweiterleitung ohne fachliche Einordnung erfüllt diese Anforderung nicht.

4.5 Plattformbetrieb, Plattformsicherheit und Zugriff

Die SIEM-Plattform wird in einem UKF-eigenen Tenant bzw. einer UKF-eigenen Instanz betrieben. Datenhaltung, Lizenzhoheit und EU-Datenverarbeitung sind im Querschnittskapitel 3 geregelt.

- Kundenspezifisch für das UKF erstellte, angepasste oder parametrisierte Use Cases, Korrelationsregeln, Auswertungen und Reports sind gemäß Kapitel 3.1 zu dokumentieren, exportierbar bereitzustellen und für Betrieb, Prüfung und Providerwechsel weiterverwendbar zu machen.
- Benannte Mitarbeitende des UKF erhalten lesenden und auswertenden Zugriff auf die Plattform (Such-, Dashboard-, Report-Funktionen). Schreibender oder konfigurierender Zugriff bleibt grundsätzlich beim Auftragnehmer; gesonderte Berechtigungen für UKF-Rollen werden im Berechtigungskonzept festgelegt.
- Der Plattformzugriff erfolgt rollenbasiert (RBAC) und ist mit Multi-Faktor-Authentifizierung abzusichern. Privilegierte administrative Zugriffe werden vollständig protokolliert und der Audit-Trail ist UKF-seitig einsehbar.
- Die Plattform selbst ist nach Stand der Technik zu härten (Patchstand, Konfigurationsstandards, Schwachstellen-Management der Plattformkomponenten). Sicherheitsvorfälle, die die Plattform selbst betreffen, sind dem UKF unverzüglich zu melden.
- Für die SIEM-Plattform sind ergänzend die Anforderungen an Service Health Monitoring, Datenqualitätskontrolle, Plattformverfügbarkeit und Reporting gemäß Kapitel 10.17, 12.3 und 12.6 einzuhalten. Der Auftragnehmer hat sicherzustellen, dass Störungen der Plattform, der Datenverarbeitung oder wesentlicher Integrationskomponenten hinsichtlich ihrer Auswirkungen auf Detektion, Analyse und Nachweisfähigkeit bewertet und dokumentiert werden.

4.6 Integration mit den übrigen Leistungsbereichen

Die SIEM-Plattform führt sicherheitsrelevante Ereignisse und Bewertungen aus den Leistungsbereichen zusammen. Erkenntnisse aus NDR, EDR, Vulnerability Management und IoMT-Security werden hier zusammengeführt und gemeinsam ausgewertet. Die fachliche Spezialfunktion der jeweiligen Domäne verbleibt bei deren Plattform; das SIEM dupliziert keine domänenspezifische Logik.

- Für IoMT-bezogene Ereignisse werden ausschließlich sicherheitsrelevante Alarme, Bewertungen und Kontextdaten in das SIEM überführt. Klinische Protokolldaten (DICOM, HL7, FHIR) werden nicht ungefiltert in das SIEM übertragen. Eine Verarbeitung oder Weitergabe erfolgt ausschließlich unter Beachtung der Anonymisierungs- und Pseudonymisierungsanforderungen gemäß Kapitel 3.4 und Kapitel 8.6.

4.7 Beitrag zum SzA-Nachweis

Die SIEM-Plattform und der zugehörige SOC-Service sind Bestandteil des Systems zur Angriffserkennung des UKF im Sinne § 8a Abs. 1a / § 30 BSIG.

- Der Auftragnehmer dokumentiert Datenquellen, Use Cases, Detektionslogiken, Eskalations- und Betriebsprozesse so, dass das UKF diese für den SzA-Nachweis nach BSI-OH-SzA und RUN-Modell verwenden kann. Die Dokumentation ist mindestens auf RUN-Reifegrad 2 zum Go-Live und auf RUN-Reifegrad 3 spätestens 12 Monate nach Betriebsaufnahme ausgerichtet. Abweichungen sind zu benennen, zu begründen und mit Maßnahmen zu hinterlegen.

5. Leistungsbereich NDR

5.1 Geltungsbereich und Zielbild

Der Leistungsbereich NDR umfasst die netzwerkbasierte Erkennung, Analyse und Bewertung sicherheitsrelevanter Kommunikationsbeziehungen, Anomalien und Angriffsmuster. Erkenntnisse fließen in das SIEM und den operativen SOC-Prozess ein. Im Zusammenspiel mit EDR adressiert NDR Angriffsphasen, die auf Endpoint-Ebene nur eingeschränkt sichtbar sind – insbesondere laterale Bewegungen, verdeckte Kommunikationskanäle, Datenabflüsse und Aktivitäten auf Geräten ohne Agenten.

5.2 Sensorik und Erfassung

- Die Lösung muss Netzwerkverkehr passiv erfassen (Port-Mirroring, TAPs, SPAN-/Mirror-Ports, NetFlow/IPFIX oder funktional gleichwertige Verfahren). Die konkrete Sensorplatzierung wird in der Feinkonzeption festgelegt.
- Die Netzabdeckung muss Ost-West- und Nord-Süd-Kommunikation, zentrale Firewall- und Routing-Punkte sowie Segmente erhöhter Kritikalität angemessen berücksichtigen.
- Sensoren an zentralen Erfassungspunkten sind so auszulegen, dass Ausfälle einzelner Komponenten nicht zu längeren Erfassungslücken führen. Konkrete Verfügbarkeitskonzepte (Redundanz, Failover, Monitoring) werden in der Feinkonzeption festgelegt.
- Änderungen in Netzwerkarchitektur, Rechenzentrumsstrukturen, Standortanbindungen oder Segmentierungslogiken sind über die definierten Change- und Betriebsprozesse zeitnah aufzunehmen, ohne dass es zu längeren Erfassungslücken kommt.

5.3 Detektion und Analysefähigkeiten

Die Lösung muss mindestens folgende Erkennungsfähigkeiten bereitstellen:

- verdächtige interne Bewegungsmuster und laterale Bewegungen
- Command-and-Control-Kommunikation und verdeckte Kanäle, einschließlich Beaconing-Mustern
- verdächtige Datenabflüsse und Exfiltrationsmuster
- DNS-Tunneling sowie verschlüsselte DNS-Auflösung (DoH/DoT) als potenzielle Verschleierungskanäle
- Verstöße gegen definierte Kommunikations- oder Segmentierungslogiken
- ungewöhnliche Kommunikationspartner, neue Kommunikationsbeziehungen, geografisch auffällige Ziele
- Auffälligkeiten an kritischen Servern, Identitätsdiensten und Sicherheitskomponenten
- Scan- und Reconnaissance-Aktivitäten innerhalb des UKF-Netzes

Verschlüsselter Datenverkehr ist ohne TLS-Termination zu analysieren. Maßgeblich sind dabei metadatenbasierte Verfahren wie TLS-Fingerprinting (z. B. JA3/JA4), Verbindungsprofile und Verhaltensanalysen.

- Die Lösung muss Verhaltens- und Baseline-Modelle für Hosts, Subnetze und Kommunikationsbeziehungen aufbauen und kontinuierlich pflegen.
- Es sind nachweislich wirksame Mechanismen zur Reduktion von False Positives einzusetzen (z. B. Baseline Learning, kontextbezogene Korrelation, Tuning-Workflow).
- Asset-, Identitäts-, Segmentierungs-, Schwachstellen- und SIEM-Kontextinformationen sind zur Priorisierung und Bewertung heranzuziehen, soweit verfügbar.
- Eine User-zu-IP-Zuordnung (Identity Tracking) für die Kontextanreicherung von Alarmen wird erwartet, soweit es die Datenlage technisch zulässt (DHCP, AD-Logs, NAC).

5.4 Datenhaltung und Investigation-Fähigkeit

- Netzwerk-Metadaten (Flow-Records, DNS-, HTTP-, TLS-Metadaten) müssen mindestens 90 Tage online für Analyse, Threat Hunting und Investigations verfügbar sein. Eine darüberhinausgehende Speicherung gemäß Querschnittskapitel 3.1 ist möglich, soweit fachlich erforderlich.
- Eine On-Demand-Erfassung von Paketdaten (PCAP) für gezielte Untersuchungen muss möglich sein. Speicherort, Aufbewahrungsfristen und Zugriffsrechte sind in der Feinkonzeption festzulegen.

5.5 Plattform- und Lizenzmodell

Die im Ist-Zustand eingesetzte NDR-Lösung Vectra AI verfügt über einen Vertrags- und Lizenzanschluss bis zum 30.09.2027. Der Bieter kann wählen, wie die NDR-Leistung erbracht wird; eine bestimmte Lösung wird nicht vorgegeben.

- Sofern der Bieter die Fortführung der bestehenden NDR-Lösung vorsieht, beschreibt er Lizenzanschluss, Sensorbetrieb, SIEM-Integration, Migration der Sensorinfrastruktur bei Rechenzentrumsänderungen und die Übergabe in den Cybersecurity Managed Service. Lizenzen werden im BYOL-Modell auf das UKF übertragen oder neu auf das UKF beschafft.
- Sofern der Bieter eine alternative NDR-Lösung vorsieht, legt er ein vollständiges Migrationskonzept vor mit Rollout, Parallelbetrieb, Ablösung der bestehenden Sensorik, Schnittstellenintegration, Test- und Abnahmeverfahren sowie Maßnahmen zur Vermeidung von Schutzlücken.
- In beiden Varianten verfügt das UKF über die erforderlichen kundenbezogenen Nutzungs-, Lizenz-, Daten- und Übergaberechte. Ein späterer Wechsel des Managed-Service-Dienstleisters darf nicht zu Verlust von kundenbezogenen Lizenzen, Konfigurationen, Sensordaten, Betriebsartefakten oder Übergaberechten führen.
- Die mit der gewählten Vorgehensweise verbundenen Implementierungs-, Migrations-, Lizenz- und Betriebskosten sind im Preisblatt entsprechend der Preisblattstruktur auszuweisen.

5.6 Integration in SIEM und Reaktionsfähigkeit

- Alarme, Bewertungen, Netzwerkmetadaten und Kontextinformationen müssen in einem dokumentierten, marktüblichen Format an das SIEM übergeben werden (Syslog, CEF, LEEF,

REST-API). Eine native API-Integration zwischen NDR-Plattform und SIEM-Plattform wird erwartet.

- Aus den Erkenntnissen der NDR-Plattform müssen Reaktionen über bestehende Sicherheitskomponenten unterstützt werden können – insbesondere die Auslösung von Firewall- oder NAC-Maßnahmen (z. B. Blockierung schädlicher Ziele, Quarantäne kompromittierter Endpunkte). Konkrete Aktionen, Freigabewege und Eskalationspfade werden in den Playbooks festgelegt; die Einschränkungen für medizinisch-kritische Segmente nach Querschnittskapitel 3.3 gelten unverändert.

6. Leistungsbereich Vulnerability Management

6.1 Geltungsbereich und Zielbild

Gefordert ist ein vollständiger, prozessual hinterlegter Vulnerability-Management-Service – kein reiner Plattformbetrieb. Der Service umfasst Discovery und Scanning, fachliche Triage, kontextbezogene Priorisierung, Maßnahmenübergabe an die UKF-Betriebsgruppen und Remediation-Tracking bis zur dokumentierten Schließung. Die Übergabe unbewerteter Scanner-Exporte oder reiner CVE-Listen erfüllt diese Anforderungen ausdrücklich nicht.

Im Ist-Zustand wird die Plattform Tenable Security Center Plus eingesetzt; der bisherige Dienstleister erbringt ausschließlich Plattformbetrieb. Die fachlichen Servicebestandteile – Triage, Priorisierung und Tracking – werden mit dieser Beschaffung neu eingeführt.

- Der Geltungsbereich umfasst Server- und Betriebssystemplattformen, Clients und VDI-Systeme, Netzwerk- und Sicherheitskomponenten, Webserver und exponierte Webanwendungen, Cloud-Dienste und Cloud-Konfigurationen, Identitätsdienste sowie sicherheitsrelevante Anwendungen. Der konkrete Scope wird in der Feinkonzeption festgelegt.
- IoMT-spezifische Schwachstellen sind in Kapitel 8 geregelt. IoMT-Risikoinformationen werden jedoch in das gesamthafte Risikobild integriert.

6.2 Plattform- und Lizenzmodell

Die im Ist-Zustand eingesetzte Vulnerability-Management-Plattform Tenable Security Center Plus (On-Premises-Konsole, Subscription IP Bands 21.000) verfügt über einen Lizenzanschluss bis zum 30.09.2027. Der Bieter kann wählen, wie die Vulnerability-Management-Leistung erbracht wird.

- Sofern der Bieter die Fortführung der bestehenden Plattform vorsieht, beschreibt er Lizenzanschluss, Übernahme der bestehenden Konfigurationen, Scan-Profile und Asset-Daten, Integration in den Cybersecurity Managed Service sowie Übergabe in den Regelbetrieb. Lizenzen werden im BYOL-Modell auf das UKF übertragen oder neu auf das UKF beschafft.
- Sofern der Bieter eine alternative Plattform vorsieht, legt er ein Migrationskonzept vor mit Rollout, Parallelbetrieb, Übernahme oder Neuaufbau von Scan-Profilen, Asset-Inventarübergabe und Maßnahmen zur Vermeidung von Erkennungslücken.
- In beiden Varianten verfügt das UKF über die erforderlichen Nutzungs-, Lizenz-, Daten- und Übergaberechte.

6.3 Scanning, Discovery und Datenerhebung

- Authenticated Scans, agenten- oder API-basierte Erhebung sowie der Import vorhandener Scan-Ergebnisse müssen unterstützt werden.
- Das Scanning ist so zu gestalten, dass eine kontinuierliche Sichtbarkeit auf den aktuellen Schwachstellenstand entsteht – nicht nur ein punktueller Scan-Zyklus. Asset-Discovery und das Erkennen neu aufgetauchter, nicht erwarteter Systeme gehören zum Leistungsumfang.

- Für die im UKF betriebenen Webserver und exponierten Webanwendungen ist eine geeignete Webanwendungsprüfung Bestandteil des Service. Tiefe und Frequenz werden in der Feinkonzeption festgelegt.
- Für die genutzten Cloud-Dienste (insb. M365 / Entra ID) ist eine grundlegende Konfigurations- und Härtingsprüfung gegen anerkannte Benchmarks (z. B. CIS, herstellereigene Best Practices) Bestandteil des Service. Auswertbare Befunde fließen in die Priorisierung ein.
- Scan-Profile, Scan-Zyklen, Zugangsdaten, Wartungsfenster und Ausnahmen werden vom Auftragnehmer geplant, verwaltet und im Betriebshandbuch dokumentiert.
- Für medizinisch geprägte Systeme gelten die gesonderten Anforderungen aus Kapitel 8 (passive Erfassung, keine aktiven Scans).

6.4 Triage, Kontextpriorisierung und Handlungsempfehlungen

Die Priorisierung darf sich nicht ausschließlich auf den CVSS-Wert stützen. Maßgeblich ist eine kombinierte Bewertung folgender Faktoren:

- CVSS-Bewertung und technische Schwere
- aktive Ausnutzung und verfügbare Exploits (Threat Intelligence, KEV-Listen)
- Asset-Kritikalität und klinische bzw. administrative Rolle des Systems
- Netzwerk-Erreichbarkeit, Exponiertheit, Segmentierungs- und Firewall-Situation
- vorhandene Kompensationsmaßnahmen
- potenzielle Auswirkungen auf Betrieb, Sicherheit oder klinische Prozesse
- Im Onboarding wird gemeinsam mit dem UKF eine Asset- und Kritikalitätsklassifizierung erarbeitet (siehe Kapitel 9.2). Sie ist die verbindliche Grundlage für die Priorisierung.
- Der Auftragnehmer überführt Schwachstellenmengen in priorisierte, begründete und handhabbare Maßnahmenpakete. Handlungsempfehlungen enthalten Patch-, Workaround- oder Kompensationshinweise, betroffene Systeme und Verantwortliche, Begründung der Priorisierung sowie Vorschläge zur Bündelung nach Systemgruppe oder Wartungsfenster.

6.5 Remediation-Tracking, Validierung und Risikoakzeptanz

- Erkannte und priorisierte Schwachstellen müssen bis zur Bearbeitung, Risikoakzeptanz oder dokumentierten Schließung nachverfolgt werden. Statuswerte umfassen mindestens: neu erkannt, in Bewertung, priorisiert, übergeben, in Bearbeitung, behoben, kompensiert, akzeptiert, zurückgestellt, erneut erkannt, geschlossen.
- Nach Abschluss einer Patching- oder Kompensationsmaßnahme ist die Wirksamkeit über einen Folgescan oder eine gleichwertige Prüfung zu validieren. Der Validierungsstand wird im Tracking dokumentiert.
- Eine Risikoakzeptanz darf nicht durch den Auftragnehmer allein erfolgen. Der Auftragnehmer bewertet, dokumentiert und schlägt vor; die Entscheidung verbleibt beim UKF.
- Die Patch-Umsetzung erfolgt durch den UKF-IT-Betrieb. Der Auftragnehmer ist verantwortlich für Bewertung, Priorisierung, Übergabe, Nachverfolgung, Validierung und Reporting.

6.6 Integration und Reporting

- Schwachstelleninformationen müssen so bereitgestellt werden, dass sie in SIEM, Incident-Bewertung, Detection Engineering und Threat Hunting genutzt werden können.
- Schwachstellenberichte werden monatlich (operativ) und quartalsweise (strategisch) bereitgestellt. Aktiv ausgenutzte oder besonders kritische Schwachstellen werden anlassbezogen kommuniziert.

7. Leistungsbereich EDR-Management

7.1 Geltungsbereich

Der Leistungsbereich umfasst Betrieb, Überwachung, Pflege und fachliche Einbindung der EDR-Plattform. Für Planung und Kalkulation ist von ca. 11.200 EDR-relevanten Endpunkten auszugehen (Clients, Workstations, Server, VDI-Systeme).

- Medizinisch geprägte Systeme und vernetzte Medizingeräte sind nicht Bestandteil des EDR-Scopes; für diese gelten die Anforderungen aus Kapitel 8.
- Mobile Endgeräte (Smartphones, Tablets) sind nicht Bestandteil dieses Leistungsbereichs. Die konzeptionelle Anschlussfähigkeit für eine spätere Integration eines Mobile-Threat-Defense-Service wird jedoch nicht ausgeschlossen.

7.2 Plattform- und Lizenzmodell

Im Ist-Zustand ist SentinelOne Singularity (Cloud) als EDR-Plattform im Einsatz. Im Projektzeitraum kann der Auftraggeber entscheiden, ob SentinelOne Singularity fortgeführt oder Microsoft Defender for Endpoint als EDR-Plattform genutzt wird.

- Der Auftragnehmer hat den EDR-Managed-Service für die vom Auftraggeber benannte EDR-Plattform zu erbringen. Zulässig sind ausschließlich der Betrieb und die fachliche Einbindung von SentinelOne Singularity oder der Betrieb und die fachliche Einbindung von Microsoft Defender for Endpoint im Rahmen der Microsoft-Umgebung des Auftraggebers.
- Eine eigene, zusätzliche oder abweichende EDR-Plattform des Auftragnehmers ist nicht Gegenstand dieser Ausschreibung und darf nicht angeboten werden.
- Der Auftragnehmer muss nachweisen, dass er beide vorgenannten Betriebsvarianten fachlich und organisatorisch beherrscht. Dies umfasst insbesondere Betrieb, Policy- und Konfigurationsmanagement, Agentenüberwachung, Alarmbewertung, Response-Unterstützung, SIEM-Integration, Reporting, Übergabe in ServiceNow sowie Mitwirkung an der Weiterentwicklung von Use Cases und Detection-Regeln.
- Der Auftraggeber legt spätestens acht Wochen vor dem Cut-over gemäß Kapitel 9.5 fest, welche der beiden Plattformen durch den Auftragnehmer zu betreiben ist. Bis zu dieser Festlegung hat der Auftragnehmer seine Planung so auszugestalten, dass beide Szenarien ohne strukturellen Neuaufbau des Managed Service abbildbar sind.
- Die für die Fortführung von SentinelOne Singularity erforderlichen Lizenzen sind vom Auftragnehmer im Preisblatt zu bepreisen und Bestandteil der wertungsrelevanten EDR-Basisleistung. Die Lizenzierung erfolgt im BYOL-Modell; der Auftraggeber ist als Lizenznehmer bzw. nutzungsberechtigte Organisation zu führen.
- Sofern der Auftraggeber Microsoft Defender for Endpoint vorgibt, sind die hierfür erforderlichen Microsoft-Produktlizenzen nicht Bestandteil der wertungsrelevanten EDR-Basisleistung, soweit sie durch den Auftraggeber bereitgestellt werden.
- Die optionale Transition von SentinelOne Singularity zu Microsoft Defender for Endpoint ist als gesondert abrufbare optionale Leistung im Preisblatt auszuweisen. Sie umfasst mindestens

Planung, Pilotierung, Rolloutsteuerung, Policy- und Regelüberführung, Anpassung von Detection- und Response-Prozessen, Test, Dokumentation und Betriebsübergabe.

- Der Parallelbetrieb beider EDR-Plattformen während der Rollout-Wellen ist von der Transition zu trennen und als gesondert abrufbare optionale Leistung je Monat im Preisblatt auszuweisen. Er umfasst den gleichzeitigen Betrieb und die Alarmbearbeitung auf beiden Plattformen; die einmaligen Projektleistungen der Transition sind darin nicht enthalten.
- Der wertungsrelevante EDR-Basispreis umfasst den Betrieb der vom Auftraggeber benannten EDR-Plattform einschließlich der Lizenzen für SentinelOne Singularity; der Angebotswertung liegt die Fortführung von SentinelOne Singularity zugrunde. Die Transition zu Microsoft Defender for Endpoint und ein hierfür erforderlicher Parallelbetrieb sind optionale Positionen; sie werden nur nach gesonderter Entscheidung des Auftraggebers abgerufen und sind nicht Bestandteil des wertungsrelevanten EDR-Basispreises. Entscheidet sich der Auftraggeber für Microsoft Defender for Endpoint, entfallen die Lizenzpositionen für SentinelOne Singularity.

7.3 Anforderungen an den Betrieb und die Serviceintegration

Der Auftragnehmer hat die vom Auftraggeber benannte EDR-Plattform als Bestandteil des Cybersecurity Managed Service zu betreiben, zu überwachen, zu konfigurieren und in die übergreifenden SOC-, SIEM-, ServiceNow-, Reporting- und Response-Prozesse einzubinden. Maßgeblich ist nicht die Bereitstellung einer eigenen EDR-Plattform, sondern die sichere, nachvollziehbare und betriebsstabile Serviceerbringung auf Basis der vom Auftraggeber vorgegebenen Plattform.

- Der Auftragnehmer stellt den laufenden Betrieb der EDR-Plattform für den vereinbarten Endpoint-Scope sicher. Dies umfasst insbesondere die Überwachung der Endpoint-Abdeckung, des Agentenstatus, der Plattformkommunikation, der Policy-Zuweisung, der Aktualität relevanter Komponenten sowie der Funktionsfähigkeit der für den Sicherheitsbetrieb erforderlichen Integrationen.
- EDR-relevante Alarmer, Ereignisse und Telemetriedaten sind durch den Auftragnehmer fachlich zu bewerten, mit verfügbaren Kontextinformationen anzureichern und in den SOC-/SIEM-Prozess zu überführen. Eine rein technische Weiterleitung von EDR-Alarmen ohne Bewertung, Priorisierung und Handlungsempfehlung erfüllt diese Anforderung nicht.
- Der Auftragnehmer ist verantwortlich für das Policy- und Konfigurationsmanagement innerhalb der vom Auftraggeber benannten EDR-Plattform. Hierzu zählen insbesondere die Pflege von Baseline-Policies, Ausnahmen, Ausschlüssen, Response-Regeln, Rollen- und Berechtigungskonzepten sowie deren nachvollziehbare Dokumentation im Betriebshandbuch.
- Response- und Containment-Maßnahmen auf Endpunkten erfolgen ausschließlich im abgestimmten Berechtigungs-, Freigabe- und Eskalationsrahmen. Der Auftragnehmer nutzt hierfür die durch die jeweilige EDR-Plattform bereitgestellten Funktionen, soweit diese verfügbar und für den konkreten Anwendungsfall freigegeben sind.
- Der Auftragnehmer stellt sicher, dass EDR-bezogene Ereignisse, Bewertungen, Maßnahmen, Abweichungen und Einschränkungen im regelmäßigen Service-Reporting berücksichtigt werden. Hierzu gehören insbesondere nicht angebundene Endpunkte, fehlerhafte oder

veraltete Agentenstände, fehlende Plattformkommunikation, Policy-Abweichungen, relevante Schutzlücken, offene Maßnahmen und erkannte Verbesserungspotenziale.

- Änderungen an EDR-Policies, Ausschlüssen, Response-Regeln, Integrationen oder sonstigen betriebsrelevanten Konfigurationen sind über den abgestimmten Change-Management-Prozess zu führen, zu dokumentieren und nach Umsetzung hinsichtlich ihrer Wirksamkeit zu überprüfen.

7.4 Agentenbetrieb und Health Monitoring

- Endpoint-Abdeckung, Agentenstatus, Aktualität, Plattformkommunikation und Funktionsfähigkeit der für den Sicherheitsbetrieb relevanten EDR-Funktionen sind durch den Auftragnehmer laufend zu überwachen.
- Endpunkte ohne Agenten, mit veraltetem Stand, ohne aktuelle Policy oder ohne Plattformkommunikation müssen identifiziert und im Betriebsreporting ausgewiesen werden. Für Abweichungen oberhalb definierter Schwellen wird eine Maßnahmenliste mit dem UKF abgestimmt.
- Schutz vor Deaktivierung und Manipulation der EDR-Funktion durch lokale Benutzer ist sicherzustellen.

7.5 Policy- und Konfigurationsmanagement

- Baseline-Policies werden für definierte Endpoint-Klassen (Server, Client, VDI) gepflegt. Ausnahmen, Ausschlüsse und Konfigurationsänderungen werden über das abgestimmte Berechtigungs- und Freigabemodell behandelt und revisionssicher protokolliert.
- Policy-Änderungen werden im Change-Management-Prozess geführt; Rollback bei Fehlkonfigurationen muss möglich sein.

7.6 Response- und Containment-Maßnahmen

Endpointbezogene Reaktionen umfassen den abgestimmten Maßnahmenkatalog: Isolation kompromittierter Endpunkte, Beenden schädlicher Prozesse, Quarantäne und Entfernung schädlicher Dateien, erhöhte Telemetrieerfassung sowie Sammlung forensischer Artefakte.

- Für Verwaltungsarbeitsplätze und vergleichbare Standard-Endpunkte sind vorab freigegebene Response-Maßnahmen – insbesondere Endpoint-Isolation – als SOAR-/Playbook-Aktionen zulässig und sollen erhalten bleiben.
- Für Systeme mit potenzieller Auswirkung auf klinische Prozesse oder kritische Betriebsabläufe gelten gesonderte Freigabe- und Eskalationsregeln gemäß Querschnittskapitel 3.3.

7.7 Integration in SIEM und XDR-Optionen

- Endpointbezogene Alarme, Telemetrie und Bewertungen werden in das SIEM übergeben. Die Integration ermöglicht die Anreicherung von SIEM-Alarmen mit Endpoint-Kontext sowie die Verknüpfung mit NDR- und Vulnerability-Erkenntnissen.
- Erweiterte XDR-Funktionen sind nur zulässig, soweit sie Bestandteil der vom Auftraggeber benannten EDR-Plattform oder der vorhandenen Microsoft-/SentinelOne-Umgebung sind. Eine zusätzliche EDR- oder Endpoint-Security-Plattform des Auftragnehmers ist ausgeschlossen. Eine gesonderte Bepreisung erfolgt nur, soweit hierfür im Preisblatt ausdrücklich optionale Positionen vorgesehen sind.

8. Leistungsbereich IoMT-Security

8.1 Geltungsbereich und Grundprinzipien

Der Leistungsbereich umfasst die sicherheitstechnische Erfassung, Überwachung, Bewertung und Einbindung vernetzter Medizingeräte und medizinisch geprägter Netzwerksegmente. Für Planung und Dimensionierung ist von ca. 5.000 vernetzten Medizingeräten auszugehen. Vernetzte Medizingeräte unterscheiden sich strukturell von der klassischen IT: Zulassung, Wartung, Lebenszyklus und Patch-Möglichkeiten sind herstellerseitig vorgegeben, agentenbasierte Standardlösungen sind regelmäßig nicht zulässig, und jede Reaktion mit potenzieller Auswirkung auf die Patientenversorgung erfordert besondere Sorgfalt.

- Die Lösung muss medizinisch-kritische Segmente ausschließlich passiv und nicht-invasiv erfassen. Aktive Scans, agentenbasierte Standardbehandlung und automatisierte Blocking-, Quarantäne- oder Isolationsmaßnahmen sind in diesen Segmenten ausgeschlossen.
- Sicherheitsrelevante Reaktionsmaßnahmen erfolgen ausschließlich nach dem Human-in-the-Loop-Prinzip mit Freigabe durch den Auftraggeber.
- Die Lösung muss für den Betrieb in OT- und IoMT-Umgebungen qualifiziert sein. Nachweis: Produktdatenblatt oder Herstellererklärung.

Die IoMT-Security-Leistung dient neben der Angriffserkennung auch der Herstellung eines nachvollziehbaren Asset- und Kommunikationslagebildes für Medizintechnik, IT-Betrieb und Informationssicherheit. Sie muss insbesondere Risikobewertung, Betriebsanalyse, Troubleshooting und Nachweisführung für vernetzte Medizingeräte unterstützen.

8.2 Passive Erkennung und Asset Discovery

- Die Lösung muss netzwerkgebundene IoMT-, IoT- und OT-Geräte sowie medizinisch geprägte Endpunkte passiv und herstellerunabhängig erkennen, als Zielwert gilt eine Erkennungsrate von mindestens 90%.
- Für erkannte Geräte müssen mittels Deep Packet Inspection oder gleichwertiger Verfahren mindestens folgende Attribute erfasst werden: Hersteller, Modell, Gerätetyp, Betriebssystem/Firmwarestand, MDR-Klassifizierung soweit verfügbar, MAC- und IP-Adresse, Seriennummer (sofern übertragen), aktive Kommunikationsverbindungen, Standort-, Segment- bzw. VLAN-Zuordnung.
- Das Geräteinventar muss durch Daten aus Medizintechnik, IT-Betrieb, Netzwerkbetrieb, Asset Management und CMMS/EAM-Systemen anreicherbar sein. MDS²-Formulardaten müssen ingestierbar und auf Asset-Ebene darstellbar sein.

8.3 Kommunikationsanalyse und Anomalieerkennung

Die Lösung muss mindestens folgende Erkennungsfähigkeiten bereitstellen:

- reguläre und unzulässige Kommunikationsbeziehungen
- neue oder ungewöhnliche Kommunikationspartner
- auffällige Protokolle und Kommunikationsmuster

-
- Richtlinien- und Segmentierungsabweichungen
 - verdächtige externe Kommunikationsziele
 - potenzielle Command-and-Control- oder Exfiltrationsmuster
 - Kommunikationsveränderungen nach Wartung oder Gerätewechsel
 - Die Bewertung von Auffälligkeiten muss Geräteart, klinische Kritikalität, Segment, bekannte Wartungsfenster und medizinische Prozessmuster berücksichtigen. Nicht jede technische Abweichung ist automatisch als Sicherheitsvorfall zu behandeln.

8.4 Risiko- und Schwachstellenbewertung

- Die Risikobewertung erfolgt Geräteebene und muss Ausnutzbarkeit, aktive Bedrohungen, Erreichbarkeit, Segmentierung, Kommunikationsbeziehungen, klinische Kritikalität, vorhandene Kompensationsmaßnahmen und Herstellerhinweise (MDS²) berücksichtigen.
- Das Ergebnis ist als priorisierte, nachvollziehbar begründete Risikobewertung darzustellen. Generische CVE-Listen ohne Einsatzkontext erfüllen die Anforderung nicht.

8.5 Reaktion und Eskalation

- Sicherheitsrelevante Ereignisse müssen analysiert, priorisiert und mit konkreten Handlungsempfehlungen bereitgestellt werden. Maßnahmen mit möglicher Auswirkung auf klinische Prozesse, Medizingeräte oder Patientenversorgung erfolgen ausschließlich nach Freigabe durch die benannten Stellen des UKF.

8.6 Datenschutz klinischer Protokolldaten

- Klinische Protokolldaten (DICOM, HL7 v2/v3, FHIR) enthalten regelmäßig Patientenidentifikationsmerkmale (Art. 9 DSGVO). Eine Übertragung dieser Rohdaten in Cloud- oder Drittumgebungen ist technisch auszuschließen. Eine On-Premises-Anonymisierung oder -Pseudonymisierung erfolgt vor jeder Cloud-Übertragung gemäß Querschnittskapitel 3.4.
- Im Angebot ist eine Data-Flow-Dokumentation mit Feldliste vorzulegen, die zeigt, welche Felder analysiert, verworfen und anonymisiert/pseudonymisiert übertragen werden.

8.7 Integration in SIEM und Abgrenzung zu NDR

- Sicherheitsrelevante Alarme, Bewertungen und Kontextdaten müssen an das SIEM übergeben werden. Klinische Protokolldaten werden nicht ungefiltert in das SIEM überführt. Eine Übertragung erfolgt ausschließlich als sicherheitsrelevanter Alarm, Bewertung oder Kontextinformation sowie unter Beachtung der Anonymisierungs- und Pseudonymisierungsanforderungen gemäß Kapitel 3.4 und Kapitel 8.6.
- Der Leistungsbereich ist von NDR fachlich abzugrenzen und technisch anschlussfähig zu gestalten. NDR adressiert die allgemeine netzwerkbasierte Erkennung; IoMT adressiert die besonderen Anforderungen medizinisch geprägter Systeme.

9. Implementierung und Transition

9.1 Vorgehensmodell und Phasen

Der Auftragnehmer hat ein belastbares Vorgehensmodell mit Phasen, Meilensteinen, Abnahmen und Verantwortlichkeiten vorzulegen. Die nachfolgenden Phasen und Richtwerte sind verbindlich; die konkrete Terminierung erfolgt im Projektplan.

Phase	Inhalt	Richtwert
1. Initialisierung	Kick-off, Projektorganisation, Rollen, Kommunikationswege, RACI, initiale Risikoübersicht	2 Wochen
2. Bestandsaufnahme & Feinkonzeption	Validierung Mengengerüst, Asset- und Kritikalitätsklassifizierung, Zielarchitektur, Datenflüsse, Schnittstellen, Berechtigungen, Integrationsreihenfolge, Test- und Abnahmekriterien	6–8 Wochen
3. Bereitstellung & Implementierung	Aufbau Plattformen, Sensorik, Konnektoren, Integrationen; EDR-Betriebsübernahme bzw. optionale EDR-Transition auf Microsoft Defender for Endpoint sowie NDR-/VM-Übernahme oder -Migration; Use-Case- und Detection-Aufbau; ServiceNow-Integration	12–16 Wochen
Meilenstein M1 – Cut-over Serviceverantwortung	Teilstand innerhalb der Phase 3: Übernahme der Serviceverantwortung vom bisherigen Dienstleister im Mindestschutzzumfang gemäß Kapitel 9.5; Beginn des Ramp-up-Betriebs	Fixtermin 31.05.2027
4. Test & Validierung	Funktions- und Integrationstests, Validierung Datenqualität, Use Cases, Eskalationswege, Response- und Freigabemechanismen	4 Wochen
5. Schulung & Wissenstransfer	Initiale Schulung der UKF-Rollen, Übergabe Betriebshandbuch und Knowledge Base	2 Wochen
6. Go-Live & Hypercare	Übergang in Regelbetrieb, engmaschige Stabilisierungsphase mit Nachsteuerung Datenqualität, Alarmqualität und Use Cases	8 Wochen

- Der Auftragnehmer benennt eine zentrale Transition- bzw. Projektleitung als verantwortliche Steuerungsrolle.
- Die Feinkonzeption ist mit dem UKF abzustimmen und vor Beginn wesentlicher Umsetzungsmaßnahmen schriftlich freizugeben.
- Die Richtwerte der Phasen beziehen sich auf deren vollständigen Leistungsumfang. Der Meilenstein M1 gemäß Kapitel 9.5 markiert einen Teilstand innerhalb der Phase 3: Zu diesem Termin ist der Mindestschutzzumfang herzustellen und abzunehmen; die übrigen Leistungsbestandteile der Phase 3 werden anschließend parallel zum Ramp-up-Betrieb fertiggestellt. Der Auftragnehmer weist die Erreichung des Meilensteins M1 im Projektplan mit Terminen, Abhängigkeiten und Mitwirkungsleistungen des Auftraggebers nach.

9.2 Asset- und Kritikalitätsklassifizierung

Eine entscheidende Voraussetzung für die fachliche Priorisierung von Alarmen, Schwachstellen und Reaktionsmaßnahmen ist das Verständnis des klinischen und operativen Kontexts der IT-Assets. Im Onboarding wird hierfür ein gemeinsamer Workshop durchgeführt.

- Im Rahmen des Onboardings müssen Auftragnehmer und UKF in einem gemeinsamen Workshop die Asset- und Kritikalitätsklassifizierung erarbeiten. Mindestkategorien sind: lebenswichtige/klinisch-kritische Systeme, klinisch relevante Systeme, unterstützende Systeme, administrative Systeme.
- Für jedes Asset ist die Exponiertheit zu bewerten (z. B. extern erreichbar, intern und unsegmentiert, hochgradig isoliert).
- Die Ergebnisse der Klassifizierung sind in einer gemeinsam zugänglichen Dokumentation zu führen und mindestens jährlich sowie anlassbezogen zu überprüfen. Sie dienen als verbindliche Grundlage für Priorisierungsentscheidungen in Detektion, Vulnerability Management, Incident Handling und Reporting.

9.3 Logquellen-, Sensorik- und Integrationskatalog

Der Auftragnehmer baut einen fortschreibbaren Integrationskatalog auf, der während der Transition gepflegt wird. Pro Quelle/Integration sind mindestens enthalten: Bezeichnung, Leistungsbereich, technische Anschlussart, erwartete Datenart und -qualität, Priorität, Abhängigkeiten, Verantwortlichkeiten, Freischaltungen, Parser-/Mapping-Bedarf sowie Test- und Abnahmekriterien.

9.4 Plattform-Übernahmen oder -Migrationen

- Bei Fortführung bestehender Lösungen in den Leistungsbereichen NDR und Vulnerability Management erfolgt eine strukturierte Übernahme inklusive Lizenz- und Vertragsanschluss, Validierung von Konfigurationen, Prüfung der Abdeckung und Übernahme relevanter Betriebsartefakte. Lizenz- und Vertragsanschluss bei NDR/VM ist vor dem 30.09.2027 sicherzustellen.
- Für den Leistungsbereich EDR erfolgt eine strukturierte Betriebsübernahme der vom Auftraggeber benannten EDR-Plattform. Dies umfasst bei Fortführung von SentinelOne Singularity insbesondere die Übernahme und Validierung bestehender Policies, Ausschlüsse, Agentenabdeckung, Alarm- und Response-Prozesse sowie die Integration in SIEM, ServiceNow und Reporting.
- Sofern der Auftraggeber Microsoft Defender for Endpoint vorgibt und die optionale Transition abruft, ist die Transition von SentinelOne Singularity zu Microsoft Defender for Endpoint nach einem abgestimmten Transitionsplan durchzuführen. Dieser umfasst mindestens Pilotierung, Rollout-Wellen, Parallelbetrieb soweit erforderlich (gesondert bepreist gemäß Kapitel 7.2), Policy- und Regelüberführung, Anpassung von Detection- und Response-Prozessen, Test, Rückfallverfahren und Maßnahmen zur Vermeidung von Schutzlücken.
- Bei Migration auf alternative Lösungen in den Leistungsbereichen NDR oder Vulnerability Management sind Pilotierung, Rollout-Wellen, Parallelbetrieb, Rückfallverfahren, Ablösung

bestehender Komponenten und Maßnahmen zur Vermeidung von Erkennungslücken im Projektplan zu dokumentieren.

- Der Auftragnehmer stellt sicher, dass in allen Leistungsbereichen ab dem Cut-over durchgehend eine gültige Lizenzierung und ein durchgehender Plattformbetrieb bestehen. Für die Leistungsbereiche SOC/SIEM und EDR-Management, deren bestehende Verträge am 31.05.2027 enden, ist die Lizenz- und Betriebsfähigkeit ab dem 01.06.2027 lückenlos sicherzustellen; die hierfür erforderlichen Lizenzen sind im Preisblatt auszuweisen. Ist eine Ablösung der Bestandsplattformen NDR und Vulnerability Management nicht bis zum 30.09.2027 abgeschlossen, verantwortet der Auftragnehmer deren Lizenzanschluss für den Zwischenzeitraum; auch diese Kosten sind im Preisblatt auszuweisen.

9.5 Übergang der Serviceverantwortung und Ramp-up-Betrieb

Der bestehende Managed-Service-Vertrag des Auftraggebers für die Leistungsbereiche SOC/SIEM und EDR-Management endet am 31.05.2027. Der Auftragnehmer übernimmt die Serviceverantwortung spätestens zu diesem Termin (Cut-over). Vom Cut-over bis zum Übergang in den Regelbetrieb erbringt er den Ramp-up-Betrieb. Eine Überwachungslücke darf zu keinem Zeitpunkt entstehen.

- Der Auftragnehmer übernimmt ab dem Cut-over den Betrieb der zu diesem Zeitpunkt beim Auftraggeber eingesetzten Plattformen in allen Leistungsbereichen, unabhängig davon, ob er diese fortführt oder im weiteren Projektverlauf ablöst.

Zum Cut-over ist ein abnahmefähiger Mindestschutzzumfang herzustellen. Er umfasst mindestens:

- 24x7-Monitoring, Triage, Eskalation und Response-Unterstützung für die Prioritäten P1 und P2
- Anbindung und produktive Auswertung mindestens folgender Quellen gemäß Mengengerüst Kapitel 2.1: Active Directory, Identity Provider (ADFS, Entra ID), Privileged Access Management, Core- und Perimeter-Firewalls, IDS/IPS, Proxy und VPN, EDR-Plattform sowie Cloud-Audit-Logs (M365 / Entra ID)
- Betrieb der zum Cut-over eingesetzten Plattformen in den Leistungsbereichen NDR und Vulnerability Management einschließlich Alarmbearbeitung und Schwachstellen-Triage
- Übernahme der beim bisherigen Dienstleister bestehenden Detektionsregeln und Use Cases oder ein gleichwertiges, dokumentiertes Ersatzregelwerk
- Meldefähigkeit für regulatorisch relevante Sicherheitsvorfälle (§ 32 BSIG, Art. 33 DSGVO) mit abgestimmten Meldevorlagen, Rollen und Eskalationskontakten
- Übergabe von Vorfällen an das UKF über ServiceNow oder über das Ersatzverfahren gemäß Kapitel 11.5
- Erreichbarkeit und Eskalationswege einschließlich benannter Ansprechpersonen und Rufbereitschaft
- Der Cut-over erfolgt erst nach Abnahme des Mindestschutzzumfangs durch den Auftraggeber. Die Abnahme wird protokolliert; offene Punkte werden in einer Restpunktliste mit Terminen und Verantwortlichkeiten geführt.

- Der Ramp-up-Betrieb umfasst die nach dem Cut-over verbleibenden Leistungsbestandteile der Phase 3 sowie die Phasen 4 und 5 und endet mit dem Übergang in den Regelbetrieb gemäß Kapitel 9.6. Für die Angebotswertung ist eine Ramp-up-Dauer von drei Monaten einheitlich zugrunde zu legen: Die laufenden Managed-Service-Leistungen sind für 57 Monate Regelbetrieb zu kalkulieren, Plattform- und Lizenzpositionen für die vollen 60 Monate. Die Abrechnung erfolgt nach der tatsächlichen Dauer des Ramp-up-Betriebs; die Vertragslaufzeit von 60 Monaten ab Cut-over bleibt hiervon unberührt.
- Der Auftraggeber wirkt an der Übernahme mit. Er stellt die erforderlichen Zugänge, Berechtigungen, Systeminformationen und Ansprechpersonen bereit und koordiniert die Übergabe von Betriebsartefakten durch den bisherigen Dienstleister. Verzögerungen, die der Auftragnehmer nicht zu vertreten hat, verschieben den Cut-over-Termin entsprechend; die Verschiebung ist zu dokumentieren und mit Maßnahmen zur Aufrechterhaltung der Überwachung zu hinterlegen.
- Leistungsbestandteile, die zum Cut-over noch nicht abgedeckt sind, sind im Projektplan mit Terminen zu hinterlegen und im Rahmen der Phasen 4 bis 6 herzustellen.

9.6 Test, Validierung und Abnahme

Vor dem Übergang in den Regelbetrieb ist ein abgestimmter Test- und Abnahmeprozess durchzuführen. Geprüft werden insbesondere: Funktionsfähigkeit der Komponenten, Datenanlieferung und -qualität, Parser/Normalisierung, Sensorik, Use Cases und Detection, Alarm- und Eskalationswege, Ticket- und Schnittstellenprozesse, Response- und Freigabemechanismen, Reportingfunktionen und die Betriebsdokumentation.

- Der Übergang in den Regelbetrieb erfolgt erst, wenn die vereinbarten Mindestvoraussetzungen erfüllt sind und ein belastbarer Betriebsmodus mit dem UKF abgestimmt wurde.

Die Mindestvoraussetzungen für den Übergang in den Regelbetrieb umfassen mindestens:

- Mindest-Use-Cases zum Go-Live
- simulierte P1-/P2-Incidents
- Parser-/Normalisierungstest
- Test kritischer Logquellenausfall
- Test ServiceNow-Übergabe (sofern die jeweils erforderlichen Mitwirkungsleistungen beider Seiten erbracht wurden)
- Datenqualitätskriterien
- Abnahmeprotokoll mit Restpunktliste

9.7 Schulung, Wissenstransfer und Betriebshandbuch

- Initial- und Nachschulungen werden für die UKF-Rollen IT-Betrieb, Informationssicherheit, Medizintechnik und Service-Steuerung durchgeführt. Schulungsunterlagen werden bereitgestellt.
- Der Auftragnehmer führt ein versioniertes Betriebshandbuch. Es enthält mindestens Architektur, Datenflüsse, Rollen, Schnittstellen, Eskalationswege, Reportingvorgaben sowie

UKF-bezogene Use Cases, Response-Regeln und Exit-relevante Artefakte. Anbieterinterne Standardverfahren sind hiervon ausgenommen, soweit sie nicht für Betrieb, Prüfung oder Providerwechsel des UKF erforderlich sind.

- Das Betriebshandbuch enthält zusätzlich die abgestimmten Prozesspfade, Meldevorlagen, Rollen, Eskalationskontakte und Mindestinformationen für regulatorisch relevante Sicherheitsvorfälle, insbesondere für BSI-/KRITIS-Kommunikation, NIS-2-/BSIG-relevante Meldungen sowie Datenschutzmeldungen nach Art. 33 DSGVO

9.8 Hypercare

- Nach Go-Live ist eine Stabilisierungsphase von mindestens 8 Wochen vorzusehen, in der Datenanlieferung, Alarmqualität, Use Cases und Schwellwerte engmaschig nachgesteuert werden.

10. Managed Service / Betriebsmodell

Dieses Kapitel beschreibt den laufenden Managed Service nach Abschluss der Transition. Die Leistungen sind so zu erbringen, dass sicherheitsrelevante Ereignisse fortlaufend aufgenommen, fachlich bewertet, priorisiert, eskaliert, bearbeitet und nachweisbar dokumentiert werden. Rückfragen an das UKF sind auf fachlich erforderliche Fälle zu begrenzen.

10.1 Betriebsorganisation und Serviceverantwortung

- Der Auftragnehmer muss einen 24x7-Security-Operations-Center-Service mit qualifizierter Triage, Analyse, Eskalation und Response-Unterstützung im freigegebenen Rahmen betreiben.
- Der SOC-Service muss die Tier-Stufen L1 (Monitoring, initiale Triage), L2 (qualifizierte Analyse, Incident-Bearbeitung) und L3 (Incident Response / DFIR-Kapazität) abdecken.
- Der Auftragnehmer benennt einen dedizierten, deutschsprachigen Service Delivery Manager als zentrale fachliche Ansprechperson sowie eine fachlich-technische Security-Ansprechrolle für Sicherheitsarchitektur, Use-Case-Weiterentwicklung und Detection-Qualität.
- Eine einheitliche, durchgängig erreichbare Service-Hotline für sicherheitskritische Vorfälle (24x7) muss bereitgestellt werden. Die Kommunikation auf L1- und L2-Ebene (Triage, initiale Analyse, Eskalation) erfolgt in deutscher Sprache. L3-Kapazitäten (tiefgehende forensische Analyse, spezialisierte IR-Expertise) können in englischer Sprache erbracht werden, sofern eine deutschsprachige Koordinationsrolle auf L2-Ebene die Kommunikation mit dem UKF sicherstellt.

10.2 Eigenständige Bearbeitung und Begrenzung von Rückfragen

Der Managed Service soll das UKF-IT-Team im laufenden Betrieb entlasten. Der Auftragnehmer bearbeitet Alarme und Vorfälle soweit möglich eigenständig.

- Rückfragen an das UKF sind auf Fälle zu beschränken, in denen sie fachlich erforderlich sind oder definierte Freigaben benötigt werden. Routinemäßiger Kontextbedarf, der durch Plattformfähigkeiten, Live-Response-Funktionen oder automatische Kontextanreicherung gedeckt werden kann, ist eigenständig zu decken.
- Der Auftragnehmer muss bei Alarmen konkrete Entscheidungs- und Handlungsempfehlungen liefern. Offene Rückfragen ohne fachliche Bewertung erfüllen diese Anforderung nicht.
- Die Häufigkeit, Bearbeitungsdauer und Inhalte von Rückfragen werden im operativen Servicebericht (Kap. 12) ausgewiesen und Trendentwicklungen kommentiert.

10.3 Security Monitoring und Triage

- Eingehende Ereignisse müssen unter Berücksichtigung von Kritikalität, Asset- und Identitätskontext, bekannten Schwachstellen, Kommunikationsbeziehungen, Segmenten und vorhergehenden Auffälligkeiten bewertet werden.
- Fehlalarme, unkritische Auffälligkeiten, Informationsereignisse und tatsächlich zu bearbeitende Sicherheitsvorfälle sind nachvollziehbar voneinander zu unterscheiden.

-
- Eingehende Alarmer müssen eine fachliche Bewertung, Priorisierung und einen konkreten Handlungsvorschlag erhalten. Eine technische Weiterleitung ohne Bewertung erfüllt diese Anforderung nicht.

10.4 Methodik (MITRE ATT&CK)

- Die operative Methodik des SOC – von der Analyse über die Investigation bis zum Threat Hunting – orientiert sich am MITRE ATT&CK Framework. Erkannte Aktivitäten und Sicherheitsvorfälle werden den entsprechenden Taktiken, Techniken und Prozeduren (TTPs) zugeordnet, soweit fachlich anwendbar.
- Reporting und Incident-Dokumentation müssen Verweise auf das ATT&CK Framework enthalten, soweit anwendbar.

10.5 Incident Handling

Das Incident Handling umfasst Aufnahme, Validierung, Analyse, Bewertung, Eskalation, Bearbeitung, Dokumentation und Abschluss sicherheitsrelevanter Vorfälle. Jeder Incident-Datensatz muss mindestens enthalten:

- eindeutige Incident-ID
- fachliche Beschreibung des Sachverhalts
- Bewertung der Kritikalität und Begründung
- Zeitstempel: Erkennung, Triage, Validierung, Eindämmung, Übergabe, Abschluss
- betroffene Systeme, Benutzer, Konten, Kommunikationsbeziehungen oder Datenflüsse
- Grundlage der Erkennung (Use Case, Quelle, IoC, MITRE ATT&CK-Mapping soweit anwendbar)
- zeitlicher Verlauf und Ereigniskette, soweit ermittelbar
- bereits erfolgte Analyse- und Reaktionsschritte
- empfohlene nächste Maßnahmen
- offene Entscheidungs- oder Freigabebedarfe
- Lessons-Learned-Bewertung beim Abschluss
- Reklassifizierungen (Änderung der Priorität nach neuen Erkenntnissen) müssen dokumentiert und nachvollziehbar begründet werden.

10.6 Investigation und forensische Analyse

- Für jeden validierten Sicherheitsvorfall muss eine fachliche Untersuchung durchgeführt werden, die Angriffsursprung (Root Cause), Angriffskette (Kill Chain), betroffene Systeme, zeitlichen Ablauf und potenzielle Auswirkungen auf Klinikbetrieb und Patientensicherheit nachvollziehbar bestimmt.
- Bei P1-Vorfällen werden forensische Artefakte (Endpoint-Telemetrie, Speicherauszüge soweit erforderlich, Netzwerk-Metadaten, Authentifizierungsspuren) gesichert. Verfahren und Aufbewahrung sind im Betriebshandbuch zu dokumentieren.

- L3-/DFIR-Kapazität ist Bestandteil des Managed Service und muss 24×7 abrufbar sein. Einsatzaufwände werden nach den im Preisblatt ausgewiesenen DFIR-Stundensätzen abgerechnet.

10.7 Reaktion: Stufenmodell

Der Auftragnehmer setzt ein dreistufiges Reaktionsmodell ein:

Stufe	Beschreibung	Beispiele
Automatisierte Reaktion	Vorab abgestimmte, automatisch ausgeführte Playbook-Aktionen für definierte Endpunkt- bzw. Systemklassen.	Endpoint-Isolation Verwaltungs-PCs, Blockierung schädlicher IP/Domain, Deaktivierung kompromittierter Konten in freigegebenen Klassen
Analysten-gesteuerte Reaktion	Direkte Maßnahmen durch SOC-Analysten ohne Mitwirkung des UKF, im Rahmen freigegebener Befugnisse.	Beenden schädlicher Prozesse, Quarantäne von Dateien, gezielte Telemetrieerhebung, Live-Response-Maßnahmen
Guided Response	Bei Maßnahmen, die potenziell den Klinikbetrieb beeinträchtigen oder klinisch-kritische Systeme betreffen, ergreift das SOC keine eigenmächtigen Schritte.	Konkrete, priorisierte und verständliche Handlungsempfehlungen an das UKF, aktive Unterstützung bei der Umsetzung

- Automatisierte Reaktionen sind ausschließlich innerhalb der vorab abgestimmten Maßnahmenkataloge zulässig. In medizinisch-kritischen Segmenten und auf Systemen mit potenzieller Auswirkung auf klinische Prozesse sind automatisierte Reaktionsmaßnahmen ausgeschlossen (vgl. Kap. 3.3).

10.8 Threat Hunting

- Threat Hunting muss mindestens einmal pro Monat hypothesenbasiert durchgeführt werden. Aktuelle Bedrohungslagen, Healthcare-/KRITIS-spezifische Angriffsmuster, Threat Intelligence, Schwachstelleninformationen und die technische Umgebung des UKF werden berücksichtigt.
- Threat Hunts sind methodisch vorzubereiten, durchzuführen und nachvollziehbar zu dokumentieren. Für jeden Threat Hunt sind mindestens Hypothese, zugrunde liegende Bedrohungslage, betrachtete Datenquellen, eingesetzte Suchlogiken, betrachteter Zeitraum, Ergebnisse, erkannte Auffälligkeiten, fachliche Bewertung, empfohlene Maßnahmen sowie Auswirkungen auf bestehende Use Cases, Detection-Regeln, Schwellwerte oder Playbooks zu dokumentieren.
- Threat Hunting darf sich nicht auf die reine Sichtung vorhandener Alarme oder Standardreports beschränken. Es muss aktiv nach bisher nicht detektierten Angriffsspuren, verdächtigen Mustern, lateralen Bewegungen, Identitätsmissbrauch, Command-and-Control-Kommunikation, ungewöhnlichen Datenflüssen, ausnutzbaren Schwachstellenkontexten sowie KRITIS- und Healthcare-relevanten Angriffstechniken gesucht werden.

- Erkenntnisse aus Threat Hunts sind in die kontinuierliche Verbesserung des Detection Engineerings zu überführen. Dies umfasst insbesondere Vorschläge zur Anpassung oder Ergänzung von Use Cases, Parsern, Korrelationen, Schwellenwerten, Anreicherungen, Playbooks und Handlungsempfehlungen. Die Umsetzung oder begründete Nichtumsetzung dieser Erkenntnisse ist im Rahmen der Regelpflege bzw. des Service Reviews nachvollziehbar zu dokumentieren.

10.9 SOAR und Playbooks

- Der Auftragnehmer muss eine SOAR-Funktionalität für die Automatisierung wiederkehrender Bearbeitungsschritte und definierter Reaktionsmaßnahmen einsetzen. Playbooks werden gemeinsam mit dem UKF abgestimmt und dokumentiert.
- Vorab freigegebene Reaktionsmaßnahmen für Standard-Endpunkte (insbesondere Endpoint-Isolation für Verwaltungs-Clients) sind als automatisierte oder halbautomatisierte Playbook-Aktionen zulässig und sollen erhalten bleiben.

10.10 Use-Case-, Detection- und Regelpflege

- Use Cases, Detection-Regeln, Korrelationen, Schwellwerte, Ausnahmen und Playbooks müssen fortlaufend gepflegt werden. Anlässe sind insbesondere neue Bedrohungslagen, Erkenntnisse aus Sicherheitsvorfällen, Threat-Hunting-Ergebnisse, Schwachstellenlagen, Infrastrukturänderungen, neue Quellen und False-Positive-Reduktion.
- Der Auftragnehmer muss kundenspezifische Security Operation Procedures (Vorbereitung, Detektion, Verifikation, Analyse, Kommunikation, Reaktion, Eskalation) pflegen und im Betriebshandbuch aktuell halten.
- Änderungen an produktiven Use Cases, Detection-Regeln, Parsern, Normalisierungen, Feldzuordnungen und Korrelationslogiken sind vor produktiver Aktivierung fachlich zu bewerten, qualitätszusichern, freizugeben und versioniert zu dokumentieren. Die Dokumentation muss mindestens Zweck, Auslöser, betroffene Datenquellen, fachliche Begründung, erwartete Wirkung sowie mögliche Auswirkungen auf Alarmqualität, False-Positive-Rate und Betriebsprozesse enthalten.
- Der Auftragnehmer muss wesentliche Detection-Use-Cases regelmäßig und anlassbezogen durch geeignete, mit dem Auftraggeber abgestimmte Testverfahren validieren. Hierzu können technische Use-Case-Tests, Replay geeigneter Logdaten, Purple-Team-Übungen oder kontrollierte Angriffssimulationen genutzt werden. Produktive Systeme, klinische Prozesse und medizinisch-kritische Segmente dürfen nicht gefährdet werden. Ergebnisse, erkannte Lücken und abgeleitete Anpassungen sind zu dokumentieren und in die Use-Case- und Regelpflege zu überführen.

10.11 Schwachstellen-Service im laufenden Betrieb

- Der Schwachstellen-Service muss Plattformbetrieb, Scan-Durchführung, fachliche Triage, kontextbezogene Priorisierung (CVSS, Asset-Kritikalität, Erreichbarkeit, Firewall-/Segmentierungssituation, aktive Ausnutzung), priorisierte Maßnahmenübergabe und Remediation-Tracking bis zur dokumentierten Schließung oder Risikoakzeptanz umfassen.

- Reporting-Frequenz und Mindestinhalt der Schwachstellenberichte sind in Kapitel 6.6 geregelt.

10.12 Incident- und Request-Klassen

- Der Auftragnehmer hat im Betriebskonzept eine verbindliche Systematik für Security Incidents, Service Incidents, Service Requests und Changes vorzusehen. Die Systematik muss so ausgestaltet sein, dass Vorgänge eindeutig klassifiziert, priorisiert, eskaliert, bearbeitet und dokumentiert werden können.
- Security Incidents sind sicherheitsrelevante Ereignisse oder Vorfälle, die auf eine tatsächliche oder mögliche Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit hinweisen. Hierzu zählen insbesondere kompromittierte Konten, Malware- oder Ransomware-Verdacht, laterale Bewegung, Command-and-Control-Kommunikation, Datenabfluss, Missbrauch administrativer Berechtigungen, aktive Ausnutzung von Schwachstellen oder sonstige sicherheitsrelevante Auffälligkeiten.
- Service Incidents sind Störungen oder Einschränkungen der Managed-Service-Leistung selbst. Hierzu zählen insbesondere Ausfälle oder Qualitätsmängel bei Monitoring, Logeingang, Sensorik, Parsern, Normalisierung, Korrelation, Portal-, Ticketing-, Reporting- oder Integrationsfunktionen.
- Für Security Incidents und Service Incidents sind im Betriebshandbuch mindestens Definition, Abgrenzung, Beispiele, Priorisierung, Bearbeitungsweg, Eskalationsweg, Dokumentationspflichten und Abschlusskriterien festzulegen
- Incidents, deren nachhaltige Behandlung eine dauerhafte Änderung an Logquellen, Parsern, Detection-Regeln, Use Cases, Eskalationswegen, Schnittstellen, Reports oder sonstigen Servicebestandteilen erfordert, sind nach der Erstbearbeitung in das Change-Management zu überführen. Die Verknüpfung zwischen Incident und Change ist im führenden Ticketsystem nachvollziehbar zu dokumentieren.

10.13 Service Requests

Service Requests sind planbare oder anlassbezogene Anforderungen an die laufende Serviceerbringung, die keinen unmittelbaren Sicherheitsvorfall und keine Störung des Managed Service darstellen.

Hierzu gehören insbesondere:

- Aufnahme neuer Log-, Event-, Telemetrie- oder Kontextquellen
- Anpassung oder Erweiterung von Use Cases, Detection-Regeln, Parsern, Mappings oder Playbooks
- Änderung von Berechtigungen, Rollen, Benachrichtigungs- oder Eskalationswegen
- Aufnahme neuer Systeme, Standorte, Segmente, Assets oder Organisationseinheiten in den Leistungsumfang
- Anpassung von Reports, Dashboards, Auswertungen oder Nachweisen

Für Service Requests sind Annahmeverfahren, Priorisierung, Bearbeitungsweg, Freigabebedarf, Kommunikationsweg, Umsetzungsfristen und Abschlusskriterien im Betriebshandbuch festzulegen.

Führt ein Service Request zu Änderungen an produktiven Erkennungs-, Integrations-, Berechtigungs-, Reporting- oder Reaktionsmechanismen, ist er in das Change-Management zu überführen

10.14 Change-Management

Der Auftragnehmer hat ein verbindliches Change Management für alle Änderungen einzurichten, die Auswirkungen auf Wirksamkeit, Stabilität, Sicherheit, Nachvollziehbarkeit oder Betriebsfähigkeit der ausgeschriebenen Managed-Service-Leistung haben können.

Als änderungsrelevant gelten insbesondere Anpassungen an Logquellen, Integrationswegen, Sensorik, Parsern, Normalisierungen, Detection-Regeln, Use Cases, Playbooks, Policies, Berechtigungen, Schnittstellen, Reports, Dashboards, Alarmierungswegen und Eskalationslogiken. Änderungen an der UKF-Infrastruktur liegen in der Verantwortung des UKF bzw. der jeweils zuständigen Betriebsgruppen. Der Auftragnehmer ist nicht für die Planung, Freigabe oder Umsetzung dieser Infrastrukturänderungen verantwortlich.

Soweit solche Änderungen Auswirkungen auf die Managed-Service-Leistung haben können, hat der Auftragnehmer die Auswirkungen auf Monitoring, Logquellen, Sensorik, Parser, Normalisierung, Detection-Regeln, Use Cases, Asset-Klassifizierung, Eskalationswege, Reports oder freigegebene Response-Mechanismen zu bewerten und erforderliche Anpassungen innerhalb seiner Servicebestandteile vorzuschlagen bzw. umzusetzen.

Dies betrifft insbesondere:

- Inbetriebnahme neuer Systeme, Anwendungen, Server, Netzwerkkomponenten, Cloud-Dienste oder Sicherheitskomponenten
- Außerbetriebnahme bestehender Systeme, Anwendungen, Logquellen, Sensoren oder Schnittstellen
- wesentliche Konfigurationsänderungen an kritischen Systemen, insbesondere Firewall-Regeln, Segmentierungslogiken, Identity-Systemen, Cloud-Diensten, Netzwerkarchitektur oder zentralen Betriebsplattformen

Im Betriebskonzept sind die beim UKF verwendeten Change-Kategorien für die vom Auftragnehmer verantworteten Servicebestandteile zu übernehmen. Maßgeblich für die Einordnung sind Aufwand, betriebliches Risiko sowie potenzielle Auswirkungen auf abhängige Systeme, Sicherheitsprozesse oder Betriebsabläufe.

Es sind mindestens folgende Change-Kategorien zu unterscheiden:

- **Standard Change:** vorab definierte, wiederkehrende und risikoarme Änderung mit dokumentiertem Verfahren. Hierzu zählen im SOC-/SIEM-Kontext insbesondere Änderungen mit vorhandener Vorlage, z. B. Anpassungen bestehender Benachrichtigungswege, kleinere Dashboard-Anpassungen, Logging-Anpassungen ohne neue Integrationslogik oder die Nutzung vorhandener Parser für Standardquellen.
- **Minor Change:** Änderung mit geringem Risiko und begrenzter Auswirkung auf den laufenden Betrieb. Hierzu zählen insbesondere kleinere Anpassungen an Parsern, Mappings, Rollen, Reports, bestehenden Detection-Regeln, Eskalationswegen oder die Anbindung einer bekannten Quelle mit geringem Anpassungsbedarf.
- **Significant Change:** Änderung mit mittlerem Risiko oder Auswirkung auf mehrere Systeme, Datenflüsse, Use Cases oder Betriebsprozesse. Hierzu zählen insbesondere neue Integrationen, neue oder wesentlich angepasste Use Cases, Änderungen an Korrelationen,

Schnittstellenanpassungen zu ServiceNow, SIEM-, NDR-, EDR-, Vulnerability-Management- oder IoMT-Plattformen sowie Änderungen mit Test- und Freigabebedarf.

- Major Change: Änderung mit hohem Risiko, wesentlicher Auswirkung auf Architektur, Betriebsmodell, Verfügbarkeit, Sicherheit oder Nachweisführung. Hierzu zählen insbesondere Plattformwechsel, größere Migrationen, grundlegende Änderungen an Datenpipelines, Wechsel zentraler Integrationskomponenten, umfangreiche Neuordnung von Logquellen, Mandanten-/Tenant-Änderungen oder Änderungen mit erheblicher Auswirkung auf den SOC-/SIEM-Betrieb.
- Emergency Change: dringende Änderung zur Gefahrenabwehr, Stabilisierung oder kurzfristigen Wiederherstellung der Betriebs- oder Sicherheitslage. Hierzu zählen insbesondere kurzfristige Detection- oder Korrelationsanpassungen bei aktiv ausgenutzten Schwachstellen, Anpassungen bei laufenden Angriffen, dringende Workarounds bei Ausfall kritischer Logquellen oder kurzfristig notwendige Änderungen zur Aufrechterhaltung der Erkennungs- und Eskalationsfähigkeit.

Für jeden Change sind mindestens Anlass, Ziel, Risiko, Auswirkungsbewertung, Verantwortlichkeiten, Freigaben, Umsetzungszeitpunkt, Rückfallverfahren, Dokumentation und Abnahme festzulegen. Jeder Change ist in einem Change-Register nachzuhalten. Dieses muss mindestens Ticket-ID, Datum, beteiligte Personen oder Rollen, Anlass, Maßnahme, Ergebnis, Freigabestatus, Rückfallstrategie und Abschlussstatus enthalten.

Nach Umsetzung eines Changes hat der Auftragnehmer zu verifizieren, dass die betroffenen Logquellen, Sensoren, Integrationen, Detection-Inhalte, Reports, Eskalationswege oder sonstigen vom Auftragnehmer verantworteten Servicebestandteile weiterhin korrekt funktionieren und die Daten in der erwarteten Qualität vorliegen.

Emergency Changes können in einem beschleunigten Verfahren umgesetzt werden. Sie sind nachträglich vollständig zu dokumentieren und im Rahmen eines geregelten Review-Verfahrens zu bewerten.

Die Informationspflicht für geplante Änderungen an der UKF-Infrastruktur liegt beim UKF. Die Bewertung der Auswirkungen auf die Managed-Service-Leistung und die Anpassung der vom Auftragnehmer verantworteten Servicebestandteile liegen beim Auftragnehmer

10.15 Major Incident und Krisenmodus

- Bei Sicherheitsvorfällen mit erheblicher oder potenziell erheblicher Auswirkung auf kritische Dienste, klinische Prozesse, Patientensicherheit, zentrale Identitäts- oder Infrastrukturdienste oder regulatorische Meldepflichten muss der Auftragnehmer auf Anforderung oder nach abgestimmten Kriterien in einen Major-Incident- bzw. Krisenmodus übergehen.

Der Krisenmodus umfasst:

- unverzügliche Eskalation an die benannten Stellen
- Bereitstellung einer fachlich qualifizierten Eskalationsinstanz
- Teilnahme an Lage- oder Krisenbesprechungen
- fortlaufende Bereitstellung technischer und fachlicher Lageinformationen
- Unterstützung bei Priorisierung und Entscheidungsfindung
- Bereitstellung von Indikatoren, Artefakten und Handlungsempfehlungen

- Unterstützung bei regulatorisch oder organisatorisch erforderlichen Nachweisen (KRITIS-Meldungen, BSI-Kommunikation)
- strukturierte Abschlussdokumentation nach Beendigung des Krisenmodus

Der Auftragnehmer unterstützt den Auftraggeber auf Anforderung bei nicht-invasiven Tabletop- oder Krisenübungen für schwerwiegende Sicherheitsvorfälle. Ziel ist die Überprüfung von Eskalationswegen, Rollen, Kommunikationswegen, Meldepflichten und der Zusammenarbeit im Major-Incident- bzw. Krisenmodus. Erkenntnisse mit Bezug zur Leistung des Auftragnehmers sind zu dokumentieren und in die Betriebsprozesse zu überführen.

10.16 Threat Intelligence

- Der Threat-Intelligence-Feed muss Bestandteil des Managed Service sein und ohne separate Lizenzierung bereitgestellt werden. Er deckt IoCs, TTPs, aktiv ausgenutzte Schwachstellen, branchenspezifische Angriffsmuster und KRITIS-/Healthcare-relevante Entwicklungen ab.

10.17 Service Health Monitoring und Datenqualitätskontrolle

- Der Auftragnehmer muss Verfügbarkeit und Funktionsfähigkeit der eingesetzten Plattformen, Sensoren, Konnektoren und Integrationen sowie Aktualität von Agenten, Regeln, Policies und Integrationen überwachen.
- Ausfälle, Unterbrechungen oder Qualitätsmängel in der Datenanlieferung kritischer Quellen sind innerhalb von 30 Minuten nach Feststellung zu melden und im Service-Health-Bericht auszuweisen.

10.18 Reporting und Service Reviews

Detaillierte Reportingpflichten (Frequenz, Mindestinhalt, Fristen) sind in Kapitel 12 geregelt. Ergänzend gilt:

- Der Auftragnehmer muss quartalsweise Service-Review-Meetings (Strategic Business Review) mit dem UKF durchführen und mindestens jährlich ein prüffähiges Nachweispaket zur Angriffserkennung (BSI-SzA) erstellen.

Der Auftragnehmer muss geeignete Nachweise zur Informationssicherheit, Resilienz und Kontrollwirksamkeit der für die Leistungserbringung eingesetzten SOC- und Betriebsstrukturen vorhalten und dem Auftraggeber auf Anforderung in geeigneter Form zur Verfügung stellen. Dies gilt insbesondere im Rahmen jährlicher Service- oder Compliance-Prüfungen sowie anlassbezogen bei schwerwiegenden Sicherheitsvorfällen oder wesentlichen Änderungen der Betriebsarchitektur. Geeignete Nachweise können Zertifikate, Auditberichte, Management Summaries, C5-Testate bei Cloud-Bestandteilen oder vergleichbare Prüf- und Testnachweise sein. Vertrauliche interne Informationen des Auftragnehmers oder Informationen anderer Kunden können geschützt werden, soweit die Prüffähigkeit für den Auftraggeber gewahrt bleibt.

10.19 Problem Management und kontinuierliche Verbesserung

- Wiederkehrende Sicherheitsereignisse, wiederholte Fehllarme, strukturelle Datenqualitätsprobleme oder wiederkehrende Betriebsstörungen müssen im Problem-

Management analysiert werden. Ursachen, Auswirkungen und Verbesserungsmaßnahmen werden dokumentiert und in Service Reviews nachverfolgt.

10.20 Business Continuity und Notbetrieb des Auftragnehmers

Der Auftragnehmer muss für die von ihm verantworteten Leistungen des Cybersecurity Managed Service angemessene Regelungen zur Business Continuity, zum Notbetrieb und zur Wiederherstellung kritischer Servicefunktionen vorhalten.

Diese Regelungen müssen insbesondere den Fall berücksichtigen, dass der Auftragnehmer selbst von einem Sicherheitsvorfall, Ransomware-Angriff, Ausfall zentraler Betriebsplattformen, Ausfall von Kommunikationswegen oder eingeschränkter Verfügbarkeit seiner SOC-Organisation betroffen ist.

Im Störfall muss der Auftragnehmer eine Mindestbetriebsfähigkeit für kritische Sicherheitsereignisse sicherstellen. Dies umfasst mindestens die Bearbeitung und Eskalation von P1- und P2-Vorfällen, alternative Kommunikationswege, eine qualifizierte Eskalationsstelle sowie die nachträgliche Dokumentation und Synchronisation betroffener Vorgänge.

Der Auftragnehmer weist die bestehenden Regelungen spätestens im Rahmen der Transition in geeigneter Form nach, z. B. durch eine Management Summary, Auditnachweise, Testnachweise oder vergleichbare Nachweise. Eine vollständige Offenlegung interner Notfallhandbücher ist nicht erforderlich, sofern die Prüffähigkeit für den Auftraggeber gewahrt bleibt.

Die Regelungen sind im Betriebshandbuch zu referenzieren und bei wesentlichen Änderungen fortzuschreiben.

11. Prozess- und Ticketintegration (ServiceNow)

11.1 Integration als gemeinsam getragene Leistung

Die bidirektionale Integration zwischen den Systemen des Auftragnehmers und dem ITSM-System ServiceNow des UKF wird von beiden Vertragsparteien getragen. Der Auftragnehmer ist für die Integration auf seiner Seite verantwortlich; der Auftraggeber stellt die für die Integration erforderlichen Komponenten auf ServiceNow-Seite bereit.

- Der Auftragnehmer muss sein Vorgangsmanagement bidirektional in ServiceNow integrieren (E-Bonding) über eine API-basierte Schnittstelle. Eine rein manuelle, ausschließlich e-mail-basierte oder anderweitig medienbruchbehaftete Übergabe erfüllt diese Anforderung nicht.
- Der Auftraggeber stellt die für die Integration erforderlichen Schnittstellen, API-Zugänge, Verbindungsendpunkte, Berechtigungen, Konfigurationen und Mapping-Strukturen in ServiceNow bereit.
- Schnittstellenspezifikation, Mapping, Test und Inbetriebnahme erfolgen gemeinsam. Verantwortlichkeiten beider Seiten sind in der RACI-Matrix (Kap. 13) geregelt.

11.2 Vorgangsarten und Mindestinformationen

Die Integration deckt mindestens folgende Vorgangsarten ab: Security Incidents, Service Incidents des Managed Service, Service Requests, Changes und Emergency Changes, Rückfragen zu Freigaben, Eskalationen, Status- und Abschlussmeldungen, Übergaben an interne Betriebsgruppen und Nachverfolgung vereinbarter Maßnahmen. Die fachliche Abgrenzung der Vorgangsarten richtet sich nach Kapitel 10.12 bis 10.14.

Pro Ticket müssen mindestens folgende Informationen übergeben werden:

Feld	Inhalt
Referenznummer	eindeutige Vorgangsnummer des Auftragnehmers
Vorgangstyp / Priorität	Klassifizierung und Schweregrad
Beschreibung	Kurzbeschreibung und fachliche Sachverhaltsdarstellung
Betroffene Objekte	Systeme, Benutzer, Konten, Standorte, Segmente, Dienste
Erkennung	Zeitpunkt, Auslöser, zugrundeliegender Use Case oder Quelle, MITRE-Bezug soweit anwendbar
Analyse	Bisherige Analyseergebnisse und Bewertung
Empfehlung	Konkrete Maßnahme oder nächster Bearbeitungsschritt
Freigabe	Erforderliche Entscheidung oder Freigabe des UKF
Status	Aktueller Bearbeitungsstand
Zuständigkeit	Bearbeitungsgruppe oder Ansprechpartner
Anlagen	Nachweise, Logs, Indikatoren, technische Anlagen

-
- Bloße technische Rohmeldungen ohne Einordnung, Priorisierung und Handlungsvorschlag erfüllen die Anforderungen nicht.

11.3 Statussynchronisation und Übergabe an Gruppen

- Die Integration muss mindestens folgende Statuswerte unterstützen: neu, in Analyse, qualifiziert, an Auftraggeber übergeben, Rückfrage offen, Freigabe erforderlich, in Bearbeitung, Maßnahme umgesetzt, gelöst, zurückgestellt, Risiko akzeptiert, wiedereröffnet.
- Vorgänge müssen an definierte Gruppen, Queues oder Verantwortliche des UKF übergeben werden können (IT-Betrieb, Netzwerkbetrieb, Server-/Client-/VDI-Betrieb, Informationssicherheit, Medizintechnik, Datenschutz, Krisen- bzw. Rufbereitschaft).

11.4 Eskalation und Sofortkommunikation

- Die Ticketintegration ersetzt nicht die direkte Kommunikation bei kritischen Vorfällen. Für P1-Vorfälle, freigabepflichtige Response-Maßnahmen, Emergency Changes und dringende Eskalationen sind zusätzliche Sofortkommunikationswege vorzusehen (insbesondere telefonische Benachrichtigung, definierte Eskalationskontakte).

11.5 Ersatzverfahren

- Für den Fall, dass die Ticketintegration zeitweise nicht verfügbar ist, muss der Auftragnehmer ein abgestimmtes Ersatzverfahren vorsehen. Sicherheitsrelevante Vorgänge sind weiterhin fristgerecht zu melden, zu bearbeiten und nachträglich in das führende System zu übertragen.

12. SLA, Reporting und Eskalation

Die nachfolgenden Service Levels sind Bestandteil der laufenden Leistungserbringung. Vertragliche Sanktionen bei Nichterfüllung (Pönalen) sind in den Vergabeunterlagen außerhalb dieser Leistungsbeschreibung geregelt.

12.1 Prioritätsmodell

Priorität	Bezeichnung	Beschreibung
P1	Kritisch	Bestätigter oder hochwahrscheinlicher Sicherheitsvorfall mit unmittelbarem oder sehr hohem Schadenspotenzial (z. B. aktive Ransomware, Kompromittierung kritischer Identitäts-/Infrastrukturdienste, laterale Bewegung mit kritischem Ziel, erhebliche Beeinträchtigung klinischer Kernprozesse).
P2	Hoch	Bestätigter oder wahrscheinlicher Sicherheitsvorfall mit erheblichem Risiko (z. B. Malware-Infektion auf Servern, Command-and-Control-Kommunikation, kompromittierte Administratorkonten, gezielter Angriff auf kritische Systeme).
P3	Mittel	Sicherheitsrelevante Auffälligkeit oder bestätigter Vorfall mit begrenzter unmittelbarer Auswirkung, Analysebedarf oder erhöhter Beobachtungsnotwendigkeit.
P4	Niedrig	Informationsereignis oder gering priorisierte Auffälligkeit ohne unmittelbare kritische Auswirkung, jedoch mit Relevanz für Nachverfolgung, Optimierung oder Reporting.

- Die Priorisierung muss vom Auftragnehmer nachvollziehbar begründet werden. Reklassifizierungen sind zu dokumentieren.
- Maßgeblich für die Priorisierung ist die fachliche Auswirkung auf Verfügbarkeit, Integrität, Vertraulichkeit, Patientensicherheit, kritische Dienste und regulatorische Anforderungen, nicht die technische Herkunft des Ereignisses.

12.2 SLA-Kennzahlen

Die Bearbeitung sicherheitsrelevanter Vorfälle wird über vier Kennzahlen gemessen. Die Zeitmessung beginnt mit Erzeugung eines Alarms durch die Plattform und wird über das gesamte SOC-Team gemessen; sie darf nicht durch interne Übergaben des Auftragnehmers unterbrochen oder zu Lasten des UKF verlängert werden.

Kennzahl	Definition	P1	P2	P3
Time to Triage (TTT)	Zeit von Alarmerstellung bis zum Beginn der Analyse durch einen SOC-Analysten	≤ 15 Min	≤ 30 Min	≤ 60 Min
Time to Validate (TTV)	Zeit von Analysebeginn bis zur validierten Einstufung als Incident (True Positive)	≤ 30 Min	≤ 60 Min	≤ 4 Std

Kennzahl	Definition	P1	P2	P3
Time to Contain (TTC)	Zeit von Validierung bis zur ersten aktiven Eindämmungsmaßnahme im freigegebenen Rahmen	≤ 15 Min	≤ 30 Min	≤ 4 Std
Time to Notify (TTN)	Zeit von Validierung bis zur Benachrichtigung des UKF bei Eskalation oder Guided Response	≤ 15 Min	≤ 60 Min	≤ 2 Std

Servicezeit: P1 und P2 werden 24×7 bearbeitet. P3 und P4 werden grundsätzlich 8×5 bearbeitet, mit definierten Eskalationspfaden bei Lageänderung.

Für P4 gelten keine zeitlichen Bearbeitungs-SLAs; die Bearbeitung erfolgt im Regelreporting.

Ab dem Cut-over gemäß Kapitel 9.5 gelten die SLA-Kennzahlen für die Prioritäten P1 und P2 innerhalb des Mindestschutzzumfangs. Die SLA für die Priorität P3, die Reportingpflichten gemäß Kapitel 12.6 sowie die Plattformverfügbarkeit gemäß Kapitel 12.3 gelten ab dem Übergang in den Regelbetrieb.

- Stellt sich während der Analyse heraus, dass ein Vorfall niedrigerer Priorität tatsächlich kritischer einzustufen ist, muss eine Hochstufung erfolgen. Die zugehörigen schärferen SLAs greifen ab dem Zeitpunkt der Reklassifizierung.
- Die Bearbeitung erfolgt durch qualifiziertes Personal. Eine rein automatisierte Meldung ohne fachliche Bewertung erfüllt die SLA-Kennzahlen nicht.

12.3 Plattformverfügbarkeit

- Die Verfügbarkeit der vom Auftragnehmer betriebenen oder unmittelbar beeinflussbaren zentralen Plattformkomponenten (SIEM, NDR, IoMT-Plattform, Vulnerability Management sowie integrationsnahe Komponenten des EDR-Betriebs) muss mindestens 99,9 % im Monatsmittel betragen, gemessen außerhalb vereinbarter Wartungsfenster.
- Geplante Wartungsfenster werden vorab kalendarisch abgestimmt und dürfen klinische Betriebszeiten nicht beeinträchtigen.

12.4 Status-Updates

Priorität	Mindestintervall
P1	alle 30 Minuten oder bei wesentlicher Lageänderung
P2	alle 2 Stunden oder bei wesentlicher Lageänderung
P3	arbeitstäglich oder bei wesentlicher Lageänderung
P4	anlassbezogen oder im Regelreporting

- Status-Updates müssen mindestens enthalten: aktuellen Bearbeitungsstand, neue Erkenntnisse, durchgeführte oder empfohlene Maßnahmen, offene Entscheidungen, Risiken, nächste Schritte.

12.5 Eskalationsmodell

- Bei P1-Vorfällen muss zusätzlich zur Ticketmeldung eine direkte telefonische Benachrichtigung über einen abgestimmten Sofortkommunikationsweg erfolgen.
- Der Auftragnehmer muss einen 24x7-Sicherheitskontakt bereitstellen, der Eskalationen entgegennimmt, fachlich einordnet und die weitere Bearbeitung beim Auftragnehmer koordiniert.

Eskalationsstufen umfassen technische, fachliche und managementbezogene Ebenen sowie die Einbindung der UKF-Rufbereitschaft, fachlicher Betriebsgruppen, Informationssicherheit, Medizintechnik, Datenschutz und der Krisenorganisation.

12.6 Reportingpflichten

Bericht	Frequenz	Mindestinhalt
Operativer Servicebericht	monatlich	Sicherheitslage, Incidents (mit MITRE-Bezug), Alarmqualität, SLA-Erfüllung (TTT/TTV/TTC/TTN), Status Datenquellen, Schwachstellenlage, Rückfragen-Statistik, offene Maßnahmen, Verbesserungen
Strategic Business Review	quartalsweise	Trendbewertung, Servicequalität, strategische Risiken, größere Incidents, Maßnahmenstatus, Weiterentwicklung, Entscheidungsbedarfe
Incident-Abschlussbericht P1	binnen 5 Arbeitstagen	Ursache, Verlauf, Kill Chain, betroffene Systeme, Auswirkungen, Maßnahmen, verbleibende Risiken, Empfehlungen, Lessons Learned
Incident-Abschlussbericht P2	binnen 10 Arbeitstagen	Analoge Inhalte zu P1 in geeignetem Detailgrad
Jahresbericht Angriffserkennung	jährlich	Wirksamkeit, wesentliche Ereignisse, Trends, Verbesserungen
SzA-Nachweispaket (BSI)	jährlich + anlassbezogen	Datenquellen, Use Cases, Detektionslogiken, Eskalations- und Betriebsnachweise, SLA-Nachweise, Verbesserungen

- SLA-Abweichungen müssen unverzüglich analysiert, dokumentiert und im nächsten Servicebericht ausgewiesen werden. Bei P1- oder P2-Abweichungen ist eine gesonderte Ursachenanalyse vorzulegen.

Muster für Monatsreport, Service-Health-Report, Incident-Report und Threat-Hunting-Report sind als Angebotsbestandteil einzureichen.

13. Rollen und Verantwortlichkeiten

13.1 Rollen des Auftragnehmers

Rolle	Mindestverantwortung
Service Delivery Manager (deutschsprachig)	Zentrale fachliche Ansprechperson für Servicequalität, Eskalationen, Regelbetrieb, Reviews und kontinuierliche Verbesserung.
Fachlich-technische Security-Ansprechrolle	Sicherheitsarchitektur, Detection-Qualität, Use-Case-Weiterentwicklung, technische Eskalationen.
SOC-Verantwortliche / SOC-Leitung	Operative SOC-Leistung, Triage- und Analysequalität, Eskalationsfähigkeit, Steuerung der SOC-Ressourcen.
Security Analysten (L1/L2)	Monitoring, Triage, Investigation, Alarmbewertung, fachliche Vorbereitung von Incidents.
Incident Response Lead (L3 / DFIR)	Koordination schwerwiegender Sicherheitsvorfälle, Major Incidents, fachliche Abstimmung von Response-Maßnahmen.
Detection / Use-Case-Verantwortliche	Pflege und Weiterentwicklung von Use Cases, Detection-Regeln, Korrelationen und Playbooks.
Fachverantwortliche NDR / VM / EDR / IoMT	Fachliche Verantwortung für Betrieb, Integration, Auswertung und Weiterentwicklung der jeweiligen Domäne.
Transition- bzw. Projektleitung	Steuerung von Implementierung, Migration, Transition, Cut-over gemäß Kapitel 9.5, Abnahme und Übergang in den Regelbetrieb.

13.2 Rollen des Auftraggebers

Rolle / Stelle	Mindestverantwortung
IT-Leitung / Serviceverantwortung	Gesamtsteuerung des Dienstleistungsverhältnisses, Priorisierung, Eskalation, Abnahme.
Informationssicherheit / CISO	Fachliche Steuerung der Sicherheitsanforderungen, Risikobewertung, Priorisierung, regulatorische Anforderungen.
IT-Betrieb	Umsetzung technischer Maßnahmen, Bereitstellung von Systeminformationen, Mitwirkung bei Changes/Incidents/Wiederherstellung.
Netzwerkbetrieb	Bereitstellung relevanter Netz-, Sensorik-, Firewall-, Segmentierungsinformationen.
Server-/Client-/VDI-Betrieb	Mitwirkung bei EDR, Patching, Remediation, Systemhärtung, Wiederherstellung.
ServiceNow-Plattformverantwortung	Bereitstellung der ServiceNow-seitigen Schnittstellen, API-Zugänge, Berechtigungen und Konfigurationen für die bidirektionale Integration.

Rolle / Stelle	Mindestverantwortung
Medizintechnik	Fachliche Bewertung medizinisch geprägter Systeme, Freigabe von Maßnahmen mit Auswirkung auf Medizingeräte oder klinische Prozesse.
Datenschutz	Bewertung datenschutzrelevanter Fragestellungen, insbesondere bei klinischen Daten.
Krisen- / Rufbereitschaftsstruktur	Entgegennahme und Bearbeitung zeitkritischer Eskalationen (P1, Major Incidents).

13.3 RACI-Übersicht (Auszug)

Die vollständige RACI- und Kontaktmatrix ist im Betriebshandbuch zu führen und während der Vertragslaufzeit aktuell zu halten. Die nachfolgende Übersicht zeigt die wesentlichen Verantwortlichkeiten:

Aktivität	AN	UKF
Monitoring, Triage, Analyse	R/A	I
Incident-Bewertung und Eskalation	R/A	C/I
Response-Maßnahmen Standard-Endpunkte	R	A
Response-Maßnahmen klinisch-kritische Systeme	C	R/A
Use-Case-Pflege, Detection Engineering	R/A	C/I
Threat Hunting	R/A	I
Schwachstellenbewertung & Priorisierung	R/A	C
Patch-Umsetzung	C	R/A
Risikoakzeptanz	C	R/A
ServiceNow-Integration: Aufbau	R (AN-Seite)	R (UKF-Seite)
ServiceNow-Integration: Betrieb	R (AN-Seite)	R (UKF-Seite)
Übernahme der Serviceverantwortung (Cut-over)	R	A/C
Asset-Klassifizierung im Onboarding	R	R
Major Incident / Krisenmodus	R	A
Reporting & Service Reviews	R/A	C/I
Plattform- und Lizenzmanagement	R	A
Change Management produktive Mechanismen	R	A

R = Responsible (Durchführung); A = Accountable (Entscheidung); C = Consulted; I = Informed.

14. Exit Management

14.1 Auslöser und Grundsätze

Ein Exit-Prozess ist mindestens vorzusehen bei regulärem Vertragsende, Kündigung, Wechsel des Managed-Service-Dienstleisters, Rückübernahme einzelner oder aller Leistungen durch das UKF und Wechsel einzelner Plattformen oder Leistungsbereiche.

- UKF-Daten sowie kundenbezogene Konfigurationen, Regeln, Lizenzen und Betriebsartefakte müssen beim UKF verbleiben bzw. dem UKF in weiterverwendbarer Form zur Verfügung stehen. Eine dauerhafte Bindung an ausschließlich beim Auftragnehmer verfügbare kundenbezogene Artefakte ist ausgeschlossen. Vorbestehendes Know-how, Standardmethoden, Standard-Playbooks, generische Regelwerke und interne Werkzeuge des Auftragnehmers bleiben hiervon unberührt, sofern hierdurch keine faktische Abhängigkeit des UKF entsteht.
- Der laufende Sicherheitsbetrieb muss bis zum abgestimmten Übergabezeitpunkt ohne Reduktion der Leistungen fortgeführt werden.

14.2 Exit-Konzept

- Der Auftragnehmer muss spätestens im Rahmen der Transition ein Exit-Konzept vorlegen. Es wird mindestens jährlich sowie bei wesentlichen Änderungen aktualisiert.

Das Exit-Konzept umfasst Exit-Szenarien, Rollen und Verantwortlichkeiten, Phasenmodell, Mitwirkungsleistungen, Übergabeobjekte, Datenexport- und Übergabeverfahren, Kommunikations- und Eskalationswege, Risiken und Maßnahmen, Verfahren zur Betriebsfortführung sowie Lösch- und Rückgabeverfahren.

14.3 Übergabeobjekte

Im Exit-Fall werden folgende Artefakte strukturiert und vollständig übergeben:

- Betriebsdokumentation und Betriebshandbuch
- Architektur-, Schnittstellen- und Datenflussdokumentation
- Logquellen-, Sensorik- und Integrationskatalog
- UKF-spezifische Use Cases, Detection-Regeln, Korrelationslogiken, Playbooks und Runbooks
- Policies, Ausnahmen und Konfigurationen (SIEM, NDR, EDR, VM, IoMT)
- Asset- und Kritikalitätsklassifizierung
- Rollen-, Berechtigungs- und Kontaktmatrix (RACI)
- Reporting- und SLA-Nachweise
- Incident-, Change- und Service-Request-Historien
- Schwachstellen-, Asset- und Risikoinformationen
- Lizenz-, Tenant- und Vertragsinformationen, soweit vom Leistungsumfang betroffen
- offene Punkte, Risiken, Maßnahmenlisten und bekannte Einschränkungen

14.4 Datenexport und Löschung

- Sicherheitsrelevante Daten, Reports, Konfigurationen und Nachweise müssen im Exit-Fall in marktüblichen, weiterverarbeitbaren Formaten exportiert werden (z. B. CSV, JSON, native Plattform-Exporte) und über einen gesicherten Übertragungsweg übergeben werden.
- Nach bestätigter vollständiger Übergabe und Ablauf etwaiger Aufbewahrungspflichten muss der Auftragnehmer Daten des UKF nachweisbar löschen. Ein Löschprotokoll dokumentiert Art, Umfang, Speicherorte, Zeitpunkt, Verfahren und verantwortliche Stelle.

14.5 Lizenz- und Übergaberechte

- Das UKF muss im Rahmen der vereinbarten Lizenzmodelle über die für Weiterbetrieb, Übergabe und Nachweisführung erforderlichen Rechte verfügen. Ein Dienstleisterwechsel darf nicht zu Verlust von Lizenzen, Mandanten, Konfigurationen, Daten, Policies oder Betriebsartefakten führen.

14.6 Abnahme des Exit-Prozesses

- Der Exit gilt erst als abgeschlossen, wenn die vereinbarten Übergabeobjekte bereitgestellt, Datenexporte durchgeführt, offene Punkte dokumentiert und Löschrückgabenachweise erbracht sind. Der Abschluss wird durch ein Übergabe- bzw. Abnahmeprotokoll dokumentiert.

14.7 Unterstützung bei der Transition auf einen Nachfolgedienstleister

- Über die Übergabeobjekte gemäß Kapitel 14.3 hinaus unterstützt der Auftragnehmer den Auftraggeber und einen vom Auftraggeber benannten Nachfolgedienstleister bei der Herstellung der Betriebsfähigkeit. Diese Leistungen werden auf Abruf des Auftraggebers erbracht und gesondert vergütet; Art und Umfang der Vergütung regelt die Anlage [X], § 11 Abs. 5. Der Auftragnehmer kalkuliert den für diese Leistungen erforderlichen Aufwand auf Grundlage der in diesem Kapitel beschriebenen Leistungsinhalte eigenverantwortlich und bietet ihn als Gesamtbetrag über die optionale Position LV 14.1 des Preisblatts an. Dieser Gesamtbetrag bildet die Budgetobergrenze für die Leistungen nach diesem Kapitel.
- Strukturierter Wissenstransfer an die Mitarbeiter des Auftraggebers oder des Nachfolgedienstleisters zu Architektur, Datenflüssen, Logquellen, Detection-Regeln, Korrelationslogiken, Use Cases, Playbooks und Runbooks, einschließlich Klärung von Rückfragen während der Übernahme.
- Begleitung der Migration der Logquellen, Sensorik und Integrationen auf die Zielplattform des Nachfolgedienstleisters, einschließlich Unterstützung bei Validierung von Vollständigkeit und Funktionsfähigkeit der übernommenen Anbindungen.
- Unterstützung bei der Nachbildung der UKF-spezifischen Detection-Logik und Alarmierungswege in der Zielumgebung, einschließlich Erläuterung der Priorisierungslogik gemäß Kapitel 12.1.
- Unterstützung während eines vom Auftraggeber angeordneten Parallelbetriebs, in dem Bestands- und Zielplattform gleichzeitig instrumentiert sind, einschließlich Abstimmung zur Vermeidung doppelter Alarmierung und widersprüchlicher Reaktionsmaßnahmen.

-
- Teilnahme an Abstimmungs- und Übergabeterminen mit dem Auftraggeber und dem Nachfolgedienstleister sowie Mitwirkung an der Erstellung des Übergabe- bzw. Abnahmeprotokolls.
 - Unterstützung bei der Übergabe der regulatorischen Meldefähigkeit (§ 32 BSIG, Art. 33 DSGVO), einschließlich Übergabe der abgestimmten Meldevorlagen, Rollen und Eskalationskontakte.
 - Während eines Parallelbetriebs bleibt die Verantwortung für Erkennung, Bewertung und Reaktion bei dem Dienstleister, der die jeweilige Leistung nach dem vom Auftraggeber festgelegten Übergabeplan schuldet. Der Auftraggeber legt für jeden Leistungsbereich den Zeitpunkt des Verantwortungsübergangs fest und dokumentiert ihn im Übergabeprotokoll. Bis zu diesem Zeitpunkt gelten die Service Levels des Auftragnehmers unverändert fort.

Universitätsklinikum Frankfurt / Universitätsmedizin Frankfurt (UKF)

Vergabeverfahren Cybersecurity Managed Services

D3 - Zuschlagskriterien und Bewertungsmatrix

Verhandlungsverfahren mit Teilnahmewettbewerb (§§ 17 ff. VgV, EU-Schwellenwert)

Stand 20.08.2026

Bezugsdokumente: D1 - Leistungsbeschreibung (LV v7); D4 - Anforderungen an die Lösungsansätze; D5 - Preis matrix.

1 Gesamtbewertung und Rangbildung

Die Gesamtwertungssumme eines Angebots ergibt sich aus der Summe der Punkte für Preis und Qualität. Die maximale Gesamtwertungssumme beträgt 100 Punkte.

Wertungsbereich	Gewichtung	Max. P.	Min. P.
Preis (Wertungssumme über 60 Monate)	40 %	40	0
Qualität - Lösungskonzept (4 Themenfelder)	60 %	60	0
Gesamtwertungssumme	100 %	100	0

Die Qualitätspunktzahl (max. 60) setzt sich aus den vier Themenfeldern des Lösungskonzepts (Dokument D4) zusammen. Alle Themenfelder sind gleich gewichtet.

Themenfeld	Gewichtung	Max. P.
Themenfeld 1 - Implementierung, Transition & Migration	15 %	15
Themenfeld 2 - Managed Service Design & Betriebsorganisation	15 %	15
Themenfeld 3 - Technisches Lösungskonzept (Erkennung, Zielarchitektur, Datenhoheit & Exit)	15 %	15
Themenfeld 4 - IoMT-Sicherheitskonzept	15 %	15
Qualität gesamt	60 %	60

Den Zuschlag erhält das Angebot mit der höchsten Gesamtwertungssumme.

Eine Mindestpunktschwelle je Themenfeld ist nicht vorgesehen. Ein Verstoß gegen eine in D1 als nicht verhandelbar bezeichnete Leitplanke oder ein erkennbares Vendor-Lock-in-Risiko wirkt sich in dem betroffenen Themenfeld bewertungsmindernd bis hin zur Stufe 'Ungenügend' aus. Die Einstufung erfolgt nach Maßgabe der themenspezifischen Indikatorenkataloge unter Berücksichtigung der Schwere des Verstoßes.

2 Preisbewertung

2.1 Wertungssumme

Grundlage der Preisbewertung ist die Wertungssumme des Angebots. Diese umfasst die wertungsrelevanten Positionen des Preisblatts (Dokument D5 - Preis matrix) über die Vertragslaufzeit von 60 Monaten, die mit dem Cut-over gemäß D1 Kapitel 9.5 beginnt. Sie setzt sich zusammen aus den einmaligen Kosten (Implementierung, Feinkonzeption, Migration, Übernahme der Serviceverantwortung zum Cut-over, Schulung sowie der Lizenzanschluss der Bestandsplattformen

für einen Zwischenzeitraum) und den laufenden Kosten (Managed Services, Plattformbetrieb, Lizenzen sowie der Ramp-up-Betrieb zwischen Cut-over und Regelbetrieb). Optionale Positionen sind gemäß Preisblatt nicht wertungsrelevant und fließen nicht in die Wertungssumme ein.

2.2 Bewertungsmethode (UfAB-Interpolationsmethode)

Die Preisbewertung erfolgt nach der Interpolationsmethode der UfAB (Unterlage für Ausschreibung und Bewertung von IT-Leistungen). Das Angebot mit der niedrigsten Wertungssumme erhält die maximale Punktzahl von 40 Punkten. Die Wertungssumme jedes weiteren Angebots wird linear in Bezug auf die niedrigste Wertungssumme bewertet. Ab einer Wertungssumme, die das Doppelte der niedrigsten Wertungssumme beträgt oder übersteigt, wird die Punktzahl 0 vergeben.

2.3 Berechnungsformel

$$P = 40 \times (2 - \text{WS-Angebot} / \text{WS-min}), \text{ begrenzt auf } 0 \leq P \leq 40$$

mit WS-Angebot = Wertungssumme des zu bewertenden Angebots und WS-min = niedrigste Wertungssumme aller wertbaren Angebote.

2.4 Berechnungsbeispiel

Zur Veranschaulichung der Methodik dient das folgende Beispiel.

Bieter	Wertungssumme (EUR)	Verhältnis zu WS-min	Preispunkte
Bieter A (günstigster)	6.000.000	1,00	40,00
Bieter B	7.200.000	1,20	32,00
Bieter C	9.000.000	1,50	20,00
Bieter D	12.000.000 (Cap)	2,00	0,00

Preispunkte werden auf zwei Nachkommastellen kaufmännisch gerundet.

3 Qualitätsbewertung

3.1 Notensystem

Je Themenfeld sind maximal 15 Punkte erreichbar. Je Themenfeld wird auf Basis des Gesamteindrucks über alle Bereiche (A, B, C...) genau eine der folgenden sechs Bewertungsstufen vergeben. Den Stufen sind feste Punktwerte zugeordnet; Zwischenwerte sind nicht zulässig.

Bewertungsstufe	Punkte	Bedeutung (übergreifend)
Sehr gut	15	Die Darstellung ist fachlich substantiell, durchgängig argumentativ begründet und zeigt belastbaren KRITIS- und Klinikbezug. Alle Bereiche des Themenfelds sind konkret und nachvollziehbar behandelt.
Gut	12	Die Darstellung ist überwiegend konkret und nachvollziehbar; KRITIS- und Klinikbezug ist klar erkennbar. Vereinzelt Aspekte bleiben allgemein gehalten oder weniger ausgearbeitet.
Befriedigend	9	Die Darstellung erfüllt die Anforderungen formal. Konkrete KRITIS- und Klinikbezüge sind nur stellenweise erkennbar; Teile des Themenfelds bleiben generisch.

Bewertungsstufe	Punkte	Bedeutung (übergreifend)
Ausreichend	6	Die Darstellung deckt die Themen formal ab, bleibt aber überwiegend generisch. KRITIS- und Klinikbezug fehlt weitgehend; einzelne wesentliche Aspekte sind nicht erkennbar behandelt.
Mangelhaft	3	Wesentliche Inhalte einzelner Bereiche fehlen oder bleiben unklar. Die Darstellung wirkt schablonenhaft; kein erkennbarer KRITIS- und Klinikbezug.
Ungenügend	0	Das Themenfeld ist nicht oder nur fragmentarisch behandelt. Inhalte sind ohne fachliche Substanz oder ohne Bezug zur Aufgabenstellung.

3.2 Bewertungsdimensionen und Abgrenzung zur Eignung

Bewertet wird ausschließlich die Qualität des im Lösungskonzept dargestellten Vorgehens für die ausgeschriebene Leistung. Die Eignung, Referenzlage oder Vorerfahrung des Bieters wird im Teilnahmewettbewerb (Dokument D2) geprüft und fließt nicht in die Zuschlagswertung ein.

Die Bewertungskommission bezieht bei der Notenfindung die folgenden übergreifenden Dimensionen in die themenspezifischen Indikatoren ein:

- Fachliche Tiefe und argumentative Qualität der dargestellten Vorgehensweise.
- Konkretheit und KRITIS-/Klinikbezug der Aussagen (gegenüber generischen, branchenneutralen Ausführungen).
- Belastbarkeit der genannten Verfahren und Maßnahmen.
- Vollständigkeit der Behandlung der definierten Bereiche (A, B, C ...) im Themenfeld.
- Plausibilität und Nachvollziehbarkeit der Schlussfolgerungen.

Die nachfolgenden Indikatorenkataloge der Themenfelder 1 bis 4 konkretisieren die Bewertungsstufen entlang dieser Dimensionen.

4 Indikatorenkatalog Themenfeld 1: Implementierung, Transition & Migration

Bewertet werden die Belastbarkeit des Vorgehens beim Übergang vom Altdienstleister einschließlich der Erreichung des Cut-over-Fixtermins zum 31.05.2027, beim Aufbau der Plattformkomponenten, bei der EDR-Migration sowie das Risikomanagement im Klinikbetrieb. Bezugsdokument: D4 - Anforderungen an die Lösungsansätze, Themenfeld 1 (Bereiche A bis E).

Bewertungsstufe	Themenspezifische Indikatoren
Sehr gut 15 Punkte	• Service Ownership Transfer ist konkret, klinikspezifisch und stützt sich auf ein belastbares Vorgehensmodell für vergleichbare KRITIS-Umgebungen; das Vorgehen bei unvollständiger Dokumentation ist nachvollziehbar. • Phasenmodell und Cut-over-Strategie sind nachvollziehbar dargestellt mit klaren Entscheidungspunkten, Abnahmegates und Behandlung des Parallelbetriebs. • EDR-Migration zeigt einen wellenbasierten Rollout mit definierten Pilotphasen, expliziter Behandlung klinisch-kritischer Systemklassen und nachvollziehbarer Vermeidung von Schutzlücken-Fenstern. • Risikomanagement und Rückfallszenarien sind klinikbezogen ausformuliert (OP, Intensivmedizin, Notaufnahme, Bildgebung) - nicht generisch.

Bewertungsstufe	Themenspezifische Indikatoren
	● Ressourcenplanung und Wissenstransfer sind über den Zeitverlauf belastbar dargestellt; Verfügbarkeit von Schlüsselpersonal und formaler Übergabeprozess an den Regelbetrieb sind erkennbar. ● Die Erreichung des Meilensteins M1 (Cut-over 31.05.2027) ist im Projektplan belastbar nachgewiesen; Mindestschutzzumfang nach D1 Kapitel 9.5, Abnahmeverfahren und Ramp-up-Betrieb sind vollständig und konkret dargestellt.
Gut 12 Punkte	● Vorgehen ist überwiegend konkret und nachvollziehbar; KRITIS- und Klinikbezug ist erkennbar, stellenweise jedoch allgemein gehalten. ● Phasenmodell und Cut-over-Logik sind plausibel; einzelne Entscheidungspunkte oder Abnahmepunkte bleiben unscharf. ● EDR-Migration ist strukturiert dargestellt; einzelne Aspekte (z. B. Behandlung von Schutzlücken-Fenstern in Pilotphasen) bleiben weniger konkret. ● Risiken im Klinikbetrieb sind benannt; Rückfallszenarien und Eskalationsregeln nur teilweise ausformuliert. ● Ressourcenplanung ist nachvollziehbar; Wissenstransfer-Konzept überwiegend vorhanden, ohne durchgängige Tiefe. ● Die Erreichung des Meilensteins M1 ist plausibel dargestellt; einzelne Aspekte des Mindestschutzzumfangs, der Abnahme oder des Ramp-up-Betriebs bleiben unscharf.
Befriedigend 9 Punkte	● Vorgehen erfüllt die Anforderungen formal; konkrete KRITIS- und Klinikbezüge sind nur stellenweise erkennbar. ● Phasenmodell ist generisch beschrieben, ohne erkennbaren Bezug zur UKF-Spezifik; Cut-over-Kriterien bleiben unscharf. ● EDR-Migration auf Standardvorgehen beschränkt; keine klare Wellenstrategie oder spezifische Behandlung klinisch-kritischer Systeme. ● Risikomanagement bleibt allgemein; konkrete Maßnahmen für klinische Bereiche fehlen weitgehend. ● Ressourcenplanung und Wissenstransfer sind nur in Grundzügen erkennbar. ● Der Meilenstein M1 wird benannt, der Nachweis der Erreichung bleibt jedoch generisch; Mindestschutzzumfang und Ramp-up-Betrieb sind nur in Grundzügen erkennbar.
Ausreichend 6 Punkte	● Konzept deckt die Themen formal ab, bleibt aber im Wesentlichen generisch; KRITIS- und Klinikbezug fehlt weitgehend. ● Phasenmodell, Cut-over-Logik, Migrationsstrategie und Risikomanagement bleiben oberflächlich. ● Einzelne wesentliche Aspekte (z. B. Behandlung klinisch-kritischer Bereiche, Rollback-Pläne, Schutzlücken-Vermeidung) sind nicht erkennbar. ● Wissenstransfer und Übergabeprozess an den Regelbetrieb sind kaum ausgearbeitet. ● Aussagen zu Meilenstein M1, Mindestschutzzumfang und Ramp-up-Betrieb bleiben oberflächlich oder unvollständig.
Mangelhaft	● Wesentliche Inhalte einzelner Bereiche fehlen oder bleiben unklar.

Bewertungsstufe	Themenspezifische Indikatoren
3 Punkte	● Vorgehen wirkt schablonenhaft; kein erkennbarer KRITIS- und Klinikbezug. ● Stellungnahme zu Risiken, Rückfallszenarien oder zur Vermeidung von Schutzlücken-Fenstern fehlt oder ist nicht belastbar. ● Ressourcenplanung ohne Bezug zur Lastsituation des Vorhabens. ● Ein Nachweis zur Erreichung des Meilensteins M1 zum 31.05.2027 fehlt oder ist nicht belastbar.
Ungenügend 0 Punkte	● Themenfeld nicht oder nur fragmentarisch behandelt. ● Inhalte ohne fachliche Substanz oder ohne Bezug zur Aufgabenstellung.

5 Indikatorenkatalog Themenfeld 2: Managed Service Design & Betriebsorganisation

Bewertet werden die Tragfähigkeit der 24/7-Betriebsorganisation, die Einbindung in die UKF-ITSM-Landschaft (ServiceNow), die Steuerung der Incident-/Problem-/Change-/Reporting-Prozesse, der Schwachstellen-Service im laufenden Betrieb und die Krisenfähigkeit des SOC-Betriebs über die Vertragslaufzeit. Bezugsdokument: D4 - Anforderungen an die Lösungsansätze, Themenfeld 2 (Bereiche A bis E).

Bewertungsstufe	Themenspezifische Indikatoren
Sehr gut 15 Punkte	● SOC-Betriebsorganisation ist klar und nachvollziehbar dargestellt: Schichtmodell, Tier-Struktur, deutschsprachige Abdeckung, Skalierbarkeit bei Lastspitzen, Standorte (EU-Datenhoheit) und kontinuierliche Besetzung der SDM-Rolle über die Vertragslaufzeit. ● ServiceNow-Integration ist architektonisch nachvollziehbar dargestellt (E-Bonding, Verantwortlichkeiten an der Schnittstelle, Vorgehen bei API-/Schema-Änderungen); Vorqualifizierung und Vermeidung von Ticket-Spam sind konkret adressiert. ● Event-to-Incident-Workflow zeigt eine echte Qualifizierung mit kontextbezogener Priorisierung; Eskalationsmodell ist klar bis hin zur UKF-Rufbereitschaft. ● Change-Management ist mit dem UKF-CAB verzahnt; Reporting-Konzept ist operativ und strategisch differenziert und mit Continuous-Improvement-Logik unterlegt. ● Business Continuity ist konkret: Verhalten bei Teilausfällen, Supply-Chain-Vorfällen, KRITIS-Meldepflichten gemäß § 32 BSIG (i.d.F. NIS-2-Umsetzungsgesetz) und Mitwirkung bei UKF-Krisenübungen sind belastbar adressiert. ● Der Schwachstellen-Service ist durchgängig dargestellt: kontextbezogene Priorisierung im klinischen Umfeld, Umgang mit nicht patchbaren medizintechnischen Systemen und Remediation-Tracking bis zur dokumentierten Schließung oder Risikoakzeptanz.
Gut 12 Punkte	● SOC-Organisation ist klar strukturiert; vereinzelte Aspekte (z. B. Behandlung von Lastspitzen, kontinuierliche Besetzung der SDM-Rolle) bleiben weniger konkret.

Bewertungsstufe	Themenspezifische Indikatoren
	- ServiceNow-Integration ist plausibel beschrieben; Vorgehen bei API-/Schema-Änderungen oder Asset-/CMDB-Inkonsistenzen bleibt teilweise allgemein. - Event-to-Incident-Workflow und Eskalationsmodell sind nachvollziehbar; Reporting-Konzept ist vorhanden, aber Continuous-Improvement-Logik nur ansatzweise erkennbar. - Business Continuity ist überwiegend behandelt; Verhalten bei eigenen Vorfällen oder konkrete Unterstützung bei KRITIS-Meldepflichten weniger ausgearbeitet. - Der Schwachstellen-Service ist nachvollziehbar dargestellt; Priorisierungslogik oder Remediation-Tracking bleiben in Teilen allgemein.
Befriedigend 9 Punkte	- SOC-Organisation ist im Grundsatz beschrieben, aber wesentliche Spezifika (deutschsprachige Abdeckung über die Vertragslaufzeit, Standorte mit EU-Bezug, Skalierbarkeit) bleiben unkonkret. - ServiceNow-Integration auf Verfügbarkeitsbeschreibung beschränkt; Architektur, Verantwortlichkeiten an der Schnittstelle und Vorqualifizierung sind nicht überzeugend ausgearbeitet. - Eskalationsmodell und Reporting sind vorhanden, aber generisch; Change-Management ohne erkennbare Verzahnung mit dem UKF. - Business Continuity wird oberflächlich behandelt; Unterstützung bei KRITIS-Meldepflichten kaum konkret. - Der Schwachstellen-Service ist in Grundzügen beschrieben; der klinische Priorisierungskontext bleibt unscharf.
Ausreichend 6 Punkte	- SOC-Organisation und ServiceNow-Integration werden formal benannt, ohne tiefergehende Argumentation. - Event-to-Incident-Workflow nur als Alarm-Weiterleitung beschrieben; keine erkennbare Qualifizierungs- oder Priorisierungslogik. - Reporting-Konzept und Continuous-Improvement-Logik kaum ausgearbeitet. - Business Continuity bleibt allgemein und ohne KRITIS-Bezug. - Aussagen zum Schwachstellen-Service bleiben oberflächlich; der Umgang mit nicht patchbaren Systemen fehlt weitgehend.
Mangelhaft 3 Punkte	- Wesentliche Inhalte einzelner Bereiche fehlen; Darstellung wirkt schablonenhaft. - ServiceNow-Integration nur als Behauptung; keine Architektur oder Verantwortlichkeiten erkennbar. - Eskalationsmodell und Krisenfähigkeit nicht belastbar. - Kein erkennbarer Klinik-/KRITIS-Bezug im dargestellten Betriebskonzept. - Der Schwachstellen-Service ist nicht oder nicht belastbar dargestellt.
Ungenügend 0 Punkte	- Themenfeld nicht oder nur fragmentarisch behandelt. - Inhalte ohne fachliche Substanz oder ohne Bezug zur Aufgabenstellung.

6 Indikatorenkatalog Themenfeld 3: Technisches Lösungskonzept - Erkennung, Zielarchitektur, Datenhoheit & Exit

Themenfeld 3 ist das zentrale fachliche Differenzierungsfeld zwischen den Bietern. Bewertet werden Detection-Engineering und SOC-Wirksamkeit, Zielarchitektur und Plattform-Integration sowie die Belastbarkeit der nicht verhandelbaren Anforderungen Datenhoheit, Lizenzhoheit und Exit. Bezugsdokument: D4 - Anforderungen an die Lösungsansätze, Themenfeld 3 (Bereiche A bis C).

Bewertungsstufe	Themenspezifische Indikatoren
Sehr gut 15 Punkte	● Detection-Engineering-Lifecycle ist als Prozess nachvollziehbar dargestellt (Hypothese, Validierung, Produktivsetzung, Pflege, Außerbetriebnahme); MITRE-ATT&CK-Coverage und systematische Schließung von Coverage-Lücken sind nachvollziehbar dargestellt. ● Threat-Intelligence-Operationalisierung und Threat Hunting (Frequenz, Hypothesen-Framework, Output gegenüber UKF) sind belastbar dargestellt; Grenzen sinnvoller SOAR-Automatisierung im Klinikumfeld sind reflektiert. ● Zielarchitektur ist schematisch dargestellt mit klarer Korrelations- und Datenflusslogik; Veränderungsfähigkeit (neue Logquellen, Standorte, RZ-Umzüge) ist ohne Zusatzprojekte gewährleistet. ● Hochverfügbarkeit, Resilienz und herstelleroffene Integration zu UKF-Bestandssystemen (AD, Entra ID/ADFS, ServiceNow, Mailsecurity, IDS/IPS, NAC, WAF, PAM) sind konkret und nachvollziehbar. ● Datenhoheit, Lizenzhoheit und Exit sind belastbar adressiert: Rohdatenhaltung beim UKF (mindestens 12 Monate Aufbewahrung, davon mindestens 90 Tage Hot Storage), EU-Verarbeitung, BYOL-Trennung und vollständige Übergabbarkeit an einen Folgedienstleister ohne Neurollout.
Gut 12 Punkte	● Detection-Engineering-Lifecycle und MITRE-ATT&CK-Coverage sind plausibel beschrieben; einzelne Aspekte (Coverage-Lücken-Schließung, Tuning-Schleife) bleiben weniger konkret. ● Threat-Hunting-Konzept und SOAR-Abgrenzung sind vorhanden, aber stellenweise allgemein gehalten. ● Zielarchitektur und Plattform-Integration sind nachvollziehbar; Veränderungsfähigkeit ist im Wesentlichen gewährleistet, einzelne Szenarien (z. B. RZ-Umzug) bleiben unspezifisch. ● Datenhoheit, Lizenzhoheit und Exit sind überwiegend belastbar; einzelne Aspekte (z. B. Behandlung von Sub-Auftragsverarbeitung, Übergabbarkeit der Detection-Regeln) sind weniger ausgearbeitet.
Befriedigend 9 Punkte	● Detection-Engineering wird als Prozess benannt; Lifecycle-Logik und MITRE-ATT&CK-Bezug bleiben unkonkret. ● Zielarchitektur ist auf Verfügbarkeitsdiagramm reduziert; Korrelations- und Datenflusslogik nicht klar erkennbar; Veränderungsfähigkeit nur generisch behauptet. ● Datenhoheit und Exit sind formal adressiert, aber ohne konkrete Aussage zur Krisenfähigkeit oder zur Übergabbarkeit ohne Neurollout. ● Herstelleroffene Integration zu UKF-Bestandssystemen wird behauptet, aber nicht belegt.
Ausreichend 6 Punkte	● Detection-Engineering und Threat Hunting werden lediglich erwähnt; keine erkennbare methodische Tiefe.

Bewertungsstufe	Themenspezifische Indikatoren
	● Zielarchitektur bleibt auf Komponentenliste beschränkt; keine Integrationslogik mit UKF-Bestandssystemen. ● Datenhoheit und Exit sind nur als Aussage vorhanden; konkrete Maßnahmen, Mindestaufbewahrungsfristen oder Übergabe-Artefakte fehlen. ● BYOL-Trennung wird nicht überzeugend nachgewiesen.
Mangelhaft 3 Punkte	● Wesentliche Inhalte einzelner Bereiche fehlen oder bleiben widersprüchlich. ● Detection-Engineering nicht erkennbar als systematischer Prozess. ● Datenhoheit, Lizenzhoheit oder Exit weisen erhebliche Lücken oder ein Vendor-Lock-in-Risiko auf, das nicht adressiert wird.
Ungenügend 0 Punkte	● Themenfeld nicht oder nur fragmentarisch behandelt. ● Inhalte ohne fachliche Substanz oder im Widerspruch zu den nicht verhandelbaren Leitplanken (Datenhoheit, BYOL, EU-Verarbeitung, Exit).

7 Indikatorenkatalog Themenfeld 4: IoMT-Sicherheitskonzept

Bewertet wird, ob das angebotene Konzept den klinischen Betrieb und die Eigenheiten der Medizintechnik (Herstellerabhängigkeit, Spezialprotokolle, klinische Kritikalität, MDR-/MDS2-Kontext) sachgerecht adressiert und die nicht verhandelbaren Leitplanken (passives Monitoring, Human-in-the-Loop, Anonymisierung klinischer Protokolldaten) belastbar einhält. Bezugsdokument: D4 - Anforderungen an die Lösungsansätze, Themenfeld 4 (Bereiche A bis E).

Bewertungsstufe	Themenspezifische Indikatoren
Sehr gut 15 Punkte	● Architektur des passiven Monitorings ist konkret beschrieben; Sensor-Topologie sowie Spiegelports/TAPs sind nachvollziehbar dargestellt. ● Asset Discovery und Klassifizierung der rund 5.000 Geräte sind nachvollziehbar dargestellt; Verarbeitung gesundheitswesensspezifischer Protokolle (DICOM, HL7, FHIR) und Risikobewertung mit MDS2-Daten und kompensierenden Maßnahmen sind belastbar. ● Anomalie-Erkennung und Threat-Intelligence-Einbindung sind konkret; SIEM-Schnittstelle ist hinsichtlich Schweregrad-Filter, Anreicherung und Eskalationspfaden klar definiert. ● Reaktionsmodell mit Human-in-the-Loop ist konsistent dargestellt; Schnittstelle zur UKF-Medizintechnik (Eskalationspfade, Rollenmodell, Entscheidungsbefugnisse) und Behandlung freigabepflichtiger Mikrosegmentierungs-Maßnahmen sind belastbar. ● Anonymisierung/Pseudonymisierung klinischer Protokolldaten und Trennung von Sicherheitsmetadaten und klinischen Inhaltsdaten sind konkret adressiert; DSGVO-Konformität nachvollziehbar.
Gut 12 Punkte	● Architektur und Asset Discovery sind plausibel beschrieben; einzelne Aspekte (Skalierbarkeit der Sensor-Platzierung, MDS2-Integration) bleiben weniger konkret.

Bewertungsstufe	Themenspezifische Indikatoren
	● Anomalie-Erkennung und SIEM-Schnittstelle sind nachvollziehbar; Eskalationspfade zwischen IoMT-Spezialisten und SOC-Tier könnten klarer sein. ● Reaktionsmodell ist im Grundsatz konsistent; Schnittstelle zur UKF-Medizintechnik bleibt teilweise allgemein. ● Anonymisierung klinischer Protokolldaten ist behandelt; einzelne Verfahren oder die Trennung Sicherheits- vs. Inhaltsdaten sind weniger ausgearbeitet.
Befriedigend 9 Punkte	● Architektur des passiven Monitorings ist auf Sensor-Konzept beschränkt; klinische Topologie-Spezifika fehlen. ● Asset Discovery und Risikobewertung bleiben generisch; keine erkennbare Verarbeitung gesundheitswesensspezifischer Protokolle oder MDS2-Daten. ● Reaktionsmodell ist formal mit Human-in-the-Loop ausgestattet, ohne klare Schnittstelle zur UKF-Medizintechnik. ● Anonymisierung klinischer Protokolldaten wird behauptet, aber nicht methodisch unterlegt.
Ausreichend 6 Punkte	● Konzept benennt die Themen formal, ohne klinikspezifische Tiefe. ● Anomalie-Erkennung und SIEM-Schnittstelle bleiben oberflächlich. ● Reaktionsmodell ohne überzeugende Behandlung des klinisch-kritischen Segments. ● Datenschutz und Anonymisierung sind nur als Aussage vorhanden; konkrete Verfahren fehlen.
Mangelhaft 3 Punkte	● Wesentliche Inhalte einzelner Bereiche fehlen; klinische Kritikalität und Patientensicherheit sind nicht erkennbar adressiert. ● Reaktionsmodell ohne erkennbares Human-in-the-Loop-Konzept oder mit Risiko automatischer Quarantäne in klinisch-kritischen Bereichen. ● Anonymisierung klinischer Protokolldaten nicht belastbar oder im Widerspruch zu DSGVO-Anforderungen.
Ungenügend 0 Punkte	● Themenfeld nicht oder nur fragmentarisch behandelt. ● Inhalte ohne fachliche Substanz oder im Widerspruch zu den nicht verhandelbaren Leitplanken (passives Monitoring, Human-in-the-Loop, Anonymisierung klinischer Protokolldaten).

8 Ranggleichheit und Verfahrenshinweise

8.1 Auflösung von Ranggleichheit

Erreichen mehrere Angebote nach Anwendung der vorstehenden Bewertungsmethodik dieselbe Gesamtwertungssumme, wird der Zuschlag in folgender Reihenfolge bestimmt:

- Vorrang erhält das Angebot mit der höheren Qualitäts-Punktzahl (Summe aus den Themenfeldern 1 bis 4, maximal 60 Punkte).
- Besteht weiterhin Ranggleichheit, erhält das Angebot Vorrang, das im Themenfeld 3 (Technisches Lösungskonzept) die höhere Punktzahl erreicht hat.

- Besteht weiterhin Rangleichheit, entscheidet das Los unter Aufsicht des Auftraggebers.

8.2 Trennung von Eignung und Zuschlag

Die Eignungsprüfung (Dokument D2) und die Zuschlagswertung (dieses Dokument) sind strikt getrennt. Eignungsnachweise, Referenzen und Umsatzangaben werden nicht erneut im Rahmen der Zuschlagswertung berücksichtigt. Grundlage der Qualitätsbewertung ist ausschließlich das eingereichte Lösungskonzept gemäß Dokument D4.

Universitätsklinikum Frankfurt / Universitätsmedizin Frankfurt (UKF)

Vergabeverfahren Cybersecurity Managed Services

D4 – Anforderungen an die Lösungsansätze

Vorgaben für das vom Bieter einzureichende Lösungskonzept

Verhandlungsverfahren mit Teilnahmewettbewerb (§§ 17 ff. VgV, EU-Schwellenwert)

Stand 20.08.2026

Bezugsdokumente: D1 – Leistungsbeschreibung (LV v7, verbindliche Anforderungen); D3 – Zuschlagskriterien und Bewertungsmatrix (Bewertung dieses Konzepts); D5 – Preismatrix (Preisblatt).

1 Zweck und Einordnung

Dieses Dokument fordert die Bieter auf, in einem strukturierten Lösungskonzept darzulegen, wie sie die in Dokument D1 (Leistungsbeschreibung) verbindlich geforderten Leistungen erbringen. Bewertet wird das Lösungskonzept nach den in Dokument D3 (Zuschlagskriterien und Bewertungsmatrix) festgelegten Kriterien.

Die drei Dokumente stehen in folgendem Verhältnis zueinander:

- D1 – Leistungsbeschreibung: legt fest, WAS zu leisten ist (verbindliche Muss- und Soll-Anforderungen).
- D4 – Anforderungen an die Lösungsansätze (dieses Dokument): fragt, WIE der Bieter die Leistung erbringt (argumentative Leitfragen je Themenfeld).
- D3 – Zuschlagskriterien und Bewertungsmatrix: legt fest, WIE das Konzept bewertet wird (sechsstufige Benotung je Themenfeld).

Das Lösungskonzept soll die Anforderungen aus D1 nicht wiederholen, sondern das eigene Vorgehen konkret, klinikbezogen und nachvollziehbar begründen. Die in D1 benannten nicht verhandelbaren Leitplanken (insbesondere Datenhoheit, Lizenzhoheit im Modell „Lizenzen im Eigentum des Auftraggebers“, ausschließliche Verarbeitung in der Europäischen Union, Exit-Fähigkeit sowie – für vernetzte Medizingeräte – passives Monitoring, menschliche Entscheidung vor Eingriffen und Anonymisierung klinischer Protokolldaten) sind einzuhalten; darzustellen ist das Wie, nicht das Ob.

2 Formale Vorgaben für das Lösungskonzept

Das Lösungskonzept ist entlang der nachfolgenden vier Themenfelder und ihrer Bereiche zu gliedern. Für jedes Themenfeld gilt eine Seitenobergrenze. Seiten, die über die jeweilige Obergrenze hinausgehen, werden nicht gewertet. Die Gliederung (Themenfeld, Bereich A, B, C ...) ist beizubehalten.

Themenfeld	Max. Seiten	Punkte (D3)
Themenfeld 1 – Implementierung, Transition & Migration	6	15
Themenfeld 2 – Managed Service Design & Betriebsorganisation	6	15
Themenfeld 3 – Technisches Lösungskonzept (Erkennung, Zielarchitektur, Datenhoheit & Exit)	8	15

Themenfeld	Max. Seiten	Punkte (D3)
Themenfeld 4 – IoMT-Sicherheitskonzept	6	15
Summe Lösungskonzept	26	60

- Sprache: Deutsch. Format: durchsuchbares PDF-Dokument (Portable Document Format).
- Schriftgröße mindestens 10 Punkt; Diagramme und Abbildungen zählen zur Seitenobergrenze.
- Deckblatt, Inhaltsverzeichnis und ein Abkürzungsverzeichnis zählen nicht zur Seitenobergrenze.
- Verweise auf Anlagen ersetzen keine geforderten Aussagen im Konzept; bewertet wird ausschließlich der Text innerhalb der Seitenobergrenze.

3 Themenfeld 1: Implementierung, Transition & Migration

Bezug: D1 – Leistungsbeschreibung, Kapitel 9 (Implementierung und Transition, insbesondere Kapitel 9.5 Übergang der Serviceverantwortung und Ramp-up-Betrieb) sowie Kapitel 7 (Leistungsbereich EDR-Management). Bewertung: D3, Themenfeld 1.

Der Bieter legt dar, wie er den Übergang vom bestehenden Dienstleister, den Aufbau der Plattformkomponenten, die Migration der Endpoint-Detection-and-Response-Plattform (EDR) und das Risikomanagement im laufenden Klinikbetrieb gestaltet. Maßgeblich ist ein zu keinem Zeitpunkt unterbrochener Schutz. Der bestehende Managed-Service-Vertrag des Auftraggebers für die Leistungsbereiche SOC/SIEM und EDR-Management endet am 31.05.2027; die Übernahme der Serviceverantwortung im Mindestschutzzumfang nach D1 Kapitel 9.5 ist ein Fixtermin. Der Vertrags- und Projektbeginn erfolgt spätestens am 01.02.2027; die Lizenzen der Bestandsplattformen für NDR und Vulnerability Management laufen bis zum 30.09.2027.

Bitte gehen Sie im Lösungskonzept auf die folgenden Bereiche und Leitfragen ein:

3.1 Bereich A: Übernahme der Serviceverantwortung vom Altdienstleister

- Wie gestalten Sie die Übernahme der Serviceverantwortung, sodass zu keinem Zeitpunkt eine Überwachungslücke entsteht?
- Wie gehen Sie mit unvollständiger oder fehlender Dokumentation des Altdienstleisters um, und wie erschließen Sie sich die bestehenden Use Cases und Regelwerke?
- Wie stellen Sie den abnahmefähigen Mindestschutzzumfang nach D1 Kapitel 9.5 zum 31.05.2027 her, und wie weisen Sie dessen Wirksamkeit im Abnahmeverfahren nach?

3.2 Bereich B: Phasenmodell und Cut-over-Strategie

- Wie strukturieren Sie die Einführung in Phasen mit klaren Entscheidungspunkten und Abnahmesteps?
- Wie gestalten Sie den Parallelbetrieb und den Umschaltzeitpunkt (Cut-over), ohne dass die Schutzwirkung sinkt?
- Wie belegen Sie in Ihrem Projektplan, dass der Meilenstein M1 (Cut-over) zum 31.05.2027 erreicht wird, und welche Mitwirkungsleistungen des Auftraggebers setzen Sie dafür zu welchem Zeitpunkt voraus?

3.3 Bereich C: Migration der EDR-Plattform

- Wie planen Sie den wellenbasierten Rollout der vom Auftraggeber gewählten EDR-Plattform vom Pilot bis in die Fläche?
- Wie behandeln Sie dabei klinisch-kritische Systemklassen und vermeiden Fenster verminderten Schutzes (Schutzlücken-Fenster)?

3.4 Bereich D: Risikomanagement und Rückfallszenarien im Klinikbetrieb

- Welche Risiken sehen Sie für den klinischen Betrieb (Operationssäle, Intensivmedizin, Notaufnahme, Bildgebung), und wie steuern Sie diese konkret?
- Welche Rückfallszenarien und Rollback-Pläne halten Sie vor, und wann greifen sie?

3.5 Bereich E: Ressourcenplanung, Wissenstransfer und Übergabe in den Regelbetrieb

- Wie stellen Sie die Verfügbarkeit von Schlüsselpersonal über den gesamten Projektverlauf sicher?
- Wie gestalten Sie den Wissenstransfer und die formale Übergabe in den Regelbetrieb?
- Welche Leistungen erbringen Sie im Ramp-up-Betrieb zwischen Cut-over und Übergang in den Regelbetrieb, und wie führen Sie den Leistungsumfang in dieser Zeit an den vollen Regelbetrieb heran?

4 Themenfeld 2: Managed Service Design & Betriebsorganisation

Bezug: D1 – Leistungsbeschreibung, Kapitel 10 (Managed Service / Betriebsmodell) und Kapitel 11 (Prozess- und Ticketintegration (ServiceNow)). Bewertung: D3, Themenfeld 2.

Der Bieter legt dar, wie die Betriebsorganisation für den durchgängigen 24/7-Betrieb (24 Stunden an 7 Tagen) aufgebaut ist, wie die Anbindung an die Fachverfahrenslandschaft des Auftraggebers (insbesondere ServiceNow) erfolgt und wie der Betrieb über die gesamte Vertragslaufzeit steuerbar und krisenfest bleibt. Einzuschließen ist der Schwachstellen-Service im laufenden Betrieb gemäß D1 Kapitel 10.11.

Bitte gehen Sie im Lösungskonzept auf die folgenden Bereiche und Leitfragen ein:

4.1 Bereich A: SOC-Betriebsorganisation (24/7)

- Wie ist Ihre Betriebsorganisation des Security Operations Center (SOC) aufgebaut (Schichtmodell, Stufenstruktur der Bearbeitung)?
- Wie sichern Sie die durchgängig deutschsprachige Service-Steuerung und die kontinuierliche Besetzung der Service-Delivery-Management-Rolle über 60 Monate?
- Wie skalieren Sie bei Lastspitzen, und an welchen Standorten (Datenhaltung ausschließlich in der Europäischen Union) erbringen Sie den Betrieb?

4.2 Bereich B: ServiceNow-Integration und Event-to-Incident-Workflow

- Wie gestalten Sie die bidirektionale ServiceNow-Anbindung (E-Bonding) architektonisch, und wer verantwortet welche Seite der Schnittstelle?
- Wie qualifizieren und priorisieren Sie Ereignisse zu Vorfällen (Incidents), sodass kein unnötiges Ticketaufkommen (Ticket-Spam) entsteht?

- Wie gehen Sie mit Änderungen an Schnittstelle oder Datenschema auf Seiten des Auftraggebers um?
- Wie gehen Sie mit Inkonsistenzen im Asset- bzw. CMDB-Bestand des Auftraggebers um, und wie ist das Eskalationsmodell bis zur Rufbereitschaft des UKF ausgestaltet?

4.3 Bereich C: Change-Management, Reporting und kontinuierliche Verbesserung

- Wie verzahnen Sie Ihr Änderungsmanagement (Change-Management) mit dem Change-Advisory-Board des Auftraggebers?
- Wie ist Ihr Berichtswesen operativ und strategisch differenziert, und wie fließt es in einen kontinuierlichen Verbesserungsprozess ein?

4.4 Bereich D: Business Continuity und Krisenfähigkeit

- Wie verhalten Sie sich bei Teilausfällen, bei eigenen Sicherheitsvorfällen und bei Vorfällen in der Lieferkette (Supply-Chain)?
- Wie unterstützen Sie den Auftraggeber bei den KRITIS-Meldepflichten (§ 32 BSI-G in der Fassung des NIS-2-Umsetzungsgesetzes) und bei Krisenübungen?

4.5 Bereich E: Schwachstellen-Service im Betrieb

- Wie priorisieren Sie Schwachstellen im klinischen Kontext, und wie gehen Sie mit Systemen um, die aus medizintechnischen oder regulatorischen Gründen nicht kurzfristig gepatcht werden können?
- Wie führen Sie das Remediation-Tracking bis zur dokumentierten Schließung oder Risikoakzeptanz, und wie stellen Sie die Übergabe an die UKF-Betriebsgruppen sicher?

5 Themenfeld 3: Technisches Lösungskonzept – Erkennung, Zielarchitektur, Datenhoheit & Exit

Bezug: D1 – Leistungsbeschreibung, Kapitel 4 (Leistungsbereich SOC/SIEM), Kapitel 5 (Leistungsbereich NDR), Kapitel 3.1 und 3.2 (Datenhoheit, Lizenzhoheit) sowie Kapitel 14 (Exit Management). Bewertung: D3, Themenfeld 3. Dies ist das zentrale fachliche Differenzierungsfeld.

Der Bieter legt die technische Wirksamkeit und Zukunftsfähigkeit der Lösung dar: die Systematik der Angriffserkennung, die Zielarchitektur mit Anbindung der Bestandssysteme sowie die belastbare Einhaltung der nicht verhandelbaren Leitplanken Datenhoheit, Lizenzhoheit und Exit. Diese Leitplanken sind einzuhalten; darzustellen ist das Wie, nicht das Ob.

Bitte gehen Sie im Lösungskonzept auf die folgenden Bereiche und Leitfragen ein:

5.1 Bereich A: Detection-Engineering und SOC-Wirksamkeit

- Wie gestalten Sie den Lebenszyklus Ihrer Erkennungsregeln (Hypothese, Validierung, Produktivsetzung, Pflege, Außerbetriebnahme)?
- Wie messen und schließen Sie Abdeckungslücken (etwa gegenüber dem MITRE-ATT&CK-Rahmenwerk), und wie operationalisieren Sie Bedrohungsinformationen (Threat Intelligence) und die aktive Bedrohungssuche (Threat Hunting)?
- Wo sehen Sie sinnvolle Grenzen automatisierter Reaktion (SOAR) im Klinikumfeld?

5.2 Bereich B: Zielarchitektur und Plattform-Integration

- Wie ist Ihre Zielarchitektur mit Korrelations- und Datenflusslogik aufgebaut, und wie gewährleisten Sie Hochverfügbarkeit und Widerstandsfähigkeit (Resilienz)?
- Wie integrieren Sie herstelleroffen die Bestandssysteme des Auftraggebers (Active Directory, Entra ID/ADFS, ServiceNow, Mailsecurity, Systeme zur Angriffserkennung, Netzzugangskontrolle, Web Application Firewall, Privileged Access Management)?
- Wie bleibt die Architektur veränderungsfähig (neue Logquellen, Standorte, Rechenzentrumsumzug), ohne dass Zusatzprojekte erforderlich werden?

5.3 Bereich C: Datenhoheit, Lizenzhoheit und Exit

- Wie stellen Sie die Rohdatenhaltung beim Auftraggeber sicher (mindestens 12 Monate Aufbewahrung, davon mindestens 90 Tage im schnell verfügbaren Speicher / Hot Storage) und die Handlungsfähigkeit des Auftraggebers auch im Krisenfall?
- Wie setzen Sie das Lizenzmodell mit Lizenzen im Eigentum des Auftraggebers (Bring Your Own License, BYOL) und die ausschließliche Verarbeitung in der Europäischen Union um?
- Wie gewährleisten Sie die vollständige Übergabbarkeit an einen Folgedienstleister ohne vollständigen Neuaufbau (Neurollout)?
- Welche Unterauftragsverarbeiter setzen Sie ein, wo verarbeiten diese Daten, und wie stellen Sie deren Bindung an die Anforderungen aus D1 Kapitel 3.1 und 3.2 sicher?

6 Themenfeld 4: IoMT-Sicherheitskonzept

Bezug: D1 – Leistungsbeschreibung, Kapitel 8 (Leistungsbereich IoMT-Security). Bewertung: D3, Themenfeld 4.

Der Bieter legt dar, wie das Sicherheitskonzept für vernetzte Medizingeräte (Internet of Medical Things, IoMT) den klinischen Betrieb und die Eigenheiten der Medizintechnik sachgerecht adressiert und die nicht verhandelbaren Leitplanken einhält: passives, nicht-invasives Monitoring, menschliche Entscheidung vor Eingriffen (Human-in-the-Loop) und Anonymisierung klinischer Protokolldaten.

Bitte gehen Sie im Lösungskonzept auf die folgenden Bereiche und Leitfragen ein:

6.1 Bereich A: Architektur des passiven Monitorings

- Wie ist Ihre passive, nicht-invasive Monitoring-Architektur aufgebaut (Sensor-Topologie, Spiegelports / Netzwerk-Abgriffe (TAPs))?
- Wie stellen Sie sicher, dass keine Rückwirkung auf medizinisch-kritische Netzsegmente entsteht?

6.2 Bereich B: Asset Discovery und Risikobewertung

- Wie erkennen und klassifizieren Sie die rund 5.000 vernetzten Medizingeräte?
- Wie verarbeiten Sie gesundheitsspezifische Protokolle (DICOM, HL7, FHIR), und wie fließen die Hersteller-Sicherheitsangaben (Manufacturer Disclosure Statement for Medical Device Security, MDS²) in Risikobewertung und kompensierende Maßnahmen ein?

6.3 Bereich C: Anomalie-Erkennung und SIEM-Anbindung

- Wie erkennen Sie Anomalien im Geräteverhalten und binden Bedrohungsinformationen ein?

- Wie ist die Schnittstelle zum SIEM hinsichtlich Schweregrad-Filterung, Anreicherung und Eskalationspfaden definiert?

6.4 Bereich D: Reaktionsmodell mit Human-in-the-Loop

- Wie stellen Sie sicher, dass in IoMT-Segmenten keine automatischen Sperr- oder Quarantäne-Aktionen erfolgen und stets ein Mensch entscheidet?
- Wie ist die Schnittstelle zur Medizintechnik des Auftraggebers gestaltet (Eskalationspfade, Rollenmodell, Entscheidungsbefugnisse), und wie behandeln Sie freigabepflichtige Maßnahmen der Feinsegmentierung (Mikrosegmentierung)?

6.5 Bereich E: Datenschutz klinischer Protokolldaten

- Wie anonymisieren oder pseudonymisieren Sie klinische Protokolldaten vor einer etwaigen Cloud-Übertragung?
- Wie trennen Sie Sicherheitsmetadaten von klinischen Inhaltsdaten und stellen die Konformität mit der Datenschutz-Grundverordnung (DSGVO) sicher?

7 Hinweise zur Bewertung

Jedes Themenfeld wird gemäß Dokument D3 auf Basis des Gesamteindrucks über alle Bereiche mit genau einer von sechs Bewertungsstufen benotet (Sehr gut 15, Gut 12, Befriedigend 9, Ausreichend 6, Mangelhaft 3, Ungenügend 0 Punkte). Maximal erreichbar sind 60 Qualitätspunkte.

Bewertet wird ausschließlich die Qualität des dargestellten Vorgehens für die ausgeschriebene Leistung. Eignung, Referenzen und Umsatz werden im Teilnahmewettbewerb (Dokument D2) geprüft und fließen nicht in die Zuschlagswertung ein. Ein Verstoß gegen eine in D1 als nicht verhandelbar bezeichnete Leitplanke oder ein erkennbares Vendor-Lock-in-Risiko wirkt sich in dem betroffenen Themenfeld bewertungsmindernd bis hin zur Stufe „Ungenügend“ aus. Die Einstufung erfolgt nach Maßgabe der themenspezifischen Indikatorenkataloge unter Berücksichtigung der Schwere des Verstoßes. Eine Mindestpunktschwelle je Themenfeld ist nicht vorgesehen.

Anlage-EN 1 Eigenerklärung Nachunternehmen

Bieter	Vergabenummer	Datum
	20261023	
Projekt		
Leistung Security Managed Services		

Ergänzung des Angebotsschreibens

Verzeichnis über Art und Umfang der Leistungen, für die sich der Bieter der Kapazitäten anderer Unternehmen bedienen wird

Zur Ausführung der im Angebot enthaltenen Leistungen benenne ich Art und Umfang der Teilleistungen, für die ich mich/wir uns anderer Unternehmen bedienen werde(n).

OZ/Leistungsbereich	Beschreibung der Teilleistungen / Firma des Nachunternehmers

In Hinsicht auf meine/unsere wirtschaftliche und finanzielle Leistungsfähigkeit	
Name des Unternehmens	Angabe zu der von diesem Unternehmen überlassenen Eignung

Anlage-EN2 Verpflichtungserklärung Nachunternehmen

Bewerber/Bieter	Vergabenummer	Datum
	20261023	
Projekt		
Leistung Security Managed Services		

Name, gesetzlicher Vertreter, Kontaktdaten des sich verpflichtenden Unternehmens
--

Verpflichtungserklärung anderer Unternehmen

Ich/Wir verpflichte(n) mich/uns gegenüber dem Auftraggeber, im Falle der Auftragsvergabe an den o.g. Bewerber/Bieter diesem mit den erforderlichen Kapazitäten meines/unseres Unternehmens für den/die nachfolgenden Leistungsbereich(e) zur Verfügung zu stehen.

OZ/Leistungsbereich	Beschreibung der (Teil)Leistungen

(Ort, Datum, Unterschrift)

- ☐ Der Bewerber bzw. Bieter nimmt zum Nachweis seiner Eignung die wirtschaftliche und finanzielle Leistungsfähigkeit meines/unseres Unternehmens in Anspruch. Ich/Wir verpflichte(n) mich/uns gegenüber dem Auftraggeber, im Falle der Auftragsvergabe an den o.g. Bewerber/Bieter mit diesem gemeinsam für die Auftragsausführung zu haften.

(Ort, Datum, Unterschrift)

Anmerkung: Sofern Verpflichtungserklärungen in Kopie oder als Telefax vorgelegt werden, behält sich die Vergabestelle vor, die Originale zu verlangen.

Anlage-EBG Erklärung Bietergemeinschaft

Bezeichnung der Leistung:

Maßnahmennummer	Projekt
Vergabenummer	Leistung
20261023	Security Managed Services

Erklärung der Bieter- /Arbeitsgemeinschaft

Wir, die nachstehend aufgeführten Unternehmen einer Bietergemeinschaft,

Bevollmächtigter Vertreter

Mitglied _____

USt-ID: _____

Weitere Mitglieder

Mitglied _____

USt-ID: _____

Mitglied _____

USt-ID: _____

Mitglied _____

USt-ID: _____

beschließen, im Falle der Auftragserteilung eine Arbeitsgemeinschaft zu bilden und erklären¹, dass der bevollmächtigte Vertreter die Mitglieder gegenüber dem Auftraggeber rechtsverbindlich vertritt und alle Mitglieder als Gesamtschuldner haften.

Ort Datum Unterschrift

Ort Datum Unterschrift

Ort Datum Unterschrift

Ort Datum Unterschrift

¹ Die Bietergemeinschaft hat mit ihrem Angebot eine Erklärung aller Mitglieder in Textform abzugeben, Auf Verlangen der Vergabestelle ist eine von allen Mitgliedern unterzeichnete bzw. fortgeschritten oder qualifiziert signierte Erklärung abzugeben.

- Anlage zum BMWK-Rundschreiben vom 14.04.2022 -

Eigenerklärung

(von allen Bewerbern / Bieter / allen Mitgliedern von Bewerber- bzw. Bietergemeinschaften)

Bezeichnung des Vergabeverfahrens / Auftrags:

Geschäftszeichen des Auftraggebers:

20261023

Die nachfolgende Erklärung gebe/n ich/wir verbindlich ab (ggf. zugleich in Vertretung für die lt. Teilnahmeantrag / Angebot Vertretenen auch für diese):

1. Der / die **Bewerber / Bieter** gehört / gehören nicht zu den

in **Artikel 5 k)** Absatz 1 der Verordnung (EU) Nr. 833/2014 in der Fassung des Art. 1 Ziff. 23 der Verordnung (EU) 2022/576 des Rates vom 8. April 2022 über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren,

genannten Personen oder Unternehmen, die einen Bezug zu Russland im Sinne der Vorschrift aufweisen,

- a) **durch die russische Staatsangehörigkeit des Bewerbers/Bieters oder die Niederlassung des Bewerbers/Bieters in Russland,**
- b) **durch die Beteiligung einer natürlichen Person oder eines Unternehmens, auf die eines der Kriterien nach Buchstabe a zutrifft, am Bewerber/Bieter über das Halten von Anteilen im Umfang von mehr als 50%,**
- c) **durch das Handeln der Bewerber/Bieter im Namen oder auf Anweisung von Personen oder Unternehmen, auf die die Kriterien der Buchstaben a und/oder b zutrifft.**

2. Die am Auftrag als **Unterauftragnehmer, Lieferanten oder Unternehmen, deren Kapazitäten im Zusammenhang mit der Erbringung des Eignungsnachweises in Anspruch genommen werden**, beteiligten Unternehmen, auf die mehr als 10 % des Auftragswerts entfällt, gehören ebenfalls nicht zu dem in der Vorschrift genannten Personenkreis mit einem Bezug zu Russland im Sinne der Vorschrift.

3. Es wird bestätigt und sichergestellt, dass auch während der Vertragslaufzeit keine als **Unterauftragnehmer, Lieferanten oder Unternehmen, deren Kapazitäten im Zusammenhang mit der Erbringung des Eignungsnachweises in Anspruch genommen werden**, beteiligten Unternehmen eingesetzt werden, auf die mehr als 10 % des Auftragswerts entfällt.

_____, den _____

Unterschriften (bei elektronischer Übermittlung: Name der erklärenden Person)

Artikel 5k der Verordnung (EU) Nr. 833/2014 in der Fassung des Art. 1 Ziff. 23 der Verordnung (EU) 2022/576 des Rates vom 8. April 2022 lautet wie folgt:

(1) Es ist verboten, öffentliche Aufträge oder Konzessionen, die in den Anwendungsbereich der Richtlinien über die öffentliche Auftragsvergabe sowie unter Artikel 10 Absatz 1, Absatz 3, Absatz 6 Buchstaben a bis e, Absatz 8, Absatz 9 und Absatz 10 und die Artikel 11, 12, 13 und 14 der Richtlinie 2014/23/EU, unter die Artikel 7 und 8, Artikel 10 Buchstaben b bis f und h bis j der Richtlinie 2014/24/EU, unter Artikel 18, Artikel 21 Buchstaben b bis e und g bis i, Artikel 29 und Artikel 30 der Richtlinie 2014/25/EU und unter Artikel 13 Buchstaben a bis d, f bis h und j der Richtlinie 2009/81/EG fallen, an folgende Personen, Organisationen oder Einrichtungen zu vergeben bzw. Verträge mit solchen Personen, Organisationen oder Einrichtungen weiterhin zu erfüllen:

- a) russische Staatsangehörige oder in Russland niedergelassene natürliche oder juristische Personen, Organisationen oder Einrichtungen,*
- b) juristische Personen, Organisationen oder Einrichtungen, deren Anteile zu über 50 % unmittelbar oder mittelbar von einer der unter Buchstabe a genannten Organisationen gehalten werden, oder*
- c) natürliche oder juristische Personen, Organisationen oder Einrichtungen, die im Namen oder auf Anweisung einer der unter Buchstabe a oder b genannten Organisationen handeln,*

auch solche, auf die mehr als 10 % des Auftragswerts entfällt, Unterauftragnehmer, Lieferanten oder Unternehmen, deren Kapazitäten im Sinne der Richtlinien über die öffentliche Auftragsvergabe in Anspruch genommen werden.

(2) Abweichend von Absatz 1 können die zuständigen Behörden die Vergabe oder die Fortsetzung der Erfüllung von Verträgen genehmigen, die bestimmt sind für

- a) den Betrieb ziviler nuklearer Kapazitäten, ihre Instandhaltung, ihre Stilllegung, die Entsorgung ihrer radioaktiven Abfälle, ihre Versorgung mit und die Wiederaufbereitung von Brennelementen und die Weiterführung der Planung, des Baus und die Abnahmetests für die Indienststellung ziviler Atomanlagen und ihre Sicherheit sowie die Lieferung von Ausgangsstoffen zur Herstellung medizinischer Radioisotope und ähnlicher medizinischer Anwendungen, kritischer Technologien zur radiologischen Umweltüberwachung sowie für die zivile nukleare Zusammenarbeit, insbesondere im Bereich Forschung und Entwicklung,*
- b) die zwischenstaatliche Zusammenarbeit bei Raumfahrtprogrammen,*
- c) die Bereitstellung unbedingt notwendiger Güter oder Dienstleistungen, wenn sie ausschließlich oder nur in ausreichender Menge von den in Absatz 1 genannten Personen bereitgestellt werden können,*
- d) die Tätigkeit der diplomatischen und konsularischen Vertretungen der Union und der Mitgliedstaaten in Russland, einschließlich Delegationen, Botschaften und Missionen, oder internationaler Organisationen in Russland, die nach dem Völkerrecht Immunität genießen.*
- e) den Kauf, die Einfuhr oder die Beförderung von Erdgas und Erdöl, einschließlich raffinierter Erdölerzeugnisse, sowie von Titan, Aluminium, Kupfer, Nickel, Palladium und Eisenerz aus oder durch Russland in die Union, oder*
- f) den Kauf, die Einfuhr oder die Beförderung von Kohle und anderen festen fossilen Brennstoffen, die in Anhang XXII aufgeführt sind, bis 10. August 2022.*

(3) Der betreffende Mitgliedstaat unterrichtet die anderen Mitgliedstaaten und die Kommission über jede nach diesem Artikel erteilte Genehmigung innerhalb von zwei Wochen nach deren Erteilung.

(4) Die Verbote gemäß Absatz 1 gelten nicht für die Erfüllung — bis zum 10. Oktober 2022 — von Verträgen, die vor dem 9. April 2022 geschlossen wurden.

(Name und Anschrift des Bieters)

Vergabenummer: 20261023

Verpflichtungserklärung zu Tariftreue und Mindestentgelt bei öffentlichen Aufträgen nach dem Hessischen Vergabe- und Tariftreuegesetz (HVTG) vom 19. Dezember 2014, GVBl. S. 354

Es wird darauf hingewiesen, dass sich die Verpflichtungserklärung zu Tariftreue und Mindestentgelt entsprechend den Vorgaben der §§ 4 und 6 des Hessischen Vergabe- und Tariftreuegesetzes (HVTG) zur Zahlung des Mindestlohns gemäß § 20 des Mindestlohngesetzes (MiLoG) bzw. des Tariflohns nach dem Arbeitnehmer-Entsendegesetz (AEntG) nicht auf Beschäftigte bezieht, die bei einem Bieter oder Nachunternehmer im EU-Ausland beschäftigt sind und die Leistung im EU-Ausland erbringen.

Nachfolgende Erklärung ist zu unterschreiben und mit dem Angebot abzugeben.

Ich/Wir erkläre/n:

1. Ich/wir nehme/n zur Kenntnis, dass ich/wir gemäß § 4 Abs. 1 HVTG die für mich/uns geltenden gesetzlichen, aufgrund eines Gesetzes festgesetzten und unmittelbar geltenden tarifvertraglichen Leistungen zu gewähren habe/n. Ich/wir nehme/n weiterhin zur Kenntnis, dass bei Vorliegen von Anhaltspunkten dafür, dass gegen diese Regelung verstoßen wird, auf Anforderung dem öffentlichen Auftraggeber oder dem Besteller die Einhaltung dieser Verpflichtung nachzuweisen ist.
 2. Ich/wir verpflichte/n mich/uns, gemäß § 4 Abs. 2 HVTG meinen/unseren Beschäftigten bei der Ausführung der Leistung diejenigen Arbeitsbedingungen einschließlich des Entgelts zu gewähren, die nach Art und Höhe mindestens den Vorgaben desjenigen Tarifvertrags entsprechen, an den mein/unser Unternehmen aufgrund des AEntG gebunden ist.
 3. Ich/wir verpflichte/n mich/uns, gemäß § 4 Abs. 3 und § 6 HVTG meinen/unseren Beschäftigten bei der Ausführung der Leistung ein Entgelt zu zahlen, das den Vorgaben des MiLoG entspricht. Im Falle der Auftragsausführung durch Nachunternehmer oder Verleihunternehmen sind im Angebot, soweit diese bereits bei Angebotsabgabe bekannt sind, spätestens jedoch vor Beginn der Ausführung der Leistung durch das Nachunternehmen oder Verleihunternehmen die entsprechenden Erklärungen in Textform abzugeben und vorzulegen.
- Die Erklärung kann entfallen, soweit sie bereits in einem Präqualifizierungsregister hinterlegt ist.

- Die Einhaltung der nach Bundesrecht oder aufgrund von Bundesrecht für mich/uns geltenden Regelungen von besonders festgesetzten Mindestentgelten (Mindestlohn) als Mindeststandard im Angebot entfällt, soweit nach § 4 HVTG Tariftreue gefordert werden kann und die danach maßgebliche tarifliche Regelung für die Beschäftigten günstiger ist als die für sie nach Bundesrecht geltenden Bestimmungen.
- 4. Ich/wir erkläre/n, dass ich/wir nicht wegen eines Verstoßes gegen § 21 MiLoG (Bußgeldvorschriften) mit einer Geldbuße von wenigstens 2.500 Euro belegt worden bin/sind und damit nicht die Voraussetzungen für einen Ausschluss von der Auftragsvergabe nach § 19 Abs. 1 und 3 MiLoG vorliegen.
- 5. Ich/wir verpflichte/n mich/uns für den Fall der Ausführung vertraglich übernommener Leistungen durch Nachunternehmen, die Erfüllung der Verpflichtungen nach den §§ 4 und 6 HVTG durch die Nachunternehmen sicherzustellen und dem öffentlichen Auftraggeber Tariftreue- und sonstige Verpflichtungs- sowie Mindestlohnerklärungen der Nachunternehmen nach Auftragserteilung, spätestens vor Beginn der Ausführung der Leistung durch das Nachunternehmen, vorzulegen. Gleiches gilt, wenn ich/wir oder ein beauftragtes Nachunternehmen zur Ausführung des Auftrags Arbeitskräfte eines Verleihunternehmens einsetze(n)/einsetzt. Diese Verpflichtung gilt entsprechend auch für alle weiteren Nachunternehmen und Verleihunternehmen.

Ort/Datum, Firma des Unternehmens, Name der natürlichen Person, die unterschriftsbefugt ist



Systemvertrag

Vertrag über die Erstellung eines Gesamtsystems

Inhaltsangabe

1	Gegenstand, Vergütung und Bestandteile des Vertrages	5
1.1	Vertragsgegenstand	5
1.2	Vergütung	5
1.3	Vertragsbestandteile	6
2	Übersicht über die vereinbarten Leistungen	6
2.1	Leistungen bis zur Abnahme	6
2.2	Leistungen nach der Abnahme	7
2.3	Vorgehensmodell	7
3	Systemumgebung* des Gesamtsystems und beizustellende Systemkomponenten*	7
4	Leistungen des Auftragnehmers zur Erstellung des Gesamtsystems	7
4.1	Verkauf von Hardware	7
4.2	Vermietung von Hardware	8
4.3	Überlassung von Standardsoftware* gegen Einmalvergütung auf Dauer (Verkauf)	8
4.3.1	Leistungsumfang und Vergütung	8
4.3.2	Mitteilung über Anpassungen der Standardsoftware* auf Quellcodeebene	9
4.3.3	Abweichende Lizenzbedingungen	10
4.3.4	Bereitstellung der Standardsoftware*	10
4.4	Überlassung von Standardsoftware* auf Zeit (Vermietung)	10
4.4.1	Leistungsumfang und Vergütung	10
4.4.2	Mitteilung über Anpassungen der Standardsoftware* auf Quellcodeebene	11
4.4.3	Abweichende Lizenzbedingungen	12
4.4.4	Bereitstellung der Standardsoftware*	12
4.5	Erstellung und Überlassung von Individualsoftware* auf Dauer	12
4.5.1	Leistungsumfang	12
4.5.2	Vergütung	13
4.5.3	Abweichende Nutzungsrechte an der Individualsoftware*	13
4.5.4	Sonderregelung: Lizenzrückvergütung (nur möglich bei nicht ausschließlicher Nutzungsrechtseinräumung)	14
4.5.5	Einräumung von Rechten an Erfindungen	14
4.5.6	Bereitstellung der Individualsoftware*	14
4.6	Übernahme von Altdaten und andere Migrationsleistungen	15
4.6.1	Leistungsumfang	15
4.6.2	Vergütung	15
4.7	Erstellung des Gesamtsystems und Herbeiführung der Betriebsbereitschaft*	15
4.7.1	Leistungsumfang	15
4.7.2	Abweichende Nutzungsrechtsvereinbarungen	15
4.7.3	Vergütung	15
4.8	Schulung	15
4.8.1	Art und Umfang der Schulungen	15
4.8.2	Schulungsunterlagen	16



Systemvertrag

- 4.8.3 Vergütung für Schulungen inkl. Schulungsunterlagen17
- 4.9 Dokumentation17
- 4.10 Software Bill of Materials (SBOM)*17
- 4.11 Sonstige Leistungen zur Systemerstellung17
 - 4.11.1 Leistungsumfang17
 - 4.11.2 Vergütung17
- 5 Systemservice18
 - 5.1 Arten von Systemserviceleistungen18
 - 5.1.1 Wiederherstellung der Betriebsbereitschaft* des Gesamtsystems (Störungsbeseitigung)18
 - 5.1.2 Aufrechterhaltung der Betriebsbereitschaft* (vorbeugende Maßnahmen)19
 - 5.1.3 Überlassung von verfügbaren Programmständen* (Standardsoftware*)20
 - 5.2 Beginn / Dauer der Systemserviceleistungen20
 - 5.3 Kündigung von Systemserviceleistungen20
 - 5.4 Vergütung/Zahlungsfristen für Systemserviceleistungen20
 - 5.4.1 Vergütung20
 - 5.4.2 Zahlungsfristen für Systemserviceleistungen21
 - 5.5 Sonstige Regelungen zu Systemserviceleistungen21
 - 5.5.1 Teleservice*21
 - 5.5.2 Abnahme der Systemserviceleistungen21
 - 5.5.3 Dokumentation der Systemserviceleistungen21
- 6 Zusätzliche Regelungen für Open Source Software*21
- 7 Weitere Leistungen nach der Abnahme22
 - 7.1 Weiterentwicklung und Anpassung des Gesamtsystems nach der Abnahme22
 - 7.2 Sonstige Leistungen nach der Abnahme22
 - 7.2.1 Leistungsumfang22
 - 7.2.2 Vergütung22
- 8 Ergänzende Vereinbarungen bei Vergütung nach Aufwand23
 - 8.1 Vereinbarung der Preiskategorien bei Vergütung nach Aufwand23
 - 8.2 Zeiten der Leistungserbringung bei Vergütung nach Aufwand23
 - 8.2.1 Während der Geschäftszeiten an Werktagen (außer an Samstagen und Feiertagen am Erfüllungsort)23
 - 8.2.2 Außerhalb der Geschäftszeiten an Werktagen (außer an Samstagen und Feiertagen am Erfüllungsort)23
 - 8.2.3 Während sonstiger Zeiten23
 - 8.3 Abweichende Regelungen für die Bestimmung und Vergütung von Personentagesätzen23
 - 8.4 Reisekosten, Nebenkosten*, Materialkosten und Reisezeiten23
 - 8.4.1 Reisekosten, Nebenkosten* und Materialkosten23
 - 8.4.2 Reisezeiten24
 - 8.5 Besondere Bestimmungen zur Vergütung nach Aufwand24
 - 8.6 Preisanpassung für Systemserviceleistungen, die nicht im Pauschalpreis* enthalten sind24
- 9 Termin- und Leistungsplan24
- 10 Zahlungsplan, Rechnungen25
- 11 Projektmanagement25



Systemvertrag

- 11.1 Projektmanager/Projektleiter²⁵
- 11.2 Weitere Schlüsselpositionen des Auftragnehmers²⁶
- 11.3 Projektsteuerung/Projektkoordination²⁶
- 11.4 Behandlung von Änderungsverlangen (Change Requests)²⁶
- 12 Weitere Pflichten des Auftragnehmers²⁶
 - 12.1 Besondere Anforderungen an Mitarbeiter des Auftragnehmers²⁶
 - 12.2 Allgemeine Sicherheitsanforderungen²⁷
 - 12.3 Kopier- oder Nutzungssperre*²⁷
 - 12.4 Mitteilungspflicht bezüglich der zur Vertragserfüllung eingesetzten Werkzeuge*²⁷
 - 12.5 Entsorgung der Hardware (ergänzend zu Ziffer 2.1 EVB-IT System-AGB)²⁷
 - 12.6 Entsorgung der Verpackung²⁷
- 13 Mitwirkung des Auftraggebers²⁷
- 14 Abnahme²⁸
 - 14.1 Gegenstand der Abnahme²⁸
 - 14.2 Testdaten²⁸
 - 14.3 Dauer, Ort und Systemumgebung* der Funktionsprüfung²⁸
 - 14.4 Vereinbarungen zur Durchführung der Funktionsprüfung und zur Erklärung der Abnahme²⁸
 - 14.5 Vereinbarungen zu Mängelklassen im Rahmen der Funktionsprüfung²⁸
- 15 Mängelhaftung (Gewährleistung)²⁸
 - 15.1 Verjährungsfrist (Gewährleistungsfrist) für Mängel des Gesamtsystems²⁸
 - 15.2 Verjährungsfrist (Gewährleistungsfrist) für Mängel an Teilleistungen²⁹
 - 15.3 Mängelmeldungen²⁹
 - 15.3.1 Form der Mängelmeldung²⁹
 - 15.3.2 Adresse für Mängelmeldungen²⁹
 - 15.4 Reaktions-* und Wiederherstellungszeiten*, Servicezeiten, Hotline²⁹
 - 15.4.1 Reaktions-* und Wiederherstellungszeiten*, Mängelklassen²⁹
 - 15.4.2 Servicezeiten³⁰
 - 15.4.3 Hotline³⁰
 - 15.5 Teleservice*³⁰
 - 15.6 Weitere Vereinbarungen zur Mängelhaftung³⁰
- 16 Haftungsregelungen³⁰
 - 16.1 Haftungsobergrenze bei leicht fahrlässiger Pflichtverletzung³⁰
 - 16.2 Haftung bei Verzug³¹
 - 16.3 Haftung für den Systemservice³¹
 - 16.4 Haftung für entgangenen Gewinn³¹
- 17 Vertragsstrafen bei Verzug³¹
 - 17.1 Verzug bei Erstellung des Gesamtsystems³¹
 - 17.2 Verzug bei Reaktions-* und Wiederherstellungszeiten*³¹
- 18 Weitere Vereinbarungen³¹
 - 18.1 Garantien³¹
 - 18.1.1 Auftragnehmergarantien³¹
 - 18.1.2 Herstellergarantien³²
 - 18.2 Übergabe bzw. Hinterlegung des Quellcodes*³²



Systemvertrag

- 18.2.1 Übergabe des Quellcodes*32
- 18.2.2 Hinterlegung des Quellcodes32
- 18.3 Haftpflichtversicherung33
- 18.4 Sicherheiten33
 - 18.4.1 Vorauszahlungsbürgschaft33
 - 18.4.2 Vertragserfüllungs- oder Mängelhaftungssicherheit33
 - 18.4.3 Kombinierte Vertragserfüllungs- oder Mängelhaftungssicherheit33
- 18.5 Datenschutz, Geheimhaltung und Sicherheit34
- 18.6 Vereinbarungen zur Korruptionsprävention34
- 18.7 Kündigungsrecht des Auftraggebers34
- 18.8 Sonstige Vereinbarungen34

Systemvertrag

Vertrag über die Erstellung eines Gesamtsystems

zwischen _____

Vertragsnummer/Kennung Auftraggeber: _____

„Auftraggeber“

und _____

Vertragsnummer/Kennung Auftragnehmer: _____

„Auftragnehmer“

wird folgender Vertrag geschlossen:

1 Gegenstand, Vergütung und Bestandteile des Vertrages

1.1 Vertragsgegenstand

Gegenstand des EVB-IT Systemvertrages ist die Erstellung des nachfolgend beschriebenen Gesamtsystems, einschließlich der Herbeiführung der Betriebsbereitschaft* durch den Auftragnehmer auf der Grundlage eines Werkvertrages und - soweit nachfolgend vereinbart - der Systemservice und die Weiterentwicklung des Gesamtsystems.

Die Leistungen zur Erstellung des Gesamtsystems bilden eine sachliche, wirtschaftliche und rechtliche Einheit. Für den Auftraggeber ist von vertragswesentlicher Bedeutung, dass der Auftragnehmer die in diesem Vertrag vereinbarte Funktionalität des Gesamtsystems herstellt und alle dafür erforderlichen Schritte vornimmt. Der Auftragnehmer ist verantwortlicher Generalunternehmer für die Erstellung des Gesamtsystems und haftet für die Leistungen seiner Subunternehmer wie für seine eigenen Leistungen.

Art und Umfang der Leistungen ergeben sich aus diesem Vertrag, insbesondere aus den in Nummer 1.3 genannten Dokumenten.

1.2 Vergütung

- ☐ Der Pauschalpreis* beträgt _____. Die einzelnen Anteile am Pauschalpreis* werden nachfolgend nicht gesondert ausgewiesen.
 - ☐ Ausgenommen vom Pauschalpreis* sind einzelne Leistungen, die gesondert vergütet werden.[1]
- ☐ Der Pauschalpreis* beträgt _____. Die einzelnen Anteile am Pauschalpreis* werden nachfolgend gesondert ausgewiesen.
 - ☐ Ausgenommen vom Pauschalpreis* sind einzelne Leistungen, die gesondert vergütet werden.[1]
- ☐ Es wird kein Pauschalpreis* vereinbart. Die Vergütungen werden nachfolgend gesondert ausgewiesen.
- ☐ Einzelheiten zur Vergütung ergeben sich darüber hinaus aus der Vergütungszusammenstellung in Anlage Nr. _____.

Für alle in diesem Vertrag genannten Beträge gilt einheitlich der Euro als Währung.

Die vereinbarte Vergütung versteht sich zuzüglich der gesetzlichen Umsatzsteuer.

[1] Die gesonderte Vergütung ergibt sich z.B. für den Systemservice aus Nummer 5.4.1

Systemvertrag

1.3 Vertragsbestandteile*

Es gelten nacheinander als Vertragsbestandteile:

1.3.1 dieser Vertragstext bestehend aus den Seiten 1 bis 34 und den folgenden Anlagen:

Anlage Nr.	Bezeichnung	Datum/ Version	Anzahl Seiten

☐ Es gelten die Anlagen in folgender Rangfolge _____.

Eine Einbeziehung von Lizenzbedingungen an Standardsoftware* erfolgt ausschließlich nach Maßgabe der Nummern 4.3.3 bzw. 4.4.3 d.h. sie gelten, unabhängig davon, ob und in welcher Rangfolge diese als Anlage in der Tabelle aus Nummer. 1.3.1 aufgelistet werden, ausschließlich hinsichtlich der Nutzungsrechtsregelungen und bei Anwendbarkeit der Nummer 4.3.3.1 bzw. 4.4.3.1 in der dort vereinbarten Rangfolge der Regelungen, unabhängig davon, ob und in welcher Rangfolge diese als Anlage in obiger Tabelle aufgelistet werden, allerdings gelten für Standardsoftware* bzw. Teile von Standardsoftware* (Softwarekomponenten), die Open Source Software* sind, die vom Rechteinhaber vorgegebenen Lizenzbedingungen und die Nummer 4.3.3.2 bzw. 4.4.3.2.

Die mit * gekennzeichneten Begriffe sind am Ende der EVB-IT System-AGB definiert.

1.3.2 die Ergänzenden Vertragsbedingungen für die Erstellung eines Gesamtsystems (EVB-IT System-AGB) in der bei Bereitstellung der Vergabeunterlagen geltenden Fassung,

1.3.3 die Allgemeinen Vertragsbedingungen für die Ausführung von Leistungen (VOL/B) in der bei Bereitstellung der Vergabeunterlagen geltenden Fassung.

Die EVB-IT System-AGB stehen unter evb-it.gov.de zur Einsichtnahme bereit. Die VOL/B wurde im Bundesanzeiger AT Nr. 178a vom 23. September 2003 veröffentlicht.

Soweit Allgemeine Geschäftsbedingungen im Sinne von § 305 BGB in den hier referenzierten Dokumenten des Auftragnehmers bzw. den sonstigen vom Auftragnehmer beigefügten Anlagen zu diesem Vertrag Regelungen in den EVB-IT System-AGB widersprechen, sind sie ausgeschlossen, soweit nicht eine anderweitige Vereinbarung in den EVB-IT System-AGB zugelassen ist.

Weitere Geschäftsbedingungen sind ausgeschlossen, soweit in diesem Vertrag nichts Anderes vereinbart ist.

2 Übersicht über die vereinbarten Leistungen

2.1 Leistungen bis zur Abnahme

- ☐ Verkauf von Hardware
- ☐ Vermietung von Hardware
- ☐ Überlassung von Standardsoftware* gegen Einmalvergütung auf Dauer (Verkauf)
- ☐ Überlassung von Standardsoftware* auf Zeit (Vermietung)
- ☐ Erstellung und Überlassung von Individualsoftware* auf Dauer
- ☐ Übernahme von Altdaten und andere Migrationsleistungen
- ☒ Erstellung des Gesamtsystems und Herbeiführung der Betriebsbereitschaft* (z. B. durch Aufstellung, Installation*, Customizing* und Integration* der Systemkomponenten*)
- ☐ Schulung
- ☒ Projektmanagement
- ☐ Sonstige Leistungen: _____

Systemvertrag

2.2 Leistungen nach der Abnahme

- ☐ Systemservice (z. B. Aufrechterhaltung und/oder Wiederherstellung der Betriebsbereitschaft*)
- ☐ Weiterentwicklung und Anpassung des Gesamtsystems
- ☐ Sonstige Leistungen: _____

2.3 Vorgehensmodell

Der Auftragnehmer erbringt seine Leistungen auf der Grundlage des folgenden Vorgehensmodells:

- ☐ V-Modell XT*
 - ☐ V-Modell XT* (Version/Stand) _____.
 Die Teile des Projekthandbuchs (AN), die der Auftraggeber in Umsetzung seiner Vorgaben in der Ausschreibung mindestens gefordert hat, ergeben sich aus Anlage Nr. _____.
 Die Teile des QS-Handbuchs (AN), die der Auftraggeber in Umsetzung seiner Vorgaben in der Ausschreibung mindestens gefordert hat, ergeben sich aus Anlage Nr. _____.
 - ☐ Organisationsspezifisches V-Modell XT* gemäß Anlage Nr. _____.
 Die Teile des Projekthandbuchs (AN), die der Auftraggeber in Umsetzung seiner Vorgaben in der Ausschreibung mindestens gefordert hat, ergeben sich aus Anlage Nr. _____.
 Die Teile des QS-Handbuchs (AN), die der Auftraggeber in Umsetzung seiner Vorgaben in der Ausschreibung mindestens gefordert hat, ergeben sich aus Anlage Nr. _____.
- ☐ Sonstiges Vorgehensmodell gemäß Anlage Nr. _____.

3 Systemumgebung* des Gesamtsystems und beizustellende Systemkomponenten*

- ☐ Die Systemumgebung* des Gesamtsystems beim Auftraggeber ergibt sich aus Anlage Nr. _____.
- ☐ Die beizustellenden Systemkomponenten* ergeben sich aus der nachfolgenden Tabelle:

Lfd. Nr.	Bezeichnung der beizustellenden Systemkomponenten*	Art der beizustellenden Systemkomponenten* (HW, SW, IS, S) ¹

¹ HW = Hardware, SW = Standardsoftware*, IS = Individualsoftware*, S = Sonstige

- ☐ Die beizustellenden Systemkomponenten* ergeben sich aus Anlage Nr. _____.

4 Leistungen des Auftragnehmers zur Erstellung des Gesamtsystems

4.1 Verkauf von Hardware

Der Auftragnehmer verkauft an den Auftraggeber die nachstehend aufgeführte Hardware:

Lfd. Nr.	Produktbezeichnung und -beschreibung Produkt-Nr.	EXP ¹	Menge	Einzelpreis ²	Gesamtpreis ²

Summe _____

Fußnote	Erläuterung
1	US = Hardware unterliegt US-amerikanischen Exportkontrollvorschriften EU = Hardware unterliegt EU-Exportkontrollvorschriften DT = Hardware unterliegt deutschen Exportkontrollvorschriften S = Hardware unterliegt _____ Exportkontrollvorschriften

Systemvertrag

Fußnote	Erläuterung
2	Bei vereinbartem Pauschalpreis* lediglich im Feld „Summe“ den Anteil daran angeben. Soweit in Nummer 1.2 vorgesehen, hat der Auftragnehmer hier den Anteil der Hardware an dem Pauschalpreis* anzugeben. Dies allein, um dem Auftraggeber die Bewertung des Pauschalpreises* zu ermöglichen.

- ☐ Die Vergütung für die gesamte Hardware gemäß Nummer 4.1 ist nicht im Pauschalpreis* enthalten.
- ☐ Die Vergütung für die Hardware gemäß Nummer 4.1 lfd. Nr. _____ bis _____ ist nicht im Pauschalpreis* enthalten.

4.2 Vermietung von Hardware

Der Auftragnehmer vermietet an den Auftraggeber die nachstehend aufgeführte Hardware:

Lfd. Nr.	Produktbezeichnung und -beschreibung, Produkt-Nr.	Menge	Mindestvertragsdauer in Monaten	Abw. Mietbeginn ¹	Mietdauer in Monaten (feste Laufzeit)	Abw. Kündigungsfrist in Monaten ²	Automatische Verlängerung um Anzahl Monate ³	Einzelpreis	Gesamtpreis

Monatlicher Gesamtmietpreis _____

Fußnote	Erläuterung
1	Wenn abweichend von Ziffer 16.1 EVB-IT System-AGB
2	Wenn abweichend von Ziffer 16.1.1 EVB-IT System-AGB
3	Das Mietverhältnis verlängert sich um die vereinbarten Monate, wenn es nicht mit einer Frist von drei Monaten zum Ende der Mietdauer gekündigt wird.

- ☐ Weitere Vereinbarungen zur Kündigungsfrist abweichend von Ziffer 16.1.1 EVB-IT System-AGB gemäß Anlage Nr. _____.
- ☐ Die Vergütung für die gesamte Hardware gemäß Nummer 4.2 ist nicht im Pauschalpreis* enthalten.
- ☐ Die Vergütung für die Hardware gemäß Nummer 4.2 lfd. Nr. _____ bis _____ ist nicht im Pauschalpreis* enthalten.

4.3 Überlassung von Standardsoftware* gegen Einmalvergütung auf Dauer (Verkauf)

4.3.1 Leistungsumfang und Vergütung

Dem Auftraggeber wird vom Auftragnehmer nachstehend aufgeführte Standardsoftware* gegen Einmalvergütung auf Dauer überlassen:

Lfd. Nr.	Produktbezeichnung und -beschreibung, Produkt-Nr.	Menge	EXP ¹	Anzahl erlaubter Sicherungskopien	Zu liefernde Version ²	Abweichende Nutzungsrechte gemäß Nutzungsrechtsmatrix Anlage Nr. (Muster 4) ³	Einzelpreis ⁴	Gesamtpreis ⁴



Systemvertrag

Summe der Gesamtpreise _____

Fußnote	Erläuterung
1	US = Standardsoftware* unterliegt US-amerikanischen Exportkontrollvorschriften EU = Standardsoftware* unterliegt EU-Exportkontrollvorschriften DT = Standardsoftware* unterliegt deutschen Exportkontrollvorschriften S = Standardsoftware* unterliegt _____ Exportkontrollvorschriften
2	A = Überlassung der bei Abnahme aktuellen Version, anderenfalls Versionsnummer eintragen
3	Die hier bezeichnete Anlage ist entweder eine Nutzungsrechtsmatrix gemäß Muster 4 oder eine vom Auftraggeber selbst erstellte Rechterege lung, keinesfalls bezieht sie sich aber auf Lizenzbedingungen des Herstellers der Standardsoftware*. In der Nutzungsrechtsmatrix erhält der Auftragnehmer im Rahmen der Vorgaben des Auftraggebers die Möglichkeit, von Ziffer 2.3 EVB-IT System-AGB abweichende Nutzungsrechte an der Standardsoftware* einzuräumen. In der vom Auftraggeber selbst erstellten Rechterege lung (in der Regel die Leistungsbeschreibung) legt der Auftraggeber den Mindestumfang an Rechten fest, dem er an der Standardsoftware* erwerben will (z.B. Volumenlizenz, keine OEM-Lizenz, etc.), wenn er die Nutzungsrechtsmatrix nicht nutzt. Die Nutzungsrechtsregelungen der Lizenzbedingungen für die jeweilige Standardsoftware* gelten dann nachrangig (siehe Nummer 4.3.3). Von den Nutzungsrechtsregelungen in Bezug auf Open Source Software* darf in der Anlage nicht abgewichen werden.
4	Bei vereinbartem Pauschal festpreis* lediglich im Feld „Summe“ den Anteil daran angeben. Soweit in Nummer 1.2 vorgesehen, hat der Auftragnehmer den Anteil der Standardsoftware* an dem Pauschal festpreis* anzugeben. Dies allein, um dem Auftraggeber die Bewertung des Pauschal festpreises* zu ermöglichen.

- ☐ Die Vergütung für die gesamte Standardsoftware* gemäß Nummer 4.3.1 ist nicht im Pauschal festpreis* enthalten.
- ☐ Die Vergütung für die Standardsoftware* gemäß Nummer 4.3.1 lfd. Nr. _____ bis _____ ist nicht im Pauschal festpreis* enthalten.

4.3.2 Mitteilung über Anpassungen der Standardsoftware* auf Quellcodeebene

- ☐ Die Standardsoftware* aus Nummer 4.3.1 lfd. Nr. _____ wird im Sinne von Ziffer 2.3.3 EVB-IT System-AGB auf Quellcodeebene angepasst.
- ☐ Der Auftragnehmer erklärt, dass er die Anpassungen nicht in den Standard aufnehmen wird.
- ☐ Der Auftragnehmer erklärt, dass er
- ☐ sämtliche Anpassungen in die Standardsoftware*
 - ☐ die Anpassungen gemäß Anlage Nr. _____ in die Standardsoftware* aufnehmen wird.
 - ☐ Der Auftragnehmer erklärt, dass dies abweichend von Ziffer 2.3.3 EVB-IT System-AGB nicht mit dem auf die Erklärung der Betriebsbereitschaft* folgenden Programmstand*, sondern
 - ☐ bis zur Abnahme des Gesamtsystems*
 - ☐ bis zu dem in Anlage Nr. _____ genannten Terminerfolgen wird.
- ☐ Näheres zu den Anpassungen und deren Übernahme in den Standard ergibt sich aus Anlage Nr. _____.



Systemvertrag

4.3.3 Abweichende Lizenzbedingungen

4.3.3.1 Bezüglich der Nutzungsrechte an der jeweiligen Standardsoftware* oder Softwarekomponenten aus Nummer 4.3.1 lfd. Nr. _____ gelten folgende Regelungen in der folgenden Rangfolge:

- Nutzungsrechtsmatrizen oder sonstige Rechte Regelungen des Auftraggebers(s.a. Nummer 4.3.1, Spalte 7),
- Ziffer 2.3.1 EVB-IT System-AGB,
- die Nutzungsrechtsregelungen aus den jeweiligen Lizenzbedingungen in Anlage Nr. _____ bzw. –im Falle der Überlassung neuer Programmstände* im Rahmen des Systemservices – aus den gemäß Nummer 5.1.3 bekanntgegebenen Nutzungsrechtsregelungen neuer Programmstände. Die jeweiligen Nutzungsrechtsregelungen gelten aber nur, soweit sie den sonstigen vertraglichen Regelungen weder entgegenstehen noch diese beschränken.

Die Nutzungsrechtsregelungen in Bezug auf die Überlassung von Standardsoftware* oder Softwarekomponenten, die Open Source Software* sind, bleiben unberührt und haben stets Vorrang.

4.3.3.2 Regelungen für Open Source Software*

- ☐ Die Standardsoftware* oder Softwarekomponente gemäß Nummer 4.3.1 lfd. Nr. _____ wird dem Auftraggeber als Open Source Software* zur Verfügung gestellt.
 - ☐ Zusätzlich weist die vorgenannte Lizenz die weiteren Eigenschaften auf, die sich aus Anlage Nr. _____ ergeben.
- ☐ Die Standardsoftware* oder Softwarekomponente gemäß Nummer 4.3.1 lfd. Nr. _____ wird dem Auftraggeber unter der folgenden Lizenz zur Verfügung gestellt, die den Anforderungen an Open Source Software* entspricht: _____.
- ☐ Die Standardsoftware* bzw. Softwarekomponente gemäß Nummer 4.3.1 lfd. Nr. _____ wird dem Auftraggeber ausschließlich unter Geltung von durch openCode* freigegebenen Lizenzen zur Verfügung gestellt.
- ☐ Hinsichtlich der Standardsoftware* bzw. Softwarekomponente gemäß Nummer 4.3.1 lfd. Nr. _____, wird vereinbart, dass diese ggf. gemeinsam mit folgender Software genutzt und verbreitet wird (siehe Ziffer 2.3.1.4 EVB-IT System-AGB): _____.

4.3.4 Bereitstellung der Standardsoftware*

Der Auftragnehmer stellt dem Auftraggeber die Standardsoftware* wie folgt zur Verfügung:

- ☐ gemäß Nummer 4.3.1 lfd. Nr. _____ auf Datenträger: Typ: _____, Kennzeichnung: _____,
- ☐ gemäß Nummer 4.3.1 lfd. Nr. _____ in folgender Form: _____,
- ☐ gemäß Nummer 4.3.1 lfd. Nr. _____, wie in Anlage Nr. _____ beschrieben.
- ☐ gemäß Nummer 4.3.1 lfd. Nr. _____, bei openCode* mit allen dafür notwendigen Bestandteilen und entsprechend deren Anforderungen.

4.4 Überlassung von Standardsoftware* auf Zeit (Vermietung)

4.4.1 Leistungsumfang und Vergütung

Der Auftragnehmer vermietet an den Auftraggeber die nachstehend aufgeführte Standardsoftware*:

Lfd. Nr.	Produktbezeichnung und -beschreibung, Produkt-Nr.	Menge	EXP ¹	Anzahl erlaubter Sicherungskopien	Zu liefernde Version ²	Abweichende Nutzungsrechte (Muster 4) ³ Anlage Nr.	Mindestvertragsdauer in Monaten	Abw. Mietbe-ginn ⁴	Mietdauer in Monaten (feste Laufzeit)	Abw. Kündigungsfrist ⁵	Automatische Verlängerung um Anzahl Monate ⁶	Einzelpreis	Gesamtpreis

Monatlicher Gesamtmietpreis (Summe der Gesamtpreise) _____

Systemvertrag

Fußnote	Erläuterung
1	US = Standardsoftware* unterliegt US-amerikanischen Exportkontrollvorschriften EU = Standardsoftware* unterliegt EU-Exportkontrollvorschriften DT = Standardsoftware* unterliegt deutschen Exportkontrollvorschriften S = Standardsoftware* unterliegt _____ Exportkontrollvorschriften
2	A = Überlassung der bei Abnahme aktuellen Version, anderenfalls Versionsnummer eintragen
3	Die hier bezeichnete Anlage ist entweder eine Nutzungsrechtsmatrix gemäß Muster 4 oder eine vom Auftraggeber selbst erstellte Rechteverteilung, keinesfalls bezieht sie sich aber auf Lizenzbedingungen des Herstellers der Standardsoftware*. In der Nutzungsrechtsmatrix erhält der Auftragnehmer im Rahmen der Vorgaben des Auftraggebers die Möglichkeit, von Ziffer 2.3 EVB-IT System-AGB abweichende Nutzungsrechte an der Standardsoftware* einzuräumen. In der vom Auftraggeber selbst erstellten Rechteverteilung (in der Regel die Leistungsbeschreibung) legt der Auftraggeber den Mindestumfang an Rechten fest, dem er an der Standardsoftware* erwerben will (z.B. Volumenlizenz, keine OEM-Lizenz, etc.), wenn er die Nutzungsrechtsmatrix nicht nutzt. Die Nutzungsrechtsregelungen der Lizenzbedingungen für die jeweilige Standardsoftware* gelten dann nachrangig (siehe Nummer 4.4.3). Von den Nutzungsrechtsregelungen in Bezug auf Open Source Software* darf in der Anlage nicht abgewichen werden.
4	Wenn abweichend von Ziffer 16.1 EVB-IT System-AGB.
5	Wenn abweichend von Ziffer 16.1.1 EVB-IT System-AGB.
6	Das Mietverhältnis verlängert sich um die vereinbarten Monate, wenn es nicht mit einer Frist von drei Monaten zum Ende der Mietdauer gekündigt wird.

- ☐ Die Vergütung für die gesamte Standardsoftware* gemäß Nummer 4.4.1 ist nicht im Pauschalpreis* enthalten.
- ☐ Die Vergütung für die Standardsoftware* gemäß Nummer 4.4.1 lfd. Nr. _____ bis _____ ist nicht im Pauschalpreis* enthalten.

4.4.2 Mitteilung über Anpassungen der Standardsoftware* auf Quellcodeebene

- ☐ Die Standardsoftware* aus Nummer 4.4.1 lfd. Nr. _____ wird im Sinne von Ziffer 2.3.3 EVB-IT System-AGB auf Quellcodeebene angepasst.
- ☐ Der Auftragnehmer erklärt, dass er die Anpassungen nicht in den Standard aufnehmen wird.
- ☐ Der Auftragnehmer erklärt, dass er
- ☐ sämtliche Anpassungen in die Standardsoftware* aufnehmen wird
 - ☐ die Anpassungen gemäß Anlage Nr. _____ in die Standardsoftware* aufnehmen wird.
 - ☐ Der Auftragnehmer erklärt, dass dies abweichend von Ziffer 2.3.3 EVB-IT System-AGB nicht mit dem auf die Erklärung der Betriebsbereitschaft* folgenden Programmstand*, sondern
 - ☐ bis zur Abnahme des Gesamtsystems*
 - ☐ bis zu dem in Anlage Nr. _____ genannten Termin erfolgen wird.
- ☐ Näheres zu den Anpassungen und deren Übernahme in den Standard ergibt sich aus Anlage Nr. _____.



Systemvertrag

4.4.3 Abweichende Lizenzbedingungen

4.4.3.1 Bezüglich der Nutzungsrechte an der jeweiligen Standardsoftware* oder Softwarekomponente aus Nummer 4.4.1 lfd. Nr. _____ gelten folgende Regelungen in der folgenden Rangfolge:

- Nutzungsrechtsmatrizen oder sonstige Rechte Regelungen des Auftraggebers (s.a. Nummer 4.4.1 Spalte 7),
- Ziffer 2.3.1 EVB-IT System-AGB,
- die Nutzungsrechtsregelungen aus den jeweiligen Lizenzbedingungen in Anlage Nr. _____ bzw. –im Falle der Überlassung neuer Programmstände* im Rahmen des Systemservices – aus den gemäß Nummer 5.1.3 bekanntgegebenen Nutzungsrechtsregelungen neuer Programmstände. Die jeweiligen Nutzungsrechtsregelungen gelten aber nur, soweit sie den sonstigen vertraglichen Regelungen weder entgegenstehen noch diese beschränken.

Die Nutzungsrechtsregelungen in Bezug auf die Überlassung von Standardsoftware* oder Softwarekomponenten, die Open Source Software* sind, bleiben unberührt und haben stets Vorrang.

4.4.3.2 Regelungen für Open Source Software*

- ☐ Die Standardsoftware* oder Softwarekomponente gemäß Nummer 4.4.1 lfd. Nr. _____ wird dem Auftraggeber als Open Source Software* zur Verfügung gestellt.
 - ☐ Zusätzlich weist die vorgenannte Lizenz die weiteren Eigenschaften auf, die sich aus Anlage Nr. _____ ergeben.
- ☐ Die Standardsoftware* oder Softwarekomponente gemäß Nummer 4.4.1 lfd. Nr. _____ wird dem Auftraggeber unter der folgenden Lizenz zur Verfügung gestellt, die den Anforderungen an Open Source Software* entspricht: _____.
- ☐ Die Standardsoftware* bzw. Softwarekomponente gemäß Nummer 4.4.1 lfd. Nr. _____ wird dem Auftraggeber ausschließlich unter Geltung von openCode* freigegebenen Lizenzen zur Verfügung gestellt.

4.4.4 Bereitstellung der Standardsoftware*

Der Auftragnehmer stellt dem Auftraggeber die Standardsoftware* wie folgt zur Verfügung:

- ☐ gemäß Nummer 4.4.1 lfd. Nr. _____ auf Datenträger: Typ: _____, Kennzeichnung: _____.
- ☐ gemäß Nummer 4.4.1 lfd. Nr. _____ in folgender Form: _____.
- ☐ gemäß Nummer 4.4.1 lfd. Nr. _____ wie in Anlage
- ☐ gemäß Nummer 4.4.1 lfd. Nr. _____, bei openCode* mit allen dafür notwendigen Bestandteilen und entsprechend deren Anforderungen.

4.5 Erstellung und Überlassung von Individualsoftware* auf Dauer

4.5.1 Leistungsumfang

- ☐ Der Auftragnehmer erstellt folgende Individualsoftware*:

Lfd. Nr.	Individualsoftware*	Vergütungsanteil am Pauschalpreis* für die Erstellung von Individualsoftware*

Gesamtsumme _____

- ☐ Die Individualsoftware* enthält folgende vorbestehende Teile*:

Lfd. Nr.	Lfd. Nr. aus Tabelle Nummer 4.5.1, Spalte 1	Bezeichnung der vorbestehenden Teile*	Übergabe nur im Objektcode*



Systemvertrag

Der Auftragnehmer wird den Auftraggeber über Änderungen im Zusammenhang mit den verwendeten vorbestehenden Teilen* im Projektverlauf rechtzeitig vorher schriftlich informieren. Sollte der Auftragnehmer nach Zuschlagserteilung zusätzliche oder andere vorbestehende Teile* in die Individualsoftware* einsetzen, so bestehen für diese vorbestehenden Teile* die Rechte gemäß Ziffer 2.3.4.1 EVB-IT System-AGB, jedoch werden keinesfalls ausschließliche Nutzungsrechte eingeräumt. Die ggf. für eine Verbreitung und Unterlizenzierung sämtlicher vorbestehenden Teile* zu zahlende Vergütung erhöht sich hierdurch nicht. Setzt der Auftragnehmer hingegen keine oder nur solche vorbestehenden Teile* ein, die Open Source Software* sind, entfällt die Vergütung.

4.5.2 Vergütung

- ☐ Die gesonderte Vergütung für Erstellung der Individualsoftware* beträgt pauschal _____ Euro.
- ☐ Die Vergütung für Erstellung der Individualsoftware* erfolgt gesondert nach Aufwand gemäß Nummer 7
 - ☐ mit einer Obergrenze in Höhe von _____ Euro.
 - ☐ Dabei ist Personal der Kategorie(n) _____ einzusetzen.
- ☐ Die Erstellung der Individualsoftware* ist mit dem Pauschalpreis* abgegolten.
- ☐ Abweichend von Ziffer 8.1 EVB-IT System-AGB wird die gemäß Ziffer 2.3.4.4 EVB-IT System-AGB geschuldete Überlassung am Markt nicht erhältlicher, jedoch für die Bearbeitung der Individualsoftware* nötiger Werkzeuge* zusätzlich gemäß Anlage _____ vergütet.

Bei Verwendung vorbestehender Teile* durch den Auftragnehmer, die keine Open Source Software* sind, gilt Folgendes:

- ☐ Die Vergütung für das Recht zur Verbreitung und Unterlizenzierung der vorbestehenden Teile* insgesamt an beliebige Dritte beträgt insgesamt _____ Euro.
- ☐ Die Verbreitung und Unterlizenzierung der vorbestehenden Teile* ist mit der Vergütung für die Individualsoftware* abgegolten.

4.5.3 Abweichende Nutzungsrechte an der Individualsoftware*

4.5.3.1 Open Source Software*

Gemäß Ziffer 2.3.4.1 Absatz 1 EVB-IT System-AGB ist die Individualsoftware* inklusive aller vorbestehenden Teile **als Open Source Software*** zur Verfügung zu stellen. Zusätzlich bzw. abweichend davon gilt Folgendes: Die Bereitstellung der

- ☐ Individualsoftware* gemäß Nummer 4.5.1 lfd. Nr. _____ muss wie vorstehend beschrieben, jedoch unter **von openCode* freigegebenen Lizenzen** erfolgen.
- ☐ Individualsoftware* gemäß Nummer 4.5.1 lfd. Nr. _____ muss wie vorstehend beschrieben, jedoch unter von openCode* freigegebenen Lizenzen, **die keinen Copyleft*-Effekt** haben, erfolgen (sog. Permissiven Lizenzen, z.B. MIT- oder ApacheLizenz > Version 1.0).
- ☐ Individualsoftware* gemäß Nummer 4.5.1 lfd. Nr. _____ muss wie vorstehend beschrieben, jedoch unter von openCode* freigegebenen Lizenzen **mit Copyleft*-Effekt** zur Verfügung gestellt werden (sog. Reziproke Lizenzen, z.B. GNU GPL oder LGPL).
- ☐ Individualsoftware* gemäß Nummer 4.5.1 lfd. Nr. _____ muss wie vorstehend beschrieben, jedoch unter der/den **folgenden Lizenz(en)** zur Verfügung gestellt werden, die den Anforderungen an Open Source Software* entspricht: _____.
- ☐ Abweichend von Ziffer 2.3.4.1 Absätze 2 ff. EVB-IT System-AGB muss die Bereitstellung der Individualsoftware* gemäß Nummer 4.5.1 lfd. Nr. _____ unter **Verschaffung von ausschließlichen Nutzungsrechten** erfolgen.

Die Regelungen gemäß Ziffer 2.3.5 EVB-IT System-AGB bleiben von den vereinbarten abweichenden Nutzungsrechten unberührt.

4.5.3.2 Keine Bereitstellung als Open Source Software*

- ☐ Abweichend von Ziffer 2.3.4.1 Absatz 1 EVB-IT System-AGB wird die Individualsoftware* **nicht als Open Source Software* (sondern als sog. proprietäre Software)** zur Verfügung gestellt; es gelten daher



Systemvertrag

ausschließlich Absätze 2 ff. von Ziffer 2.3.4.1 EVB-IT System-AGB. Zudem gelten die Regelungen mit folgenden Maßgaben. Für die

- ☐ Individualsoftware* gemäß Nummer 4.5.1 lfd. Nr. _____ wird ein **ausschließliches Nutzungsrecht** gewährt.
- ☐ Individualsoftware* gemäß Nummer 4.5.1 lfd. Nr. _____ wird das **Recht zur gewerblichen Verwertung**, also insbesondere auch zur Unterlizenzierung, Vervielfältigung und Verbreitung zu gewerblichen Zwecken **an beliebige Dritte** gewährt.
- ☐ Individualsoftware* gemäß Nummer 4.5.1 lfd. Nr. _____ gelten **vorrangig** vor den Regelungen in Ziffer 2.3.4.1 Absätze 2 ff. EVB-IT System-AGB **die Regelungen zu den Nutzungsrechten aus Anlage Nr. _____**.

Sonderregelungen für vorbestehende Teile* vorgenannter Individualsoftware*

- ☐ Das Recht zur Verbreitung und Unterlizenzierung der vorbestehenden Teile* ist ausgeschlossen.
- ☐ Abweichend von Ziffer 2.3.4.1 Absätze 2 ff. EVB-IT System-AGB ist der Auftraggeber zur gewerblichen Verbreitung und Unterlizenzierung vorbestehender Teile* der Individualsoftware* in Verbindung mit der Individualsoftware* selbst an beliebige Dritte berechtigt.
- ☐ Die Verbreitung und Unterlizenzierung von vorbestehenden Teilen* der Individualsoftware* ist in Anlage Nr. _____ geregelt.

4.5.3.3 Werkzeuge*

- ☐ Abweichend von Ziffer 2.3.4.4 EVB-IT System-AGB wird dem Auftraggeber das Recht eingeräumt, statt nur eines weiteren Vervielfältigungsstücks _____ Vervielfältigungsstücke herzustellen, diese gemeinsam mit der Individualsoftware* zu verbreiten und dem Dritten daran die Rechte aus Ziffer 2.3.4.4 EVB-IT System-AGB mit Ausnahme des Verbreitungs- und Vervielfältigungsrechts einzuräumen.
- ☐ Abweichend von Ziffer 2.3.4.4 EVB-IT System-AGB werden dem Auftraggeber folgende Rechte gemäß Anlage Nr. _____ eingeräumt.

4.5.4 Sonderregelung: Lizenzrückvergütung (nur möglich bei nicht ausschließlicher Nutzungsrechtseinräumung)

- ☐ Hat der Auftraggeber sich kein ausschließliches Nutzungsrecht ausbedungen, verpflichtet sich der Auftragnehmer, an den Auftraggeber für jede Einräumung eines Nutzungsrechtes an der Individualsoftware* gemäß Nummer 4.5.1 lfd. Nr. _____ an einen Dritten eine finanzielle Gegenleistung
 - ☐ in Höhe von _____% der in Nummer 4.5.1 lfd. Nr. _____ vereinbarten Vergütung
 - ☐ in Höhe von _____% der erzielten, mindestens aber eine angemessene Lizenzgebühr (netto)
 - ☐ gem. Anlage Nr. _____ zu zahlen.Die Lizenzrückvergütung ist insgesamt begrenzt auf
 - ☐ die gemäß Nummer 4.5.1 lfd. Nr. _____ zu zahlende Vergütung, zuzüglich eines Aufschlages von _____%.
 - ☐ _____% der gemäß Nummer 4.5.1 zu zahlenden Vergütung.

4.5.5 Einräumung von Rechten an Erfindungen

- ☐ Für Erfindungen, die anlässlich der Vertragserfüllung gemacht werden, gelten abweichend von Ziffer 2.3.4.5 EVB-IT System-AGB die Regelungen in Anlage Nr. _____.

4.5.6 Bereitstellung der Individualsoftware*

Der Auftragnehmer stellt dem Auftraggeber die Individualsoftware* wie folgt zur Verfügung:

- ☐ gemäß Nummer 4.5.1 lfd. Nr. _____ auf Datenträger: Typ: _____ Kennzeichnung: _____.
- ☐ gemäß Nummer 4.5.1 lfd. Nr. _____ in folgender Form: _____.
- ☐ gemäß Nummer 4.5.1 lfd. Nr. _____ wie in Anlage Nr. _____ beschrieben.
- ☐ gemäß Nummer 4.5.1 lfd. Nr. _____, bei openCode* mit allen dafür notwendigen Bestandteilen und entsprechend deren Anforderungen.



Systemvertrag

4.6 Übernahme von Altdaten und andere Migrationsleistungen

4.6.1 Leistungsumfang

- ☐ Die Übernahme von Altdaten und andere Migrationsleistungen erfolgen gemäß Anlage Nr. ____.

4.6.2 Vergütung

- ☐ Die Übernahme von Altdaten und die anderen vereinbarten Migrationsleistungen sind mit dem Pauschalpreis abgegolten.
- ☐ Der Vergütungsanteil am Pauschalpreis* für die Übernahme von Altdaten und die anderen vereinbarten Migrationsleistungen beträgt ____ Euro.
- ☐ Die gesonderte Vergütung für die Übernahme von Altdaten und für die anderen vereinbarten Migrationsleistungen beträgt pauschal ____ Euro.
- ☐ Die Vergütung für die Übernahme von Altdaten und für die anderen vereinbarten Migrationsleistungen erfolgt gesondert nach Aufw and gemäß Nummer 8
- ☐ mit einer Obergrenze in Höhe von ____ Euro.
- ☐ Dabei ist Personal der Kategorie(n) ____ einzusetzen.

4.7 Erstellung des Gesamtsystems und Herbeiführung der Betriebsbereitschaft*

4.7.1 Leistungsumfang

Der Auftragnehmer schuldet die Herbeiführung der Betriebsbereitschaft* des Gesamtsystems (Ziffer 2.4 EVB-IT System-AGB).

- ☐ Der Auftragnehmer schuldet die Herbeiführung der Betriebsbereitschaft* wie in Anlage Nr. ____ beschrieben.

4.7.2 Abweichende Nutzungsrechtsvereinbarungen

- ☐ Abweichend von Ziffer 2.4 EVB-IT System-AGB werden gem. Anlage Nr. ____ für die dort genannten Arbeitsergebnisse die dort aufgeführten Nutzungsrechte vereinbart.
- ☐ Abweichend von Ziffer 2.4 EVB-IT System-AGB werden dem Auftraggeber auch für die vorbestehenden Materialien Bearbeitungsrechte eingeräumt.

4.7.3 Vergütung

- ☐ Die Herbeiführung der Betriebsbereitschaft* ist mit dem Pauschalpreis* abgegolten.
- ☐ Der Vergütungsanteil am Pauschalpreis* für die Herbeiführung der Betriebsbereitschaft* beträgt ____ Euro.
- ☐ Die gesonderte Vergütung für die Herbeiführung der Betriebsbereitschaft* beträgt pauschal ____ Euro.
- ☐ Die Vergütung für die Leistungen zur Herbeiführung der Betriebsbereitschaft* erfolgt gesondert nach Aufw and gemäß Nummer 8
- ☐ mit einer Obergrenze in Höhe von ____ Euro.
- ☐ Dabei ist Personal der Kategorie(n) ____ einzusetzen.

4.8 Schulung

4.8.1 Art und Umfang der Schulungen

- ☐ Es sind Schulungen gemäß nachfolgender Tabelle vereinbart:



Systemvertrag

Lfd. Nr.	Anzahl der Schulungen	Art der Schulung (NZ/AD/MP/S) ¹	Inhalt der Schulung	Schulungstage pro Schulung	Ort ²	Maximale Anzahl Teilnehmer pro Schulung	Betrag pro Schulung ³	Gesamtpreis ³

Summe der Gesamtpreise _____

Fußnote	Erläuterung
1	NZ = Nutzerschulung AD = Administratorenschulung MP = Multiplikatorenschulung S = sonstige Schulung
2	Von Ziffer 2.5 EVB-IT System-AGB abweichender Ort der Schulung
3	Sofern im Pauschalpreis* enthalten, keine Angabe notwendig

- ☐ Vorbereitung und Durchführung von Schulungen erfolgen gemäß Anlage Nr. _____.

4.8.2 Schulungsunterlagen

- ☐ Es werden folgende Schulungsunterlagen geschuldet:

Lfd. Nr.	Schulung (hier lfd. Nr. aus Nummer 4.8.1 eintragen)	Schulungsunterlage	EXP ¹	Menge

Fußnote	Erläuterung
1	US = Schulungsunterlage unterliegt US-amerikanischen Exportkontrollvorschriften EU = Schulungsunterlage unterliegt EU-Exportkontrollvorschriften DT = Schulungsunterlage unterliegt deutschen Exportkontrollvorschriften S = Schulungsunterlage unterliegt _____ Exportkontrollvorschriften

- ☐ Soweit für die Individualsoftware* Nummer 4.5.3 ausschließliche Nutzungsrechte vereinbart sind, gilt dies abweichend von Ziffer 2.5 EVB-IT System-AGB nicht für die Schulungsunterlagen gemäß Nummer 4.8.2 lfd. Nr. _____, die für den Auftraggeber individuell erstellt wurden. An diesen Schulungsunterlagen werden lediglich nicht ausschließliche Nutzungsrechte * gemäß Ziffer 2.3.4.1 EVB-IT System-AGB eingeräumt.
- ☐ Für folgende Schulungsunterlagen werden von Ziffer 2.5 EVB-IT System-AGB abweichende weitergehende Nutzungsrechte vereinbart:
- ☐ Für die Schulungsunterlagen gemäß Nummer 4.8.2 lfd. Nr. _____ wird statt des nicht ausschließlichen Nutzungsrechts ein ausschließliches Nutzungsrecht gewährt.
 - ☐ Für die Schulungsunterlagen gemäß Nummer 4.8.2 lfd. Nr. _____ wird zusätzlich das Recht zur Vervielfältigung und Verbreitung gewährt.
 - ☐ Für die Schulungsunterlagen gemäß Nummer 4.8.2 lfd. Nr. _____ wird zusätzlich das Recht zur Bearbeitung sowie Vervielfältigung und Verbreitung der Bearbeitungen gewährt.
- ☐ Nutzungsrechte an den Schulungsunterlagen ergeben sich aus Anlage Nr. _____.



Systemvertrag

4.8.3 Vergütung für Schulungen inkl. Schulungsunterlagen

- ☐ Die in Nummer 4.8.1 vereinbarte Vergütung für die Schulungen inkl. der Schulungsunterlagen ist nicht im Pauschalpreis* enthalten.
- ☐ Die Vergütung für die Schulungen inkl. der Schulungsunterlagen gemäß Nummer 4.8.1 lfd. Nr. _____ bis _____ ist nicht im Pauschalpreis* enthalten.

4.9 Dokumentation

- ☐ Ergänzend/abweichend von Ziffer 5.3 EVB-IT System-AGB ist die Dokumentation in folgender Sprache / in folgender Form zu erstellen: _____.
- ☐ Ergänzend/abweichend von Ziffer 5.3 EVB-IT System-AGB sind folgende Teile der Dokumentation: _____ bis zum _____ zu liefern.
- ☐ Abweichend von Ziffern 4.5 und 5.5 EVB-IT System-AGB sind Anpassungen und Änderungen, die aufgrund von Maßnahmen zum Systemservice oder im Rahmen der Mängelbeseitigung an den Dokumentationen erforderlich sind, **nicht** in die Dokumentation einzuarbeiten, sondern als separate Dokumente zu liefern.
- ☐ Abweichend von Ziffer 5.4 EVB-IT System-AGB ist der Auftragnehmer nicht über das gesetzliche Maß hinaus verpflichtet, die im Rahmen der Mängelhaftung gemäß Ziffer 13 EVB-IT System-AGB durchgeführten Maßnahmen zu dokumentieren.
- ☐ Abweichend von Ziffer 5.6 EVB-IT System-AGB wird an den für den Auftraggeber erstellten Dokumentationen statt des nicht ausschließlichen Nutzungsrechts ein ausschließliches Nutzungsrecht gewährt.
- ☐ Die Dokumentation ist gemäß dem in Nummer 2.3 vereinbarten Vorgehensmodell zu erstellen.
- ☐ Die Anwenderdokumentation ist zusätzlich als kontextsensitive "Online-Hilfe" im Gesamtsystem abzulegen.
- ☐ Weitere Vereinbarungen zur Dokumentation gemäß Anlage Nr. _____.

4.10 Software Bill of Materials (SBOM)*

- ☐ Der Auftragnehmer stellt dem Auftraggeber eine Software Bill of Materials (SBOM)* gemäß BSI TR-03183-2 für die nach diesem Vertrag überlassene bzw. erstellte Software*
 - ☐ im Format SPDX
 - ☐ im Format CycloneDX

zur Verfügung.

Soweit Systemserviceleistungen zur Wiederherstellung und/oder zur Aufrechterhaltung der Betriebsbereitschaft* des Gesamtsystems oder von Systemkomponenten* vereinbart ist, aktualisiert der Auftragnehmer die von ihm bereitgestellte Software Bill of Materials (SBOM)* für alle neuen Programmstände*, die er dem Auftraggeber nach diesem Vertrag zur Verfügung stellen muss, sofern sich aus den neuen Programmständen* Änderungen an der Software Bill of Materials (SBOM)* ergeben.

4.11 Sonstige Leistungen zur Systemerstellung

4.11.1 Leistungsumfang

- ☐ Der Umfang der sonstigen Leistungen zur Systemerstellung ergibt sich aus Anlage Nr. _____.

4.11.2 Vergütung

- ☐ Sonstige Leistungen sind mit dem Pauschalpreis* abgegolten.
 - ☐ Der Vergütungsanteil am Pauschalpreis* für die sonstigen Leistungen beträgt _____ Euro.
- ☐ Die gesonderte Vergütung für sonstige Leistungen beträgt pauschal _____ Euro.
- ☐ Die Vergütung erfolgt gesondert nach Aufwand gemäß Abschnitt 7
 - ☐ mit einer Obergrenze in Höhe von _____ Euro.
 - ☐ Dabei ist Personal der Kategorie(n) _____ einzusetzen.



Systemvertrag

5 Systemservice

Der Auftragnehmer verpflichtet sich im Rahmen des Systemservices zur Wiederherstellung und/oder zur Aufrechterhaltung der Betriebsbereitschaft* des Gesamtsystems und/oder zur Lieferung neuer Programmstände* nach folgenden Regelungen:

5.1 Arten von Systemserviceleistungen

5.1.1 Wiederherstellung der Betriebsbereitschaft* des Gesamtsystems (Störungsbeseitigung)

Der Auftragnehmer verpflichtet sich bei Störungen die Betriebsbereitschaft*

- ☐ des Gesamtsystems gemäß Ziffer 4.1 EVB-IT System-AGB wiederherzustellen.
- ☐ des Gesamtsystems gemäß Ziffer 4.1 EVB-IT System-AGB mit Ausnahme folgender gelieferter, erstellter oder beizustellender Systemkomponenten* aus Nummer _____ lfd. Nr. _____ wiederherzustellen.
- ☐ folgender Systemkomponenten* aus Nummer _____ lfd. Nr. _____ gemäß Ziffer 4.1 EVB-IT System-AGB wiederherzustellen.
- ☐ gemäß Anlage Nr. _____ wiederherzustellen.

5.1.1.1 Störungsmeldung

5.1.1.1.1 Form der Störungsmeldung

- ☐ Die Störungsmeldung erfolgt abweichend von Ziffer 11.3 EVB-IT System-AGB in der Regel gemäß Anlage Nr. _____.

5.1.1.1.2 Adresse für Störungsmeldungen

Die Störungsmeldung erfolgt

- ☐ an folgende Adresse:

Art des Kontakts	Kontaktdaten
Name/Firma:	
Organisationseinheit/Abteilung:	
☐ Postanschrift:	
☐ Telefon:	
☐ Fax:	
☐ E-Mail:	
☐ Web-Adresse:	

- ☐ gemäß Anlage Nr. _____.

5.1.1.2 Reaktions-* und Wiederherstellungszeiten*, Mängelklassen

- ☐ Es werden folgende Reaktions-* und Wiederherstellungszeiten* (Ziffer 4.1.2 EVB-IT System-AGB) vereinbart:



Systemvertrag

Mängelklasse	Reaktionszeit* in Stunden	Wiederherstellungszeit* in Stunden
Betriebsverhindernder Mangel		
Betriebsbehindernder Mangel		
Leichter Mangel		

- ☐ Die Reaktions-* und Wiederherstellungszeiten* werden in Anlage Nr. _____ für die dort abweichend von Ziffer 3 EVB-IT System-AGB definierten Mängelklassen festgelegt.
- ☐ Weitere Vereinbarungen (z.B. Reaktionszeiten*, Wiederherstellungszeiten*, Service Level Agreement) gemäß Anlage Nr. _____.

Reaktions-* und Wiederherstellungszeiten* beginnen ausschließlich mit dem Zugang der Störungsmeldung während der vereinbarten Servicezeiten und laufen ausschließlich während der vereinbarten Servicezeiten. Ergänzend können in Nummer 17.2 für die Nichteinhaltung der o.g. Zeiten Vertragsstrafen vereinbart werden.

5.1.1.3 Servicezeiten

- ☐ Es werden folgende Servicezeiten vereinbart:

Tag	Uhrzeit
_____ bis _____	von _____ bis _____ Uhr
An Sonntagen	von _____ bis _____ Uhr
An Feiertagen am Erfüllungsort	von _____ bis _____ Uhr

5.1.1.4 Hotline

- ☐ Der Auftragnehmer gewährt eine telefonische deutschsprachige Unterstützung (Hotline) zu folgenden Zeiten:

Tag	Uhrzeit
_____ bis _____	von _____ bis _____ Uhr
An Sonntagen	von _____ bis _____ Uhr
An Feiertagen am Erfüllungsort	von _____ bis _____ Uhr

- ☐ Weitere Vereinbarungen zur Hotline (z.B. Kreis der Berechtigten, Leistungsumfang) gemäß Anlage Nr. _____.

5.1.2 Aufrechterhaltung der Betriebsbereitschaft* (vorbeugende Maßnahmen)

Der Auftragnehmer verpflichtet sich

- ☐ angemessene Maßnahmen mit dem Ziel zu ergreifen, das Auftreten zukünftiger Störungen
- ☐ des Gesamtsystems
 - ☐ des Gesamtsystems mit Ausnahme folgender gelieferter, erstellter oder beizustellenden Systemkomponenten* aus Nummer _____ lfd. Nr. _____
 - ☐ folgender Systemkomponenten* aus Nummer _____ lfd. Nr. _____

EVB-IT

Systemvertrag

zu vermeiden.

- ☐ zu vorbeugenden Maßnahmen gemäß Anlage Nr. ____.

5.1.3 Überlassung von verfügbaren Programmständen* (Standardsoftware*)

- ☐ Der Auftragnehmer verpflichtet sich, folgende Programmstände* für die aufgeführte Standardsoftware* zu überlassen, sobald sie am Markt verfügbar sind:

Lfd. Nr. aus Nummer 4.3.1	Lfd. Nr. aus Nummer 4.4.1	Patches*, Updates*	Upgrades*	Releases/ Versionen*	Leistung auf Anforderung des Auftraggebers	Leistung unverzüglich, sobald verfügbar

- ☐ Besondere Vereinbarung zur Herbeiführung der Betriebsbereitschaft* durch den Auftragnehmer gemäß Anlage Nr. ____.
- ☐ Besondere Vereinbarung zu Installation* und Customizing* der Programmstände* gemäß Anlage Nr. ____.

Soweit bezüglich der Nutzungsrechte der Standardsoftware* Nutzungsrechtsregelungen aus den Lizenzbedingungen in Nummer 4.3.3 bzw. 4.4.3 einbezogen sind, werden diese bei Überlassung neuer Programmstände* der jeweiligen Standardsoftware* durch die für den neuen Programmstand* geltenden Nutzungsrechtsregelungen ersetzt, wobei die in Nummer 4.3.3 bzw. 4.4.3 getroffenen Vereinbarungen auch für diese gelten. Diese neuen Nutzungsrechtsregelungen gelten aber nur unter den Voraussetzungen von Ziffer 4.2.2.2 EVB-IT System-AGB und nur, soweit die neuen Lizenzbedingungen dem Auftraggeber bei Überlassung mit Hinweis auf diese Regelung schriftlich bekannt gegeben werden.

5.2 Beginn / Dauer der Systemserviceleistungen

Der Auftragnehmer verpflichtet sich, die vereinbarten Systemserviceleistungen beginnend mit

- ☐ dem Tag nach Ablauf der Verjährungsfrist für Sachmängelansprüche (Gewährleistungsfrist) des Gesamtsystems
- ☐ dem Tag nach der Abnahme des Gesamtsystems
- ☐ folgendem Datum ____

jeweils

- ☐ für die Dauer von ____ Monaten
- ☐ für die Dauer von mindestens ____ Monaten (Mindestvertragsdauer)
- ☐ für die in Anlage Nr. ____ vereinbarte Dauer

zu erbringen.

5.3 Kündigung von Systemserviceleistungen

- ☐ Abweichend von Ziffer 16.1.1 EVB-IT System-AGB beträgt die Kündigungsfrist ____ Monat(e) zum Ablauf eines ____ (z.B. Kalendermonat/Kalendervierteljahr/Kalenderjahr).
- ☐ Ergänzend zu Ziffer 16.1.1 EVB-IT System-AGB wird bei vereinbarter fester Laufzeit ein Sonderkündigungsrecht des Auftraggebers gem. Anlage Nr. ____ vereinbart.

5.4 Vergütung/Zahlungsfristen für Systemserviceleistungen

5.4.1 Vergütung

- ☐ Der Systemservice ist (bei fester Laufzeit) insgesamt mit dem Pauschalfestpreis* abgegolten. Der Vergütungsanteil für den Systemservice am Pauschalfestpreis* beträgt ____ Euro[1].
- ☐ Die gesonderte Vergütung für den Systemservice insgesamt (bei fester Laufzeit) beträgt pauschal ____ Euro.



Systemvertrag

- ☐ Die gesonderte monatliche Vergütung für den Systemservice beträgt pauschal ____ Euro.
 - ☐ Für den Zeitraum bis zum Ablauf der Verjährungsfrist der Sachmängelansprüche für das Gesamtsystem wird eine abweichende monatliche Vergütung in Höhe von pauschal ____ Euro vereinbart.
- ☐ Die Vergütung für die Systemserviceleistungen gemäß Nummer(n) ____ (hier die relevanten Nummer(n) aus Nummer 5.1 eintragen) erfolgt gesondert nach Aufw and gemäß Nummer 8
 - ☐ mit einer Obergrenze in Höhe von ____ Euro monatlich.
 - ☐ Dabei ist Personal der Kategorie(n) ____ einzusetzen.
- ☐ Die Vergütung erfolgt gemäß Anlage Nr. ____.

[1] Der Auftragnehmer hat den Anteil des Systemservices an dem Pauschalpreis* anzugeben, selbst wenn in Nummer 1.2 keine gesonderte Ausweisung von Preisanteilen vorgesehen ist. Dies allein, um die Berechnung der Haftungsobergrenze gemäß Ziffer 15.2 EVB-IT System-AGB und - bei Vereinbarung einer gesonderten Ausweisung - eine Bewertung des Pauschalpreises* zu ermöglichen.

5.4.2 Zahlungsfristen für Systemserviceleistungen

- ☐ monatlich (zahlbar bis zum 15. eines jeden Monats)
- ☐ quartalsweise (zahlbar bis zum 15. des zweiten Quartalsmonats)
- ☐ jährlich (zahlbar bis zum ____)
- ☐ einmalig zum ____
- ☐ gemäß Anlage Nr. ____

5.5 Sonstige Regelungen zu Systemserviceleistungen

5.5.1 Teleservice*

- ☐ Der Auftragnehmer erbringt Teile der Leistung mittels Teleservice* entsprechend der Teleservicevereinbarung gemäß Anlage Nr. ____.

5.5.2 Abnahme der Systemserviceleistungen

- ☐ Abweichend von Ziffer 4.3 EVB-IT System-AGB vereinbaren die Parteien eine Abnahme bestimmter Systemserviceleistungen gemäß Anlage Nr. ____.

5.5.3 Dokumentation der Systemserviceleistungen

- ☐ Abweichend von Ziffer 4.5 Satz 1 EVB-IT System-AGB ist der Auftragnehmer in dem in Anlage Nr. ____ aufgeführten Umfang verpflichtet, die im Rahmen des Systemservices durchgeführten Maßnahmen zu dokumentieren.

6 Zusätzliche Regelungen für Open Source Software*

- ☐ Der Auftragnehmer ist verpflichtet, hinsichtlich der pflegegegenständlichen Software* eine Lizenzbestandsaufnahme durchzuführen, deren Ergebnis eine vollständige Software Bill of Materials (SBOM*) ist. Die Lizenzbestandsaufnahme ist unverzüglich nach Vertragsschluss durchzuführen.
 - ☐ Die Lizenzbestandsaufnahme ist spätestens binnen ____ Kalendertagen abzuschließen.
 - ☐ Die Vergütung für die Lizenzbestandsaufnahme erfolgt nach Aufw and gemäß Kategorie(n) ____ aus Nummer 8.
 - ☐ mit einer Obergrenze in Höhe von ____ Euro.
 - ☐ Die Vergütung für die Lizenzbestandsaufnahme erfolgt zu einem gesonderten Pauschalpreis in Höhe von ____ Euro.
- Die SBOM* ist gemäß Ziffer 5.7 der EVB-IT System-AGB zu pflegen.
- ☐ Neue Programmstände* von Standardsoftware* bzw. Softwarekomponenten müssen stets



Systemvertrag

- ☐ Open Source Software* sein,
- ☐ Open Source Software* sein, für die ausschließlich von openCode* freigegebenen Lizenzen gelten, soweit die Parteien nicht im Einzelfall ausdrücklich etwas anderes vereinbaren.
- ☐ Ist die Störungsbeseitigung oder die Überlassung neuer Programmstände* vereinbart, so setzt der Auftragnehmer den Auftraggeber über das Erscheinen neuer Programmstände* in Kenntnis und berät ihn dazu, wann ein neuer Programmstand* übernommen werden sollte.
- ☐ Der Auftragnehmer überlässt dem Auftraggeber neue Programmstände* von Open Source Software* nur nachdem er diese in einer von ihm bereitgehaltenen, geeigneten Testumgebung auf Funktionalität und Eignung für die Zwecke des Auftraggebers erfolgreich getestet hat.
 - ☐ Abweichend von Satz 1 stellt der Auftraggeber eine hierfür geeignete Umgebung zur Verfügung
- ☐ Der Auftragnehmer stellt die Ergebnisse der Systemserviceleistungen zusätzlich zur Überlassung an den Auftraggeber auf derjenigen öffentlichen Plattform für Softwareentwicklungsprojekte zur Verfügung, auf der die gepflegte Software* hauptsächlich entwickelt und verwaltet wird. Die Zurverfügungstellung der Ergebnisse der Systemserviceleistungen umfasst jeweils, soweit dort vorhanden, auch den ausführbaren Code, die Pflege der Dokumentation, der Software Bill of Materials (SBOM)* und eines Verzeichnisses verwendeter Softwarekomponenten.

Zusätzlich erfolgt die Bereitstellung durch den Auftragnehmer wie folgt:

 - ☐ auf der folgenden öffentlichen Plattform für Softwareentwicklungsprojekte: _____
 - ☐ auf openCode*.

7 Weitere Leistungen nach der Abnahme

7.1 Weiterentwicklung und Anpassung des Gesamtsystems nach der Abnahme

- ☐ Der Auftragnehmer verpflichtet sich, das Gesamtsystem jeweils nach den Vereinbarungen in Anlage Nr. _____ weiterzuentwickeln, zu optimieren und an die sich ändernden Bedürfnisse des Auftraggebers anzupassen. Soweit in der Anlage nichts anderes geregelt ist, erfolgt die Beauftragung entsprechend den Konditionen dieses Vertrages und der einbezogenen EVB-IT System-AGB.

7.2 Sonstige Leistungen nach der Abnahme

7.2.1 Leistungsumfang

- ☐ Der Umfang der sonstigen Leistungen nach der Abnahme ergibt sich aus Anlage Nr. _____.

7.2.2 Vergütung

- ☐ Die sonstigen Leistungen nach der Abnahme sind mit dem Pauschalfestpreis* abgegolten.
 - ☐ Der Vergütungsanteil am Pauschalfestpreis* für sonstige Leistungen nach der Abnahme beträgt _____ Euro.
- ☐ Die sonstigen Leistungen nach der Abnahme sind mit der pauschalen Vergütung für Systemserviceleistungen gemäß Nummer 5.4.1 abgegolten.
- ☐ Die gesonderte Vergütung für sonstige Leistungen nach der Abnahme beträgt pauschal _____ Euro.
- ☐ Die Vergütung erfolgt gesondert nach Aufwand gemäß Nummer 8
 - ☐ mit einer Obergrenze in Höhe von _____ Euro.
 - ☐ Dabei ist Personal der Kategorie(n) _____ einzusetzen.

Systemvertrag

8 Ergänzende Vereinbarungen bei Vergütung nach Aufwand

8.1 Vereinbarung der Preiskategorien bei Vergütung nach Aufwand

Lfd. Nr.	Bezeichnung der Personalkategorie	Preis innerhalb der Zeiten gemäß Nummer 8.2.1 je Stunde	Preis innerhalb der Zeiten gemäß Nummer 8.2.1 je Tag	Preis innerhalb der Zeiten gemäß Nummer 8.2.2 je Stunde	Preis innerhalb der Zeiten gemäß Nummer 8.2.2 je Tag	Preis innerhalb der Zeiten gemäß Nummer 8.2.3 je Stunde	Preis innerhalb der Zeiten gemäß Nummer 8.2.3 je Tag
Kategorie							

8.2 Zeiten der Leistungserbringung bei Vergütung nach Aufwand

Die Leistungen des Auftragnehmers werden erbracht:

8.2.1 Während der Geschäftszeiten an Werktagen (außer an Samstagen und Feiertagen am Erfüllungsort)

Wochentag	Uhrzeit
_____ bis _____	von _____ bis _____ Uhr

8.2.2 Außerhalb der Geschäftszeiten an Werktagen (außer an Samstagen und Feiertagen am Erfüllungsort)

Wochentag	Uhrzeit
_____ bis _____	von _____ bis _____ Uhr

8.2.3 Während sonstiger Zeiten

Wochentag	Uhrzeit
Samstag	von _____ bis _____ Uhr
Sonntag	von _____ bis _____ Uhr
Feiertag am Erfüllungsort	von _____ bis _____ Uhr

☐ Weitere Vereinbarungen gemäß Anlage Nr. _____.

8.3 Abweichende Regelungen für die Bestimmung und Vergütung von Personentagesätzen

- ☐ Abweichend von Ziffer 8.5 Satz 1 EVB-IT System-AGB können bei entsprechendem Nachweis für einen Personentag bis zu 10 Stunden abgerechnet werden.
- ☐ Abweichend von Ziffer 8.5 Satz 2 und Satz 3 EVB-IT System-AGB wird Folgendes vereinbart:
Ein voller Tagessatz kann nur in Rechnung gestellt werden, wenn mindestens 10 Zeitstunden geleistet wurden. Werden weniger als 10 Zeitstunden pro Tag geleistet, sind diese anteilig in Rechnung zu stellen.
- ☐ Weitere Vereinbarungen gemäß Anlage Nr. _____.

8.4 Reisekosten, Nebenkosten*, Materialkosten und Reisezeiten

8.4.1 Reisekosten, Nebenkosten* und Materialkosten

- ☐ Reisekosten werden nicht gesondert vergütet.
- ☐ Reisekosten werden vergütet gemäß Anlage Nr. _____.

EVB-IT

Systemvertrag

- ☐ Nebenkosten* werden nicht gesondert vergütet.
- ☐ Nebenkosten* werden vergütet gemäß Anlage Nr. ____.

- ☐ Materialkosten werden nicht gesondert vergütet.
- ☐ Materialkosten werden vergütet gemäß Anlage Nr. ____.

8.4.2 Reisezeiten

- ☐ Reisezeiten werden nicht gesondert vergütet.
- ☐ Reisezeiten werden zu 50 % als Arbeitszeiten vergütet.
- ☐ Reisezeiten werden vergütet gemäß Anlage Nr. ____.

8.5 Besondere Bestimmungen zur Vergütung nach Aufwand

- ☐ Besondere Bestimmungen zur Vergütung nach Aufwand sind in Anlage Nr. ____ vereinbart.

8.6 Preisanpassung für Systemserviceleistungen, die nicht im Pauschalpreis* enthalten sind

- ☐ Gemäß Ziffer 8.6 EVB-IT System-AGB wird eine Preisanpassung vereinbart für Systemserviceleistungen gemäß Nummer(n) ____ (hier entsprechende Nummer(n) eintragen: 5.1.1, 5.1.2 oder/und 5.1.3).
- ☐ Abweichend von Ziffer 8.6 EVB-IT System-AGB wird eine Preisanpassung für Systemserviceleistungen nach Maßgabe der Anlage Nr. ____ vereinbart.

9 Termin- und Leistungsplan

- ☐ Der Termin- und Leistungsplan ergibt sich aus folgender Tabelle:

Lfd. Nr.	Bezeichnung der zu erbringenden Leistung	Art des Termins MS ¹ , BB ² , BBTA ³ , TA ⁴ , VE ⁵	Leistungszeit (Datum oder Zeitpunkt nach Zuschlagserteilung)	Leistungsort (einschließlich Anschrift)	Bemerkungen

Fußnote	Erläuterung
1	MS = Meilenstein
2	BB = Termin der Betriebsbereitschaftserklärung
3	BBTA = Termin der Betriebsbereitschaftserklärung zur Teilabnahme
4	TA = Teilabnahmetermin
5	VE = Vertragserfüllungstermin*

- ☐ Gemäß dem in Nummer 2.3 vereinbarten Vorgehensmodell V-Modell XT* bzw. dem vereinbarten organisationsspezifischen V-Modell XT* ergibt sich der Termin- und Leistungsplan aus dem Lastenheft gemäß Anlage Nr. ____ und den Teilen des Projekthandbuchs (AN), die der Auftraggeber in Umsetzung seiner Vorgaben in der Ausschreibung mindestens gefordert hat gemäß Anlage Nr. ____.
- ☐ Der Termin- und Leistungsplan ergibt sich aus Anlage Nr. ____.

EVB-IT

Systemvertrag

10 Zahlungsplan, Rechnungen

- ☐ Der Auftraggeber leistet zum _____ (Datum) eine Vorauszahlung in Höhe von _____ Euro Zug um Zug gegen Übergabe einer Vorauszahlungsbürgschaft in gleicher Höhe gemäß Ziffer 20.1.1 EVB-IT System-AGB.
- ☐ Der Zahlungsplan ergibt sich aus folgender Tabelle:

Termin gemäß Nummer 9, lfd. Nr.	Art der Zahlung AZ ¹ , TZ ² , SZ ³	Betrag	Bemerkungen

Fußnote	Erläuterung
1	AZ = Abschlagszahlung*
2	TZ = Teilzahlung. Diese setzt eine erfolgreiche Teilabnahme voraus, gilt anderenfalls als AZ.
3	SZ = Schlusszahlung

- ☐ Der Zahlungsplan ergibt sich aus Anlage Nr. _____.
- ☐ Rechnungen sind nach den Vorgaben der folgenden E-Rechnungsverordnung elektronisch einzureichen
- ☐ E-Rechnungsverordnung des Bundes - ERechV
- ☐ _____ [z.B. E-Rechnungsverordnung des jeweiligen Landes]
- Dabei ist folgende Leitweg-ID _____ zu verwenden. Zudem müssen alle Pflichtfelder sowie die Zusatzfelder _____ gefüllt sein. Weitere Details ergeben sich aus Anlage Nr. _____.
- Eine Rechnung, die entgegen vorstehender Regelung nicht elektronisch gestellt wird, begründet keinen Verzug nach § 286 Abs. 3 BGB.
- ☐ Für die Rechnungsstellung gilt abweichend davon die folgende Regelung: _____

11 Projektmanagement

11.1 Projektmanager/Projektleiter

des Auftragnehmers (Schlüsselpositionen):

Art des Kontakts	Gesamtprojektverantwortlicher Projektmanager für die Erstellung des Gesamtsystems	Gesamtprojektverantwortlicher Projektleiter als Ansprechpartner
Name:		
Position:		
Organisationseinheit/Abteilung:		
Telefon:		
Fax:		
E-Mail:		
Postanschrift:		

Systemvertrag

des Auftraggebers:

Art des Kontakts	Projektmanager	Projektleiter als Ansprechpartner
Name:		
Position:		
Organisationseinheit/Abteilung:		
Telefon:		
Fax:		
E-Mail:		
Postanschrift:		

11.2 Weitere Schlüsselpositionen des Auftragnehmers

Die Parteien definieren gemäß Ziffer 7.4 EVB-IT System-AGB folgende weitere Schlüsselpositionen auf Seiten des Auftragnehmers und deren Besetzung:

Lfd. Nr.	Schlüsselposition	Name	Kontaktdaten

11.3 Projektsteuerung/Projektkoordinierung

Die Regeln zur Projektsteuerung und Projektkoordinierung ergeben sich aus

- ☐ dem vereinbarten Vorgehensmodell gemäß Nummer 2.3.
- ☐ folgenden Vereinbarungen gemäß Anlage Nr. _____.

11.4 Behandlung von Änderungsverlangen (Change Requests)

Ergänzend/abweichend zu Ziffer 17 EVB-IT System-AGB sind die Vereinbarungen über die Behandlung von Änderungsverlangen (Change Requests), die während der Vertragsdauer vom Auftraggeber vorgebracht werden, festgelegt:

- ☐ in dem vereinbarten Vorgehensmodell gemäß Nummer 2.3.
- ☐ in Anlage Nr. _____.

12 Weitere Pflichten des Auftragnehmers

Der Auftragnehmer hat folgende weitere Pflichten:

12.1 Besondere Anforderungen an Mitarbeiter des Auftragnehmers

- ☐ Mindestanforderungen an das einzusetzende Personal des Auftragnehmers:

Lfd. Nr.	Position	Fachliche Qualifikation	Sicherheitsüberprüfung SÜ 1, 2 oder 3 ¹	Sonstige Anforderungen, z.B. weitere Sicherheitsanforderungen

¹ Stufen der Sicherheitsüberprüfung gemäß Sicherheitsüberprüfungsgesetz

- ☐ Mindestanforderungen an das einzusetzende Personal des Auftragnehmers ergeben sich aus Anlage Nr. _____.



Systemvertrag

12.2 Allgemeine Sicherheitsanforderungen

Der Auftragnehmer verpflichtet sich, für die Laufzeit des Vertrages:

- ☐ bei der Erbringung der vertraglichen Leistungen die Regelungen zur IT-Sicherheit gemäß Anlage Nr. _____ zu beachten;
- ☐ sich der Geheimschutzbetreuung gemäß Anlage Nr. _____ zu unterstellen;
- ☐ die Regelungen des Auftraggebers zur Sicherheit am Einsatzort gemäß Anlage Nr. _____ zu beachten;
- ☐ folgende weitere Regelungen einzuhalten: _____.

12.3 Kopier- oder Nutzungssperre*

- ☐ Die vom Auftragnehmer gelieferten oder erstellten Systemkomponenten* weisen keine Kopier- oder Nutzungssperren* auf.
- ☐ Die vom Auftragnehmer gelieferten oder erstellten Systemkomponenten* weisen folgende Kopier- oder Nutzungssperren* auf: _____. Näheres siehe Anlage Nr. _____.

12.4 Mitteilungspflicht bezüglich der zur Vertragserfüllung eingesetzten Werkzeuge*

- ☐ Der Auftragnehmer teilt dem Auftraggeber mit, dass er folgende Werkzeuge* für die Erstellung der Individualsoftware*, die für die Bearbeitung und Umgestaltung der Individualsoftware* notwendig sind,
 - ☐ verwenden wird: _____. Näheres siehe Anlage Nr. _____.
 - ☐ entwickeln wird: _____. Näheres siehe Anlage Nr. _____.
- ☐ In Ergänzung zu Ziffer 6.4 der EVB-IT System-AGB erstreckt sich die Mitteilungspflicht des Auftragnehmers auch auf die für die Erstellung des Gesamtsystems insgesamt eingesetzten Werkzeuge*.

12.5 Entsorgung der Hardware (ergänzend zu Ziffer 2.1 EVB-IT System-AGB)

- ☐ Ergänzend zu Ziffer 2.1 EVB-IT System-AGB und den entsprechenden gesetzlichen Regelungen gelten die in Anlage Nr. _____ aufgeführten zusätzlichen Vereinbarungen über die Entsorgung von in der Nummer 4.1 genannter Hardware.
- ☐ Der Auftragnehmer übernimmt die Entsorgung auch von nicht in Nummer 4.1 genannter Hardware (Altgeräte) aufgrund gesonderter Vereinbarung gemäß Anlage Nr. _____.

12.6 Entsorgung der Verpackung

- ☐ Ergänzende Vereinbarung zur Entsorgung der Verpackung durch den Auftragnehmer gemäß Anlage Nr. _____.
- ☐ Die Entsorgung der Verpackung erfolgt durch den Auftraggeber (abweichend von Ziffern 2.1 und 2.2 EVB-IT System-AGB).

13 Mitwirkung des Auftraggebers

- ☐ Dem Auftraggeber obliegt folgende Mitwirkung (z.B. Infrastruktur, Organisation, Personal, Technik, Dokumente):

Lfd. Nr.	Art der Mitwirkung	Erläuterungen (z.B. fachliche Qualifikation des Personals, das Mitwirkungsleistungen erbringt)	max. Aufwand	Termin/ Zeitraum	Ort

- ☐ Gemäß dem in Nummer 2.3 vereinbarten Vorgehensmodell V-Modell XT* bzw. dem vereinbarten organisationsspezifischen V-Modell XT* ergibt sich die Mitwirkung des Auftraggebers aus dem Lastenheft gemäß Anlage Nr. _____ und dem Teil „Mitwirkung und Beistellungen des Auftraggebers“ des Projekthandbuchs (AN) gemäß Anlage Nr. _____.
- ☐ Die Mitwirkung des Auftraggebers ergibt sich aus Anlage Nr. _____.



Systemvertrag

14 Abnahme

14.1 Gegenstand der Abnahme

Der Abnahmegegenstand ist das Gesamtsystem im Sinne dieses Vertrages und, soweit in Nummer 8 vereinbart, die einer Teilabnahme unterliegenden, in sich abgeschlossenen und funktional nutzbaren Teile des Gesamtsystems.

- ☐ Ergänzende Vereinbarungen zum Gegenstand der Abnahme gemäß Anlage Nr. _____.
- ☐ Das Gesamtsystem beinhaltet jeweils die aktuellste Version der vereinbarten Software* zum Zeitpunkt des Beginns der Erklärung der Betriebsbereitschaft*.

14.2 Testdaten

- ☐ Die Testdaten erstellt der Auftraggeber. Einzelheiten gemäß Anlage Nr. _____.
- ☐ Die Testdaten erstellt der Auftragnehmer. Einzelheiten gemäß Anlage Nr. _____.

14.3 Dauer, Ort und Systemumgebung* der Funktionsprüfung

- ☐ Dauer der Funktionsprüfungszeit (abweichend von der 30tägigen Frist in Ziffer 12.3 Satz 1 EVB-IT System-AGB): _____.
- ☐ Dauer der Funktionsprüfungszeit für teilabzunehmende Leistungen (abweichend von der 14tägigen Frist in Ziffer 12.3 Satz 2 EVB-IT System-AGB): _____.
- ☐ Ort der Funktionsprüfung (abweichend von Ziffer 12.4 EVB-IT System-AGB): _____.
- ☐ Ort der Funktionsprüfung für teilabzunehmende Leistungen (abweichend von Ziffer 12.4 EVB-IT System-AGB): _____.
- ☐ Ort und Dauer der Funktionsprüfung(en) ergeben sich aus Anlage Nr. _____ (abweichend von Ziffern 12.3 und 12.4 EVB-IT System-AGB).
- ☐ Abweichend von Ziffer 12.6 EVB-IT System-AGB beträgt der Zeitrahmen für erneute Funktionsprüfungen statt 14 Tagen jeweils _____.
- ☐ Die Durchführung der Funktionsprüfung erfolgt abweichend von Ziffer 12.4 EVB-IT System-AGB nicht in der in Nummer 3 genannten, sondern in folgender Systemumgebung*: _____.

14.4 Vereinbarungen zur Durchführung der Funktionsprüfung und zur Erklärung der Abnahme

- ☐ Gemäß dem in Nummer 2.3 vereinbarten Vorgehensmodell V-Modell XT* ergeben sich die Regelungen zur Durchführung der Funktionsprüfung und der Abnahme aus dem Lastenheft gemäß Anlage Nr. _____ und den Teilen des Projektplans (AN), die der Auftraggeber in Umsetzung seiner Vorgaben in der Ausschreibung mindestens gefordert hat gemäß Anlage Nr. _____.
- ☐ Die Regelungen zur Durchführung der Funktionsprüfung und der Abnahme ergeben sich aus Anlage Nr. _____ (abweichend von Ziffer 12 EVB-IT System-AGB).

14.5 Vereinbarungen zu Mängelklassen im Rahmen der Funktionsprüfung

- ☐ Abweichend von Ziffer 3 EVB-IT System-AGB werden in Anlage Nr. _____ die dort genannten Mängelklassen vereinbart.
- ☐ Abweichend von Ziffer 12 EVB-IT System-AGB werden die Auswirkungen der bei der Funktionsprüfung gefundenen Mängel in Anlage Nr. _____ vereinbart.

15 Mängelhaftung (Gewährleistung)

15.1 Verjährungsfrist (Gewährleistungsfrist) für Mängel des Gesamtsystems

- ☐ Es gilt Ziffer 13.3 EVB-IT System-AGB mit der Maßgabe, dass für Sachmängel und Rechtsmängel, die nicht Rechtsmängel der Individualsoftware* sind, die Verjährungsfrist statt 24 Monate _____ Monate beträgt.
- ☐ Es gilt Ziffer 13.3 EVB-IT System-AGB mit der Maßgabe, dass für Rechtsmängel der Individualsoftware* die Verjährungsfrist statt 36 Monate _____ Monate beträgt.



Systemvertrag

- ☐ Anstelle der in Ziffer 13.3 EVB-IT System-AGB geregelten zwölffmonatigen Frist für den Rücktritt bezogen auf die Standardsoftware* tritt eine _____ monatige Frist.
- ☐ Es gilt Ziffer 13.3 EVB-IT System-AGB mit der Maßgabe, dass die für Rechtsmängel an Individualsoftware* vereinbarte Verjährungsfrist für Rechtsmängel an folgenden vereinbarten Systemkomponenten* _____ gilt.
- ☐ Die Verjährungsfristen für Sach- und Rechtsmängel ergeben sich aus Anlage Nr. _____.

15.2 Verjährungsfrist (Gewährleistungsfrist) für Mängel an Teilleistungen

- ☐ Abweichend von Ziffer 13.4 EVB-IT System-AGB endet die Verjährungsfrist für Mängel an Teilleistungen nicht zwei Jahre nach der Teilabnahme und frühestens neun Monate nach der Gesamtabnahme, sondern gemäß Anlage Nr. _____.

15.3 Mängelmeldungen

15.3.1 Form der Mängelmeldung

Abweichend von Ziffer 11.3 EVB-IT System-AGB erfolgt die Mängelmeldung gemäß Anlage Nr. _____.

15.3.2 Adresse für Mängelmeldungen

Die Mängelmeldung erfolgt:

- ☐ an folgende Adresse:

Adressdaten	
Name/Firma:	
Organisationseinheit/Abteilung:	
☐ Postanschrift:	
☐ Telefon:	
☐ Fax:	
☐ E-Mail:	
☐ Web-Adresse:	

- ☐ gemäß Anlage Nr. _____.

15.4 Reaktions-* und Wiederherstellungszeiten*, Servicezeiten, Hotline

15.4.1 Reaktions-* und Wiederherstellungszeiten*, Mängelklassen

- ☐ Für die Zeit bis zur Verjährung der Mängelansprüche (Gewährleistungsfrist) werden folgende Reaktions-* und Wiederherstellungszeiten* vereinbart:

Mängelklasse	Reaktionszeit* in Stunden	Wiederherstellungszeit* in Stunden
Betriebsverhindernder Mangel		
Betriebsbehindernder Mangel		
Leichter Mangel		



Systemvertrag

Reaktions-* und Wiederherstellungszeiten* beginnen ausschließlich mit dem Zugang der Mängelmeldung während der Servicezeiten und laufen ausschließlich während der vereinbarten Servicezeiten.

Ergänzend können in Nummer 17.2 für die Nichteinhaltung der o.g. Zeiten Vertragsstrafen vereinbart werden.

- ☐ Die Reaktions-* und Wiederherstellungszeiten* werden in Anlage Nr. _____ für die dort abweichend von Ziffer 3 EVB-IT System-AGB definierten Mängelklassen festgelegt.

15.4.2 Servicezeiten

- ☐ Es werden folgende Servicezeiten vereinbart:

Tag	Uhrzeit
_____ bis _____	von _____ bis _____ Uhr
An Sonntagen	von _____ bis _____ Uhr
An Feiertagen am Erfüllungsort	von _____ bis _____ Uhr

15.4.3 Hotline

- ☐ Der Auftragnehmer gewährt eine telefonische deutschsprachige Unterstützung (Hotline) zu folgenden Zeiten:

Tag	Uhrzeit
_____ bis _____	von _____ bis _____ Uhr
An Sonntagen	von _____ bis _____ Uhr
An Feiertagen am Erfüllungsort	von _____ bis _____ Uhr

- ☐ Weitere Vereinbarungen zur Hotline (Leistungsumfang) gemäß Anlage Nr. _____.

15.5 Teleservice*

- ☐ Der Auftragnehmer erbringt Teile der Leistung mittels Teleservice* entsprechend der Teleservicevereinbarung gemäß Anlage Nr. _____.

15.6 Weitere Vereinbarungen zur Mängelhaftung

- ☐ Der Ausschluss der Rechtsmängelhaftung wegen Patentverletzungen, die Dritte gegen den Auftraggeber wegen einer Nutzung außerhalb von EU und EFTA geltend machen (Ziffer 13.7 EVB-IT System-AGB), gilt nicht.
- ☐ Weitere Vereinbarungen gemäß Anlage Nr. _____.

16 Haftungsregelungen

16.1 Haftungsobergrenze bei leicht fahrlässiger Pflichtverletzung

- ☐ Abweichend von Ziffer 15.1 EVB-IT System-AGB beträgt die Haftungsobergrenze für leicht fahrlässige Pflichtverletzungen insgesamt für diesen Vertrag _____ Euro.
- ☐ Abweichend von Ziffer 15.1 EVB-IT System-AGB gelten für die Haftung bei leicht fahrlässigen Pflichtverletzungen die Regelungen gemäß Anlage Nr. _____.



Systemvertrag

16.2 Haftung bei Verzug

- ☐ Abweichend von Ziffer 15.1 EVB-IT System-AGB beträgt die Haftungsobergrenze für Verzug bei leichter Fahrlässigkeit insgesamt für diesen Vertrag 50 % des Auftragswertes*.
- ☐ Abweichend von Ziffer 15.1 EVB-IT System-AGB gelten für die Haftung für Verzug bei leichter Fahrlässigkeit die Regelungen gemäß Anlage Nr. _____.

16.3 Haftung für den Systemservice

- ☐ Abweichend von Ziffer 15.2 EVB-IT System-AGB beträgt die Haftungsobergrenze für leicht fahrlässige Pflichtverletzungen beim Systemservice insgesamt _____ Euro pro Vertragsjahr.
- ☐ Abweichend von Ziffer 15.2 EVB-IT System-AGB beträgt die Haftungsobergrenze für leicht fahrlässige Pflichtverletzungen beim Systemservice insgesamt für diesen Vertrag _____ Euro.
- ☐ Abweichend von Ziffer 15.2 EVB-IT System-AGB beträgt die Haftungsobergrenze für leicht fahrlässige Pflichtverletzungen beim Systemservice
 - ☐ minimal das _____fache (statt des Doppelten)
 - ☐ maximal das _____fache (statt des Vierfachen)der Vergütung, die für das erste Vertragsjahr des Systemservices zu zahlen ist. Ziffer 15.2 letzter Satz EVB-IT System-AGB bleibt unberührt.

16.4 Haftung für entgangenen Gewinn

- ☐ Abweichend von Ziffer 15.5 EVB-IT System-AGB haftet der Auftragnehmer auch für entgangenen Gewinn.

17 Vertragsstrafen bei Verzug

17.1 Verzug bei Erstellung des Gesamtsystems

- ☐ Abweichend von Ziffer 9.3 EVB-IT System-AGB gilt die dort aufgeführte Vertragsstrafe auch bei Überschreitung der für die einzelnen Meilensteine im Termin- und Leistungsplan gemäß Nummer 9 festgelegten Termine.
Die Summe der vorstehenden Vertragsstrafen ist auf den in Ziffer 9.3 EVB-IT System-AGB festgelegten Höchstbetrag anzurechnen.
- ☐ Abweichend von Ziffer 9.3 EVB-IT System-AGB gilt die dort aufgeführte Vertragsstrafe nicht bei Überschreitung der für die Teilabnahmen gemäß Nummer 8 festgelegten Termine.
- ☐ Abweichend von Ziffer 9.3 EVB-IT System-AGB wird bei Verzug der Leistung die Vertragsstrafenregelung gemäß Anlage Nr. _____ vereinbart.

17.2 Verzug bei Reaktions-* und Wiederherstellungszeiten*

- ☐ Zusätzlich zur Vertragsstrafe gemäß Ziffer 9.3 EVB-IT System-AGB werden in Anlage Nr. _____ Vertragsstrafen für die Nichteinhaltung der in Nummer 5.1.1.2 geregelten Reaktions-* und Wiederherstellungszeiten* zur Wiederherstellung der Betriebsbereitschaft* nach der Abnahme des Gesamtsystems vereinbart.
- ☐ Zusätzlich zur Vertragsstrafe gemäß Ziffer 9.3 EVB-IT System-AGB werden in Anlage Nr. _____ Vertragsstrafen für die Nichteinhaltung der in Nummer 15.4.1 geregelten Reaktions-* und Wiederherstellungszeiten* im Rahmen der Mängelhaftung (Gewährleistung) vereinbart.

18 Weitere Vereinbarungen

18.1 Garantien

18.1.1 Auftragnehmergarantien

- ☐ Der Auftragnehmer übernimmt zusätzlich zu der in diesem Vertrag (Nummer 15 und Ziffer 13 EVB-IT System-AGB) vereinbarten Mängelhaftung eine Haltbarkeitsgarantie, deren Konkretisierung und/oder Begrenzung, z.B. des Inhalts oder der Rechtsfolgen in der Anlage Nr. _____ erfolgt.



Systemvertrag

- ☐ Der Auftragnehmer übernimmt zusätzlich zu der in diesem Vertrag vereinbarten Mängelhaftung (Nummer 15 und Ziffern 13, 14 EVB-IT System-AGB) eine Beschaffenheitsgarantie, deren Konkretisierung und/oder Begrenzung, z.B. des Inhalts oder der Rechtsfolgen in Anlage Nr. _____ erfolgt.

18.1.2 Herstellergarantien

- ☐ Der Auftragnehmer erklärt, dass die Hersteller der folgenden Systemkomponenten* folgende Haltbarkeitsgarantien übernehmen:

Tabelle und lfd. Nr. der betroffenen Systemkomponente* gemäß Nummer 4	Garantiebeginn	Dauer der Garantie in Monaten	Name des Herstellers	Umfang der Leistung im Garantiefall (z.B. VOS/BIS ¹)
lfd. Nr.				

Fußnote	Erläuterung
1	VOS = Vorortservice (am Erfüllungsort) BIS = Bring-In-Service (zum Auftragnehmer auf dessen Kosten)

- ☐ Weitere Vereinbarungen (Konkretisierung und/oder Begrenzung z.B. des Inhalts oder der Rechtsfolgen) zur Haltbarkeitsgarantie und/oder Beschaffenheitsgarantie des Herstellers gemäß Anlage Nr. _____.

18.2 Übergabe bzw. Hinterlegung des Quellcodes*

18.2.1 Übergabe des Quellcodes*

- ☐ Abweichend von Ziffern 18.1 und 18.2 EVB-IT System-AGB wird der Quellcode* der Individualsoftware* gemäß Anlage Nr. _____ übergeben.
- ☐ Abweichend von Ziffern 18.1 und 18.2 EVB-IT System-AGB wird die Individualsoftware* gemäß Nummer 4.5.1 lfd. Nr. _____ nur im Objektcode* und nicht im Quellcode* übergeben.
- ☐ Abweichend von Ziffern 18.1 und 18.2 EVB-IT System-AGB wird der Quellcode* der Anpassungen der Standardsoftware*, die nicht in den Standard übernommen werden, gemäß Ziffer 2.3.3 EVB-IT System-AGB gemäß Anlage Nr. _____ übergeben.
- ☐ Abweichend von Ziffern 18.1 und 18.2 EVB-IT System-AGB wird der Quellcode* der Individualsoftware* am Ende jedes Erstellungstages in dem Software-Depository des Auftraggebers gespeichert.
- ☐ Näheres ergibt sich aus Anlage Nr. _____.
- ☐ Abweichend von Ziffer 18.1 EVB-IT System-AGB wird der Quellcode* der Anpassungen der Standardsoftware* gemäß Ziffer 2.3.3 EVB-IT System-AGB am Ende jedes Erstellungstages in dem Software-Depository des Auftraggebers gespeichert.
- ☐ Näheres ergibt sich aus Anlage Nr. _____.

Die Pflichten in Bezug auf die Übergabe des Quellcodes* von Open Source Software* bleiben von den vereinbarten Abweichungen nach dieser Nummer 18.2.1 unberührt.

18.2.2 Hinterlegung des Quellcodes

- ☐ Es wird gemäß Ziffer 18.3 EVB-IT System-AGB die Hinterlegung des Quellcodes* folgender Standardsoftware* oder Individualsoftware* (abweichend von Ziffer 18.1 EVB-IT System-AGB) vereinbart.

Systemvertrag

Lfd. Nr. aus Tabelle	Hinterlegungsstelle und Hinterlegungsvereinbarung	Beitritt zu einer bestehenden Hinterlegungsvereinbarung ja/nein
Tabelle lfd. Nr.	Hinterlegungsstelle: Hinterlegungsvereinbarung gemäß Anlage Nr.	

18.3 Haftpflichtversicherung

- ☐ Der Nachweis einer Haftpflichtversicherung gemäß Ziffer 19.1 EVB-IT System-AGB wird vereinbart.

18.4 Sicherheiten

18.4.1 Vorauszahlungsbürgschaft

- ☐ Die Übergabe einer Vorauszahlungsbürgschaft gemäß Ziffer 20.1.1 EVB-IT System-AGB wird vereinbart.
- ☐ Abweichend von Ziffer 20.1.1 EVB-IT System-AGB beträgt die Höhe der Vorauszahlungsbürgschaft statt 100% der Vorauszahlung _____ Euro (Hinweis: wenn niedriger als 100% der Vorauszahlung, haushaltsrechtlich i.d.R. nicht zulässig).

18.4.2 Vertragserfüllungs- oder Mängelhaftungssicherheit

Es werden für die Vertragserfüllung folgende Vertragserfüllungs- oder Mängelhaftungssicherheiten vereinbart:

- ☐ Vertragserfüllung

Es wird die Leistung einer Sicherheit für die Vertragserfüllung durch Hinterlegung von Geld auf einem Sperrkonto oder Übergabe einer Vertragserfüllungsbürgschaft gemäß Ziffer 20.1.2 EVB-IT System-AGB vereinbart.

Höhe der Sicherheit:

- ☐ Abweichend von Ziffer 20.1.2 EVB-IT System-AGB beträgt die Höhe der Sicherheit _____ % des Erstellungspreises*.
- ☐ Abweichend von Ziffer 20.1.2 EVB-IT System-AGB wird die teilweise Rückgabe der Sicherheit nach Teilabnahmen gemäß Anlage Nr. _____ geregelt.

Der Auftraggeber kann eine Anpassung der Sicherheit gemäß Ziffer 20.1.2 EVB-IT System-AGB verlangen.

- ☐ Mängelhaftung (Gewährleistung)

Es wird die Leistung einer Sicherheit für die Mängelhaftung durch Hinterlegung von Geld auf einem Sperrkonto oder Übergabe einer Mängelhaftungsbürgschaft gemäß Ziffer 20.1.3 EVB-IT System-AGB vereinbart.

Höhe der Sicherheit:

- ☐ Abweichend von Ziffer 20.1.3 EVB-IT System-AGB beträgt die Höhe der Sicherheit _____ % des Auftragswertes*.

ODER

18.4.3 Kombinierte Vertragserfüllungs- oder Mängelhaftungssicherheit

Es wird die Leistung einer Sicherheit für die Vertragserfüllung und Mängelhaftung durch Hinterlegung von Geld auf einem Sperrkonto oder Übergabe einer Vertragserfüllungs- und Mängelhaftungsbürgschaft gemäß Ziffer 20.1.4 EVB-IT System-AGB vereinbart.

- ☐ kombinierte Vertragserfüllungs- und Mängelhaftungssicherheit

Höhe der Sicherheit:



Systemvertrag

- ☐ Abweichend von Ziffer 20.1.4 EVB-IT System-AGB beträgt die Höhe der Sicherheit für die Vertragserfüllung _____% des Erstellungspreises* und für die Mängelhaftung _____% des Erstellungspreises*.

Der Auftraggeber kann eine Anpassung der Sicherheit gemäß Ziffer 20.1.4 EVB-IT System-AGB verlangen.

18.5 Datenschutz, Geheimhaltung und Sicherheit

- ☐ Ergänzend zu bzw. abweichend von Ziffer 21 EVB-IT System-AGB ergeben sich Regelungen zur Geheimhaltung bzw. zur Sicherheit aus Anlage Nr. _____.
- ☐ Da durch den Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet werden sollen (Auftragsdatenverarbeitung), treffen die Parteien in Anlage Nr. _____ eine schriftliche Vereinbarung, die zumindest die gesetzlichen Mindestanforderungen beinhaltet (z.B. gemäß DSGVO).
- ☐ Die Parteien treffen sonstige Vereinbarungen zum Datenschutz gemäß Anlage Nr. _____.

18.6 Vereinbarungen zur Korruptionsprävention

Der Auftragnehmer verpflichtet sich für die Laufzeit des Vertrages

- ☐ die in Anlage Nr. _____ aufgeführten Vorschriften zur Korruptionsprävention in der öffentlichen Verwaltung zu beachten.
- ☐ folgende weitere Regelungen einzuhalten: _____.

18.7 Kündigungsrecht des Auftraggebers

- ☐ Abweichend von den gesetzlichen Regelungen und Ziffer 16.2 EVB-IT System-AGB ergeben sich die Ansprüche des Auftragnehmers bei einer Kündigung des Auftraggebers gemäß § 648 BGB aus Anlage Nr. _____.

18.8 Sonstige Vereinbarungen

- ☐ Sonstige Vereinbarungen: _____
- ☐ Die sonstigen Vereinbarungen ergeben sich aus Anlage Nr. _____.

Unterschrift Auftraggeber

Unterschrift Auftragnehmer

Datum, Auftraggeber

Datum, Auftragnehmer

Anlage [X] zum EVB-IT Vertrag

Gesamtkonzept für Exit, Service-Transition, Incident Management (SLAs) und Vergütungsregelungen

Vergabeverfahren: Cybersecurity Managed Services (SOC/SIEM, NDR, Vulnerability Management, EDR-Management, IoMT-Security)

Auftraggeber: Universitätsklinikum Frankfurt / Universitätsmedizin Frankfurt

Die fachlichen Anforderungen an die Leistung ergeben sich aus der Leistungsbeschreibung D1. Soweit diese Anlage auf D1 Bezug nimmt, gilt die dortige Regelung; diese Anlage regelt die zugehörigen Fristen, Vergütungen und Rechtsfolgen. Bei Widersprüchen hat D1 für den Leistungsinhalt Vorrang, diese Anlage für Fristen, Vergütung und Rechtsfolgen.

TEIL A: EXIT- UND SERVICE-TRANSITION

§ 1 Gegenstand und Zielsetzung

(1) Dieser Teil regelt die Pflichten des Auftragnehmers bei Beendigung des Vertrags (sei es durch Zeitablauf der 60 Monate, ordentliche oder außerordentliche Kündigung), um eine unterbrechungsfreie Übergabe der Leistungsbereiche SOC/SIEM, NDR, Vulnerability Management, EDR-Management und IoMT-Security sowie des Incident Managements an den Auftraggeber oder einen vom Auftraggeber benannten Nachfolgedienstleister (nachfolgend „Dritter“) zu gewährleisten. Die Vertragslaufzeit beginnt mit dem Cut-over gemäß D1 Kapitel 9.5.

(2) Das übergeordnete Ziel ist die Vermeidung eines Lock-in-Effekts sowie die Sicherstellung der vollen Business Continuity während der Transition-Phase. Eine Überwachungslücke darf zu keinem Zeitpunkt entstehen.

(3) Die Auslöser eines Exit-Prozesses richten sich im Übrigen nach D1 Kapitel 14.1.

§ 2 Allgemeine Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer verpflichtet sich, die Beendigungsphase aktiv, kooperativ und nach besten Kräften zu unterstützen. Er wird sämtliche hierfür erforderlichen Informationen und Daten unverzüglich und vollständig bereitstellen.

(2) Der Auftragnehmer wird auf Anforderung des Auftraggebers mit dem Dritten im erforderlichen Umfang zusammenarbeiten. Dies schließt die Teilnahme an Abstimmungsgesprächen (Jour Fixe) zur Steuerung des Transitionsverfahrens ein.

§ 3 Bereitstellung von Dokumentation und Wissenstransfer

(1) Spätestens 3 Monate vor Ablauf der regulären Vertragslaufzeit (bzw. unverzüglich im Falle einer außerordentlichen Kündigung) hat der Auftragnehmer sämtliche Übergabeobjekte gemäß D1 Kapitel 14.3 auf den aktuellen Stand zu bringen und dem Auftraggeber in elektronisch editierbarer Form zu übergeben. Dies umfasst insbesondere Betriebsdokumentation und Betriebshandbuch, Architektur-, Schnittstellen- und Datenflussdokumentation, den Logquellen-, Sensorik- und Integrationskatalog, UKF-spezifische Use Cases, Detection-Regeln, Korrelationslogiken, Playbooks und Runbooks sowie Policies, Ausnahmen und Konfigurationen.

(2) Der Auftragnehmer legt das Exit-Konzept gemäß D1 Kapitel 14.2 spätestens im Rahmen der Transition vor und schreibt es mindestens jährlich sowie bei wesentlichen Änderungen fort.

(3) Auf Anforderung des Auftraggebers führt der Auftragnehmer einen strukturierten Wissenstransfer (Workshops/Einweisungen) für die Mitarbeiter des Auftraggebers oder des Dritten durch. Der Umfang beträgt bis zu 5 Personentage, sofern nicht anders vereinbart.

§ 4 Datenhoheit, Datenmigration und Bereinigung

(1) Alle sicherheitsrelevanten Daten, Protokolle, Logfiles, Telemetriedaten, Incident-Informationen und konfigurationsspezifischen Datenbanken stehen gemäß D1 Kapitel 3.1 im ausschließlichen Eigentum des Auftraggebers. Für kundenbezogene Plattform- und Produktlizenzen gilt D1 Kapitel 3.2 und 14.5.

(2) Der Auftragnehmer ist verpflichtet, alle exportierbaren Daten in einem gängigen, offenen und maschinenlesbaren Standardformat (z. B. CSV, JSON, native Plattform-Exporte) strukturiert und vollständig über einen gesicherten Übertragungsweg an den Auftraggeber zu übergeben.

(3) Erst nach schriftlicher Freigabe durch den Auftraggeber und nach Bestätigung der erfolgreichen Migration durch den Dritten hat der Auftragnehmer alle Daten auf seinen eigenen Systemen (z. B. in Ticketsystemen, Backup-Speichern des Incident Managements) nach den Vorgaben des BSI (Bundesamt für Sicherheit in der Informationstechnik) datenschutzkonform und unwiderruflich zu löschen. Die Löschung ist gemäß D1 Kapitel 14.4 in einem Löschprotokoll zu dokumentieren und zu bestätigen.

§ 5 Aufrechterhaltung des laufenden Betriebs während der Transition

(1) Während der gesamten Transitionsphase – auch über das rechtliche Vertragsende hinaus, sofern für die Migration erforderlich – gelten die in Teil B dieser Anlage vereinbarten Service Levels (SLAs) und Incident-Management-Prozesse uneingeschränkt weiter.

(2) Der Auftragnehmer darf Monitoring, Alarmbearbeitung, Eskalation, Support oder den Zugriff auf administrative Werkzeuge nicht vor der endgültigen Systemübergabe einschränken oder einstellen.

(3) Die Meldefähigkeit für regulatorisch relevante Sicherheitsvorfälle (§ 32 BSIG, Art. 33 DSGVO) einschließlich der abgestimmten Meldevorlagen, Rollen und Eskalationskontakte gemäß D1 Kapitel 9.5 und 9.7 bleibt bis zum abgeschlossenen Übergang an den Auftraggeber oder den Dritten uneingeschränkt erhalten.

(4) Der Exit gilt erst als abgeschlossen, wenn die Voraussetzungen gemäß D1 Kapitel 14.6 erfüllt sind. Der Abschluss wird durch ein Übergabe- bzw. Abnahmeprotokoll dokumentiert.

TEIL B: INCIDENT MANAGEMENT UND SLAs

§ 6 Servicezeiten und Erreichbarkeit

(1) Das Incident Management steht dem Auftraggeber während der vertraglich vereinbarten Servicezeiten zur Verfügung.

(2) Die Servicezeiten richten sich nach D1 Kapitel 12.2 und werden definiert als:

- Prioritäten P1 und P2: 24 Stunden an 7 Tagen der Woche, einschließlich Sonn- und Feiertagen.
- Prioritäten P3 und P4: Montag bis Freitag 08:00 Uhr bis 17:00 Uhr (MEZ/MESZ), ausgenommen die gesetzlichen Feiertage des Landes Hessen, mit definierten Eskalationspfaden bei Lageänderung.

(3) Der Auftragnehmer stellt einen 24×7-Sicherheitskontakt gemäß D1 Kapitel 12.5 bereit.

§ 7 Definition der Prioritäten (Fehlerklassen) und SLA-Matrix

(1) Eingehende sicherheitsrelevante Ereignisse werden gemäß D1 Kapitel 12.1 in eine der vier Prioritäten P1 bis P4 eingestuft. Maßgeblich für die Priorisierung ist die fachliche Auswirkung auf Verfügbarkeit, Integrität, Vertraulichkeit, Patientensicherheit, kritische Dienste und regulatorische Anforderungen, nicht die technische Herkunft des Ereignisses. Die Priorisierung ist vom Auftragnehmer nachvollziehbar zu begründen; Reklassifizierungen sind zu dokumentieren.

(2) Die Bearbeitung wird über die vier Kennzahlen gemäß D1 Kapitel 12.2 gemessen. Die Zeitmessung beginnt mit Erzeugung eines Alarms durch die Plattform und wird über das gesamte SOC-Team gemessen; sie darf nicht durch interne Übergaben des Auftragnehmers unterbrochen oder zu Lasten des Auftraggebers verlängert werden. Die Fristen laufen für P1 und P2 durchgehend, für P3 ausschließlich innerhalb der Servicezeit gemäß § 6 Abs. 2.

Priorität	TTT	TTV	TTC	TTN	Zielerreichung (Quote pro Monat)
P1 - kritisch	15 Min.	30 Min.	15 Min.	15 Min.	99,5 %
P2 - hoch	30 Min.	60 Min.	30 Min.	60 Min.	98,5 %
P3 - mittel	60 Min.	4 Stunden	4 Stunden	2 Stunden	95,0 %
P4 - niedrig	/	/	/	/	/

Time to Triage (TTT): Zeitspanne von der Alarmerstellung bis zum Beginn der Analyse durch einen SOC-Analysten.

Time to Validate (TTV): Zeitspanne vom Analysebeginn bis zur validierten Einstufung als Incident (True Positive).

Time to Contain (TTC): Zeitspanne von der Validierung bis zur ersten aktiven Eindämmungsmaßnahme im freigegebenen Rahmen. Fällt ein Vorfall in die Stufe Guided Response gemäß D1 Kapitel 10.7, endet die Messung mit der dokumentierten Übergabe einer konkreten, priorisierten Handlungsempfehlung an den Auftraggeber; die Umsetzungszeit beim Auftraggeber wird nicht angerechnet.

Time to Notify (TTN): Zeitspanne von der Validierung bis zur Benachrichtigung des Auftraggebers bei Eskalation oder Guided Response.

Zielerreichung: Der prozentuale Anteil der Vorgänge pro Kalendermonat innerhalb einer Prioritätsstufe, bei denen sämtliche für die jeweilige Priorität maßgeblichen Kennzahlen eingehalten wurden.

(3) Für P4 gelten gemäß D1 Kapitel 12.2 keine zeitlichen Bearbeitungs-SLAs; die Bearbeitung erfolgt im Regelreporting.

(4) Stellt sich während der Analyse heraus, dass ein Vorfall höher einzustufen ist, greifen die schärferen Kennzahlen ab dem Zeitpunkt der Reklassifizierung. Eine rein automatisierte Meldung ohne fachliche Bewertung erfüllt die Kennzahlen nicht.

(5) Zeiten, in denen die Bearbeitung nachweislich ausschließlich wegen einer ausstehenden Mitwirkung oder Freigabe des Auftraggebers ruht, werden nicht auf die Fristen angerechnet. Der Auftragnehmer dokumentiert Beginn und Ende dieser Zeiten im Vorgang.

(6) Ab dem Cut-over gemäß D1 Kapitel 9.5 gelten die Kennzahlen und die Rechtsfolgen dieses Teils für die Prioritäten P1 und P2 innerhalb des dort definierten Mindestschutzzumfangs. Für die Priorität P3 sowie für die Plattformverfügbarkeit gemäß D1 Kapitel 12.3 gelten sie ab dem Übergang in den Regelbetrieb gemäß D1 Kapitel 9.6.

(7) Der Auftragnehmer weist die Einhaltung der Kennzahlen monatlich im operativen Servicebericht gemäß D1 Kapitel 12.6 nach. Der Nachweis umfasst je Priorität die Anzahl der Vorgänge, die je Kennzahl eingehaltenen und überschrittenen Fristen sowie die daraus errechnete Zielerreichungsquote.

§ 8 Eskalationsmanagement und Vertragsstrafen bei SLA-Verletzung

(1) Überschreitet der Auftragnehmer eine der vereinbarten Kennzahlen gemäß § 7 Abs. 2 schuldhaft, gerät er ohne gesonderte Mahnung in Verzug.

(2) Für jede angefangene Stunde der Überschreitung der vereinbarten Fristen zahlt der Auftragnehmer eine Vertragsstrafe in Höhe von:

- Bei Priorität P1: 250,00 € pro angefangene Stunde.
- Bei Priorität P2: 100,00 € pro angefangene Stunde.
- Bei Priorität P3: 50,00 € pro angefangene Stunde.

(3) Unterschreitet der Auftragnehmer die monatliche Zielerreichungsquote in den Stufen P1 bis P3, wird für jeden Prozentpunkt der Unterschreitung ein pauschaler Abzug von 2 % des monatlichen Managed-Service-Entgelts fällig.

(4) Unterschreitet die Verfügbarkeit der vom Auftragnehmer betriebenen oder unmittelbar beeinflussbaren zentralen Plattformkomponenten den gemäß D1 Kapitel 12.3 geschuldeten Wert von 99,9 % im Monatsmittel, wird für jeden angefangenen Prozentpunkt der Unterschreitung ein pauschaler Abzug von 2 % des monatlichen Managed-Service-Entgelts fällig. Vereinbarte Wartungsfenster bleiben unberücksichtigt.

(5) Monatliches Managed-Service-Entgelt im Sinne dieser Anlage ist die Summe der monatlichen Entgelte für die laufenden Managed-Service-Anteile sämtlicher Leistungsbereiche gemäß Preisblatt (Positionen LV 4.1, LV 5A.2 bzw. LV 5B.3, LV 6.1, LV 7.2 und LV 8.1). Plattform- und Lizenzpositionen sowie einmalige und optionale Positionen bleiben unberücksichtigt. Während des Ramp-up-Betriebs tritt an die Stelle dieses Betrags das monatliche Entgelt der Position LV M1.2.

(6) Die maximale Vertragsstrafe pro Incident ist auf 5.000,00 € gedeckelt. Die Gesamt-Vertragsstrafen und pauschalen Abzüge pro Vertragsmonat dürfen 10 % des monatlichen Managed-Service-Entgelts nicht überschreiten.

(7) SLA-Abweichungen sind gemäß D1 Kapitel 12.6 unverzüglich zu analysieren, zu dokumentieren und im nächsten Servicebericht auszuweisen. Bei Abweichungen der Prioritäten P1 oder P2 ist eine gesonderte Ursachenanalyse vorzulegen. Das Eskalationsmodell richtet sich nach D1 Kapitel 12.5.

§ 8a Außerordentliches Kündigungsrecht bei wiederholter SLA-Verfehlung

(1) Verfehlt der Auftragnehmer die monatliche Zielerreichungsquote der Priorität P1 oder P2 gemäß § 7 Abs. 2, die Kennzahlen TTT, TTV, TTC oder TTN gemäß § 7 Abs. 2 bei Vorgängen der Priorität P1 oder P2 oder die Plattformverfügbarkeit gemäß § 8 Abs. 4 in drei (3) aufeinanderfolgenden Kalendermonaten oder in insgesamt vier (4) Kalendermonaten innerhalb eines Zeitraums von zwölf (12) Monaten, liegt ein wichtiger Grund zur außerordentlichen Kündigung vor.

(2) Der Auftraggeber ist in diesem Fall berechtigt, den Vertrag mit einer Frist von 30 Tagen zum Monatsende ganz oder teilweise zu kündigen.

(3) Der Auftragnehmer ist verpflichtet, die Leistungen auf Verlangen des Auftraggebers für bis zu sechs (6) Monate nach dem Kündigungstermin gegen Fortzahlung der vereinbarten Vergütung zur Sicherung einer reibungslosen Migration auf einen Nachfolgedienstleister unvermindert fortzuführen. Während dieses Zeitraums gelten die Regelungen des Teils B dieser Anlage uneingeschränkt weiter.

(4) Bereits entstandene Ansprüche auf Vertragsstrafen und pauschale Abzüge gemäß § 8 bleiben von einer Kündigung unberührt; sie sind bis zur tatsächlichen Beendigung der Leistungserbringung einschließlich eines Zeitraums gemäß Absatz 3 auszuzahlen oder zu verrechnen.

TEIL C: VERGÜTUNGSREGELUNGEN UND MEILENSTEINE

§ 9 Zahlungsplan und Fälligkeit (Einmalige Vergütung)

Die einmalige Vergütung für Implementierung, Transition und Einweisung (Abschnitt 6 des Preisblatts) wird nach folgendem Meilensteinplan fällig. Voraussetzung ist jeweils der vom Auftraggeber schriftlich bestätigte Phasen- bzw. Meilensteinabschluss gemäß D1 Kapitel 9.

Position	Bedingung	Bezug in D1
LV 9.1 – Kick-off & Projektorganisation	Projektorganisation, Rollen, Kommunikationswege, RACI und initiale Risikoübersicht sind bestätigt	Kapitel 9.1, Phase 1
LV 9.2 – Bestandsaufnahme & Feinkonzeption	Die Feinkonzeption ist vom Auftraggeber schriftlich freigegeben	Kapitel 9.1, Phase 2
LV 9.3 – Bereitstellung & Implementierung	Die Leistungsbestandteile der Phase 3 sind gemäß Projektplan fertiggestellt	Kapitel 9.1, Phase 3
LV M1.1 – Übernahme der Serviceverantwortung	Der Mindestschutzumfang zum Cut-over ist hergestellt und protokolliert abgenommen	Kapitel 9.5
LV M1.3 – Lizenzanschluss NDR/VM im Zwischenzeitraum	Der durchgehende Lizenzanschluss für den Zwischenzeitraum ist nachgewiesen	Kapitel 9.4
LV 9.4 – Test & Validierung	Abnahmeprotokoll mit Restpunktliste liegt vor	Kapitel 9.6
LV 9.5 – Schulung & Wissenstransfer	Initialschulung ist durchgeführt, Betriebshandbuch und Knowledge Base sind übergeben	Kapitel 9.7
LV 9.6 – Go-Live & Hypercare	Die Hypercare-Phase ist ohne wesentliche offene Restpunkte abgeschlossen	Kapitel 9.8

Die einmaligen Positionen der Leistungsbereiche NDR (LV 5A.1 bzw. LV 5B.1 und LV 5B.2) und EDR (LV 7.1) werden mit der protokollierten Abnahme der jeweiligen Übernahme oder Migration fällig.

§ 10 Vergütung der laufenden Leistungen

(1) Die Vergütung für den Managed Service und die Einhaltung der SLAs (Teil B) erfolgt als monatliche Pauschale gemäß den laufenden Positionen des Preisblatts.

(2) Die Abrechnung erfolgt zwingend monatlich nachträglich nach Ablauf des jeweiligen Leistungsmonats und nach Vorlage des Serviceberichts einschließlich des SLA-Nachweises gemäß § 7 Abs. 7.

(3) Vom Cut-over bis zum Übergang in den Regelbetrieb wird der Ramp-up-Betrieb über die Position LV M1.2 nach seiner tatsächlichen Dauer vergütet. Die laufenden Managed-Service-Anteile (LV 4.1, LV 5A.2 bzw. LV 5B.3, LV 6.1, LV 7.2 und LV 8.1) werden ab dem Übergang in den Regelbetrieb abgerechnet. Eine gleichzeitige Abrechnung beider Positionsgruppen für denselben Leistungsmonat ist ausgeschlossen. Die Vertragslaufzeit von 60 Monaten ab Cut-over bleibt unberührt.

(4) Die Vergütung der Plattform- und Lizenzpositionen richtet sich nach dem tatsächlichen Beginn des jeweiligen Lizenz- bzw. Betriebsanschlusses gemäß D1 Kapitel 9.4.

§ 11 Vergütung von Exit-Leistungen (Kopplung an das Preisblatt)

(1) Die Bereitstellung der Übergabeobjekte, des Exit-Konzepts sowie der vollständige Datenexport gemäß § 3 und § 4 dieser Anlage sind mit der regulären, laufenden Managed-Service-Vergütung abgegolten. Für diese Grundleistungen fällt kein separates Entgelt an.

(2) Weitergehende Unterstützungsleistungen (z. B. Wissenstransfer über den Umfang gemäß § 3 Abs. 3 hinaus oder Migrationsbegleitung) werden nach tatsächlichem Aufwand abgerechnet.

(3) Die Abrechnung dieser zusätzlichen Leistungen erfolgt zwingend auf Basis der vom Auftragnehmer im Angebot eingereichten Stundenverrechnungssätze gemäß Abschnitt 7 des Preisblatts. Es dürfen ausschließlich die dort für die jeweiligen Personalkategorien verbindlich angebotenen Sätze herangezogen werden. Aufschläge über die dort angebotenen Zuschläge hinaus sind unzulässig.

(4) Der Auftragnehmer muss vor Beginn jeglicher Exit-Leistungen ein schriftliches Aufwandsschätzungsangebot vorlegen, welches vom Auftraggeber schriftlich freigegeben werden muss.

(5) Auf Grundlage seiner Expertise in diesem Umfeld kalkuliert der Auftragnehmer im Angebot eigenverantwortlich den erforderlichen Aufwand für die Unterstützung des Auftraggebers und ggf. eines Dritten bei der Exit-Transition gemäß Position LV 14.1 des Preisblatts und bietet diesen als Gesamtbetrag an.

Die Abrechnung erfolgt nach tatsächlichem Aufwand auf Basis des angebotenen Personaleinsatzes gemäß den Stundenverrechnungssätzen aus Abschnitt 7 des Preisblatts, wobei ein Personentag acht (8) Leistungsstunden entspricht. Zuschläge gemäß Abschnitt 7 des Preisblatts finden auf diese Position keine Anwendung.

Dem Auftraggeber wird das Recht eingeräumt, diese Leistungen als Option ganz oder teilweise abzurufen. Der im Angebot des Auftragnehmers ausgewiesene Gesamtbetrag bildet bei Zuschlagserteilung das maximal abrufbare Budget (Budgetobergrenze) für diese Leistungen, auf welches der Auftraggeber beim Exit direkt referenzieren kann.

Ein Anspruch auf Abnahme des vollen Budgetvolumens besteht nicht. Der Abruf erfolgt nach dem Freigabeverfahren gemäß Absatz 4. Leistungen gemäß Absatz 2 werden auf dieses Budget angerechnet.

(6) Für den Fall einer optionalen temporären Weiterführung der laufenden SOC-Betriebsleistungen gemäß § 8a Abs. 3 über das reguläre Vertragsende hinaus, wird diese zu den zu diesem Zeitpunkt geltenden monatlichen Pauschalen der laufenden Positionen des Preisblatts (LV 4.1, LV 5A.2 bzw. LV 5B.3, LV 6.1, LV 7.2 und LV 8.1) vergütet; bei einer Weiterführung einzelner Leistungsbereiche anteilig nach den betroffenen Positionen.

Zuschläge sind ausgeschlossen. Diese Vergütung zur Aufrechterhaltung der Business Continuity ist nicht auf das optionale Budget gemäß Absatz 5 anzurechnen.

Das Freigabeverfahren nach Absatz 4 gilt für die reine Betriebsweiterführung nicht.

§ 12 Preisanpassungsklausel (Indexierung)

(1) Die monatlichen Pauschalen für den Managed Service bleiben für die ersten 36 Monate ab dem Cut-over gemäß D1 Kapitel 9.5 unverändert (Festpreisphase).

(2) Nach Ablauf der Festpreisphase ist der Auftragnehmer berechtigt, eine Anpassung der monatlichen Pauschalen zu verlangen. Die Anpassung orientiert sich an der Entwicklung des vom Statistischen Bundesamt veröffentlichten Verbraucherpreisindex für Deutschland (VPI). Basis für die erste Anpassung ist der Indexstand im Monat des Cut-over. Eine Erhöhung kann frühestens nach Ablauf von jeweils 12 weiteren Monaten verlangt werden und muss 3 Monate im Voraus angekündigt werden.

(3) Die Preiserhöhung wird auf maximal 2 % pro Vertragsjahr gedeckelt. Sinkt der VPI, ist der Auftraggeber berechtigt, eine entsprechende Absenkung der Pauschalen zu verlangen.

(4) Plattform- und Lizenzpositionen sowie die Stundenverrechnungssätze gemäß Abschnitt 7 des Preisblatts sind von der Anpassung ausgenommen.



System-AGB

Ergänzende Vertragsbedingungen für die Erstellung eines Gesamtsystems

– EVB-IT System AGB –

Inhaltsangabe

1	Gegenstand des EVB-IT Systemvertrages.....	2
2	Art und Umfang der Leistungen zur Erstellung des Gesamtsystems.....	3
3	Mängelklassifizierung	9
4	Systemservice nach Abnahme.....	9
5	Dokumentation und Software Bill of Materials (SBOM)*	12
6	Mitteilungspflichten des Auftragnehmers.....	13
7	Personal des Auftragnehmers, Subunternehmer.....	14
8	Vergütung.....	14
9	Verzug.....	15
10	Projektmanagement.....	15
11	Mitwirkung des Auftraggebers.....	16
12	Abnahme.....	17
13	Rechte des Auftraggebers bei Mängeln des Gesamtsystems (Gewährleistung).....	18
14	Schutzrechte Dritter.....	19
15	Haftungsbeschränkung.....	20
16	Laufzeit und Kündigung	20
17	Änderung der Leistung nach Vertragsschluss.....	21
18	Quellcodeübergabe und Quellcodehinterlegung.....	22
19	Haftplichtversicherung	23
20	Vorauszahlungsbürgschaft, Vertragserfüllungs– und Mängelhaftungssicherheit.....	23
21	Datenschutz, Geheimhaltung und Sicherheit.....	24
22	Zurückbehaltungsrechte.....	25
23	Schlichtungsverfahren	25
24	Textform.....	25
25	Anwendbares Recht.....	25

Ergänzende Vertragsbedingungen für die Erstellung eines Gesamtsystems – EVB-IT System AGB –

1 Gegenstand des EVB-IT Systemvertrages

1.1 Gegenstand des EVB-IT Systemvertrages ist die Erstellung eines Gesamtsystems auf der Grundlage eines Werkvertrages und - soweit vereinbart - Systemservice nach Abnahme und/oder die Weiterentwicklung und Anpassung des Gesamtsystems.

Das Gesamtsystem ergibt sich aus den vom Auftragnehmer zu erbringenden Leistungen und Lieferungen gemäß Nummern 2 und 4 des EVB-IT Systemvertrages einschließlich der vom Auftraggeber beizustellenden Systemkomponenten*. Die Leistungen zur Erstellung des Gesamtsystems können insbesondere umfassen:

- Verkauf von Hardware,
- Vermietung von Hardware,
- Überlassung von Standardsoftware* gegen Einmalvergütung auf Dauer,
- Überlassung von Standardsoftware* auf Zeit,
- Erstellung und Überlassung von Individualsoftware* auf Dauer,
- Erstellung des Gesamtsystems und Herbeiführung der Betriebsbereitschaft*,
- Schulung,
- Dokumentation.

1.2 Die Leistungen zur Erstellung des Gesamtsystems bilden eine sachliche, wirtschaftliche und rechtliche Einheit.

1.3 Die dem Auftraggeber obliegenden Mitwirkungsleistungen ergeben sich aus Nummer 12 des EVB-IT Systemvertrages sowie aus Ziffer 11 dieser Bedingungen.

1.4 Für den Auftraggeber ist von vertragswesentlicher Bedeutung, dass der Auftragnehmer die im EVB-IT Systemvertrag vereinbarte Gesamtfunktionalität herstellt.

1.5 Der Auftragnehmer leitet das Projekt und trägt die Erfolgsverantwortung für die vereinbarten Leistungen. Er haftet für die Leistungen seiner Subunternehmer wie für seine eigenen Leistungen.

1.6 Die im Rahmen des EVB-IT Systemvertrages gelieferte oder erstellte Software* wurde zu einem angemessenen Zeitpunkt vor der Überlassung mit aktueller Scan-Software auf Befehl mit Schaden stiftender Software* überprüft. Der Auftragnehmer erklärt, dass die Überprüfung keinen Hinweis auf Schaden stiftende Software* ergeben hat. Diese Regelung gilt für jede, auch die vorläufige und Vorabüberlassung, z.B. zu Testzwecken.

1.7 Der Auftragnehmer gewährleistet darüber hinaus, dass die von ihm zu liefernde bzw. zu erstellende Software* frei von Funktionen ist, die die Integrität, Vertraulichkeit und Verfügbarkeit der Software*, anderer Soft- und/oder Hardware oder von Daten gefährden und den Vertraulichkeits- oder Sicherheitsinteressen des Auftraggebers zuwiderlaufen durch

- Funktionen zum unerwünschten Absetzen/Ausleiten von Daten,
- Funktionen zur unerwünschten Veränderung/Manipulation von Daten oder der Ablauflogik oder
- Funktionen zum unerwünschten Einleiten von Daten oder unerwünschte Funktionserweiterungen.

Unerwünscht ist eine mögliche Aktivität einer Funktion, wenn die Aktivität so weder vom Auftraggeber in seiner Leistungsbeschreibung gefordert, noch vom Auftragnehmer unter konkreter Beschreibung der



System-AGB

Aktivität und ihrer Funktionsweise angeboten, noch im Einzelfall vom Auftraggeber ausdrücklich autorisiert („opt-in“) wurde.

1.8 Unterliegt die Software* Exportkontrollvorschriften, weist der Auftragnehmer im EVB-IT Systemvertrag darauf hin.

2 Art und Umfang der Leistungen zur Erstellung des Gesamtsystems

Soweit im EVB-IT Systemvertrag nichts anderes vereinbart ist, räumt der Auftragnehmer dem Auftraggeber mit Lieferung bzw. Überlassung die vereinbarten Rechte an den vereinbarten Teil- oder Gesamtleistungen ein, aufschiebend bedingt durch

- die auf die jeweilige Lieferung bzw. Überlassung folgende Abschlags-, Teil-, oder Schluss- zahlung,
- eine Abnahme der betreffenden Teil- oder Gesamtleistung oder
- eine Kündigung des Auftraggebers aus wichtigem Grunde gemäß Ziffer 16.3.

Es gelten hinsichtlich der jeweiligen Leistungsbestandteile folgende Regelungen:

2.1 Verkauf von Hardware

Ist der Verkauf von Hardware vereinbart, liefert der Auftragnehmer die Hardware, stellt sie entsprechend den Vereinbarungen im EVB-IT Systemvertrag auf und verschafft dem Auftraggeber das Eigentum daran.

Der Auftragnehmer übernimmt die Entsorgung der Verpackungen und nach Ende der Nutzung die Entsorgung der von ihm gelieferten Hardware, soweit in Nummern 11.5 oder 11.6 des EVB-IT Systemvertrages nichts anderes vereinbart ist.

2.2 Vermietung von Hardware

Ist die Vermietung von Hardware vereinbart, stellt der Auftragnehmer die Hardware entsprechend den Vereinbarungen im EVB-IT Systemvertrag auf, überlässt sie dem Auftraggeber und hält den vertragsgemäßen Zustand während der Mietzeit aufrecht. Der Auftragnehmer nimmt die Verpackung zurück.

2.3 Überlassung von Software*

Ist die Überlassung von Software* vereinbart, gilt Folgendes:

2.3.1 Dauerhafte Überlassung von Standardsoftware*

2.3.1.1 Der Auftragnehmer verschafft dem Auftraggeber mit Vertragsschluss das Recht, die Standardsoftware* bzw. Softwarekomponenten zu nutzen, das heißt insbesondere dauerhaft oder temporär zu speichern und zu laden, sie anzuzeigen und ablaufen zu lassen. Dies gilt auch, soweit hierfür Vervielfältigungen notwendig werden.

Dieses Recht ist

- nicht ausschließlich,
- mit der Einschränkung gemäß Ziffer 2.1.1.9 übertragbar,
- dauerhaft, unwiderruflich und unkündbar,
- örtlich unbeschränkt und
- in jeder beliebigen Hard- und Softwareumgebung ausübbar
- zu verschaffen.

Das Recht, die Standardsoftware* bzw. Softwarekomponente in jeder beliebigen Hard- und Softwareumgebung zu nutzen, lässt die Einschränkung der Mängelansprüche gemäß Ziffer 12.5 unberührt.

Softwarekomponenten dürfen nur in Verbindung mit der Standardsoftware* genutzt werden, deren Bestandteil sie sind. Diese Beschränkung gilt nicht für Softwarekomponenten, die gemäß Ziffer 2.3.1.2 lizenziert sind.



System-AGB

2.3.1.2 Abweichend von Ziffer 2.3.1.1 gelten die vom Rechteinhaber vorgegebenen Lizenzbedingungen für die Standardsoftware* bzw. Softwarekomponenten, wenn es sich um Open Source Software* handelt.

2.3.1.3 An der Dokumentation der Standardsoftware* verschafft der Auftragnehmer dem Auftraggeber das nicht ausschließliche, dauerhafte, unwiderrufliche, unkündbare und örtlich unbeschränkte Recht, die Dokumentation zu nutzen und zu vervielfältigen. Sofern von den jeweiligen Rechteinhabern an der Dokumentation der Standardsoftware* Rechte eingeräumt werden wie an Open Source Software*, gelten diese anstelle der Rechte gemäß Satz 1 dieser Ziffer 2.3.1.3.

2.3.1.4 Der Auftragnehmer hat sicherzustellen, dass die Lizenz, unter der die Standardsoftware* bzw. Softwarekomponente überlassen wird, keine Bedingungen enthält, die die nach dem Vertrag vorausgesetzte Nutzung und/oder die Verbreitung der Standardsoftware* bzw. Softwarekomponente zusammen mit anderer nach diesem Vertrag überlassener Standardsoftware* oder zusammen mit anderer lizenzierter Software des Auftraggebers verbietet, soweit die gemeinsame Nutzung und/oder Verbreitung der jeweiligen Standardsoftware* oder Softwarekomponente vertraglich vereinbart sind. Eine Haftung des Auftragnehmers aus diesem Vertrag gegenüber Dritten im Zusammenhang mit einer Verbreitung der Standardsoftware* und Softwarekomponente ist ausgeschlossen.

2.3.1.5 Soweit die Anforderungen gemäß Ziffern 2.3.1.1 bis 2.3.1.4 durch die Rechteverschaffung nicht erfüllt werden, ist der Auftragnehmer zu einer ergänzenden Rechteverschaffung, z.B. durch Erwerb und Einräumung zusätzlicher Nutzungsrechte auf eigene Kosten verpflichtet. Ansprüche wegen Mängeln bleiben unberührt.

2.3.1.6 Für Open Source Software* finden die Ziffern 2.3.1.7 bis 2.3.1.12 keine Anwendung.

2.3.1.7 Soweit im Vertrag die Geltung von anderen als den in Ziffer 2.3.1.1 genannten Nutzungsrechtsregelungen vereinbart ist, hat der Auftragnehmer dem Auftraggeber gleichwohl mindestens dauerhafte, unwiderrufliche und unkündbare Nutzungsrechte zu verschaffen, die für die nach dem Vertrag vorausgesetzte Verwendung der Software* notwendig sind. Zudem ist der Auftragnehmer dafür verantwortlich, dass diese weiteren Nutzungsrechtsregelungen den sonstigen vertraglichen Regelungen weder entgegenstehen noch diese beschränken.

2.3.1.8 Dem Auftraggeber obliegt es, durch angemessene technische und organisatorische Maßnahmen für eine bestimmungsgemäße Nutzung der Standardsoftware* bzw. Softwarekomponenten gemäß Ziffer 2.3.1.1 zu sorgen.

2.3.1.9 Macht der Auftraggeber von seinem Recht zur Übertragung des Nutzungsrechts Gebrauch, hat er seine vertraglichen Verpflichtungen bezüglich Inhalt und Umfang der Nutzungsrechte dem Dritten aufzuerlegen. Mit der Übertragung an den Dritten ist der Auftraggeber unbeschadet der Rechte gemäß dem letzten Satz dieser Ziffer nicht mehr zur Nutzung berechtigt. Sofern nach den vertraglichen Bestimmungen das Nutzungsrecht an der Standardsoftware* endet, ist der Auftraggeber verpflichtet, die erstellten Vervielfältigungen zu vernichten bzw. dauerhaft zu löschen. Der Auftraggeber ist jedoch berechtigt, eine Kopie ausschließlich für Prüf- und Archivierungszwecke zu behalten und zu nutzen.

2.3.1.10 Der Auftraggeber ist berechtigt, von der Standardsoftware* bzw. Softwarekomponente eine Kopie zu Sicherungszwecken herzustellen. Die der Softwareverteilung zur bestimmungsgemäßen Nutzung oder der ordnungsgemäßen Datensicherung dienenden Vervielfältigungen der Standardsoftware* bzw. Softwarekomponente sind Teil des bestimmungsgemäßen Gebrauchs.

2.3.1.11 Werden die Nutzungsrechte auf eine im EVB-IT Systemvertrag definierte Hard- und/oder Softwareumgebung beschränkt, bedarf eine hier- von abweichende Nutzung der Zustimmung des Auftragnehmers. Ist eine im EVB-IT Systemvertrag definierte Hard- und/oder Softwareumgebung nicht funktionsfähig, ist die Nutzung bis zu deren Wiederherstellung in einer anderen Umgebung auch ohne Zustimmung des Auftragnehmers zulässig.

2.3.1.12 Der Auftraggeber verpflichtet sich, die Standardsoftware* nicht in eine andere Codeform zu bringen oder Veränderungen am Code vorzunehmen, es sei denn, dass dies nach den gesetzlichen Vorschriften zulässig ist.

2.3.1.13 Erkennt der Auftragnehmer, dass der Auftraggeber etwaig vereinbarten Obliegenheiten oder Pflichten aus Nutzungsrechtsregelungen nicht ausreichend nachkommt oder die Grenzen der vereinbarten Nutzungsrechte überschreitet bzw. zu überschreiten droht, hat er dies und die ihm erkennbaren Folgen dem Auftraggeber unverzüglich in Textform mitzuteilen.

2.3.2 Überlassung von Standardsoftware* auf Zeit

Ist die Überlassung von Standardsoftware* auf Zeit vereinbart, überlässt der Auftragnehmer die Standardsoftware* dem Auftraggeber und hält den vertragsgemäßen Zustand während der vereinbarten Überlassungszeit aufrecht. Soweit im EVB-IT Systemvertrag keine andere bestimmungsgemäße Nutzung vereinbart ist, räumt der Auftragnehmer dem Auftraggeber mit Beginn der vereinbarten Überlassungszeit

- das nicht ausschließliche,
- zeitlich auf die vereinbarte Nutzungszeit beschränkte, nach der vertraglichen Vereinbarung ordentlich und im Übrigen nur außerordentlich kündbare,
- örtlich unbeschränkte,
- in jeder beliebigen Hard- und Softwareumgebung ausübbar,
- nicht übertragbar

Recht ein, die Standardsoftware* zu nutzen, das heißt insbesondere, sie für die vereinbarte Nutzungszeit oder temporär zu speichern und zu laden, sie anzuzeigen und ablaufen zu lassen. Dies gilt auch, soweit hierfür Vervielfältigungen notwendig werden.

2.3.3 Standardsoftware mit Anpassungen auf Quellcodeebene

Werden Anpassungen an der Standardsoftware* auf Quellcodeebene vorgenommen, hat der Auftragnehmer spätestens mit der Angebotsabgabe mitzuteilen, ob er die Anpassungen in den Standard aufnehmen werde. Erklärt er dies, ist er verpflichtet, die Anpassungen in den auf die Erklärung der Betriebsbereitschaft* folgenden Programmstand* der Standardsoftware* aufzunehmen. Erfolgt keine entsprechende Erklärung oder ist keine Aufnahme der Anpassungen in den Standard erfolgt, ist der Auftragnehmer verpflichtet, die Anpassungen auf Quellcodeebene im Quellcode* und die unangepassten Teile der Standardsoftware* im Objektcode* so zu übergeben, dass der Auftraggeber in der Lage ist, mit entsprechend qualifiziertem Personal hieraus wieder die angepasste Standardsoftware* zu erstellen. An dem zu übergebenden Quellcode* erhält der Auftraggeber die Rechte für Individualsoftware*.

2.3.4 Erstellung und Überlassung von Individualsoftware* bzw. Individualsoftwarekomponenten

Ist die Erstellung und Überlassung von Individualsoftware* bzw. Individualsoftwarekomponenten vereinbart, erstellt der Auftragnehmer diese entsprechend den Vereinbarungen, insbesondere in den Nummern 2 und 4 des EVB-IT Systemvertrages und stellt sie zur Verfügung.

2.3.4.1 Rechteinhalt Individualsoftware*

Soweit im Vertrag nichts anderes vereinbart ist, stellt der Auftragnehmer die Individualsoftware* bzw. die Individualsoftwarekomponente als Open Source Software* zur Verfügung. Soweit vereinbart, umfasst dies auch, dass die Bereitstellung durch den Auftragnehmer zusätzlich auf openCode* entsprechend deren Bedingungen erfolgt.

Zusätzlich zur vorgenannten Lizenzierung verschafft der Auftragnehmer dem Auftraggeber jeweils, soweit die Individualsoftware bzw. die Individualsoftwarekomponente entstanden ist, das Recht, die Individualsoftware* bzw. Individualsoftwarekomponente im Original oder in abgeänderter, übersetzter, bearbeiteter oder umgestalteter Form

- zu nutzen, das heißt insbesondere, sie dauerhaft oder temporär zu speichern und zu laden, sie anzuzeigen und ablaufen zu lassen, auch soweit hierfür Vervielfältigungen notwendig werden,
- abzuändern, zu übersetzen, zu bearbeiten oder auf anderem Wege umzugestalten,
- auf einem beliebigen bekannten Medium oder in anderer Weise zu speichern, zu vervielfältigen, auszustellen, zu veröffentlichen, in körperlicher oder unkörperlicher Form zu verbreiten, insbesondere nichtöffentlich und mit Ausnahme des Quellcodes* öffentlich wiederzugeben, auch durch Bild-, Ton- und sonstige Informationsträger, jeweils
- in Datenbanken, Datennetzen und Online-Diensten einzusetzen, einschließlich des Rechts, die Individualsoftware*, nicht jedoch den Quellcode*, den Nutzern der vorgenannten Datenbanken, Netze und Online-Dienste zur Recherche und zum Abruf mittels vom Auftraggeber gewählter Tools bzw. zum nicht gewerblichen Herunterladen zur Verfügung zu stellen,



System-AGB

- durch Dritte nutzen und bearbeiten oder für den Auftraggeber betreiben zu lassen,
- nicht nur für eigene Zwecke zu nutzen, sondern auch zur Erbringung von Leistungen an Dritte einzusetzen,
- in körperlicher oder unkörperlicher Form zu verbreiten, jedoch gewerblich nur an wie in §§ 99 bis 101 GWB definierte Auftraggeber.

Das Recht ist

- nicht ausschließlich,
- dauerhaft, unwiderruflich und unkündbar
- örtlich unbeschränkt
- für nichtgewerbliche Zwecke unterlizenzierbar
- für gewerbliche Zwecke an wie in §§ 99 bis 101 GWB definierte Auftraggeber unterlizenzierbar,
- in jeder beliebigen Hard- und Softwareumgebung ausübbar,
- übertragbar,

zu verschaffen.

Das Nutzungsrecht bezieht sich auf die Individualsoftware*, insbesondere deren Objekt- und Quellcode* in allen Entwicklungs-, Zwischen- und Endstufen und auf die zugehörigen Dokumentationen sowie auf sonstige für die Ausübung der Nutzungsrechte notwendige Materialien, wie beispielsweise Analysen, Lasten- bzw. Pflichtenhefte, Konzepte und Beschreibungen.

Soweit die Individualsoftware bzw. Individualsoftwarekomponente nicht als Open Source Software* bereitgestellt wird, gilt folgendes:

- Macht der Auftraggeber von seinem Recht zur Übertragung des Nutzungsrechts an der Individualsoftware* ganz oder teilweise Gebrauch oder überlässt er Dritten im Rahmen seines Vervielfältigungs-, Unterlizenzierungs- oder Verbreitungsrechts die Nutzung, hat er seine vertraglichen Verpflichtungen bezüglich Inhalt und Umfang der Nutzungsrechte dem Dritten aufzuerlegen. Eine Haftung des Auftragnehmers aus diesem Vertrag gegenüber Dritten im Zusammenhang mit einer Unterlizenzierung oder Weiterverbreitung ist ausgeschlossen. Dies gilt auch für Mängelansprüche und auch, soweit der Auftraggeber Ansprüche gegen den Auftragnehmer geltend macht, die der Dritte seinerseits wegen der Individualsoftware* gegen den Auftraggeber geltend gemacht hat.
- Soweit der Auftraggeber seine Nutzungsrechte an den Dritten übertragen hat, ist er nicht mehr zur Nutzung berechtigt. Der Auftraggeber ist jedoch berechtigt, eine Kopie ausschließlich für Prüf- und Archivierungszwecke zu behalten und zu nutzen.

2.3.4.2 Rechte an vorbestehenden Teilen*, Mitteilungspflichten des Auftragnehmers

Ziffer 2.3.4.1 gilt grundsätzlich auch für vorbestehende Teile*, jedoch werden keinesfalls ausschließliche Nutzungsrechte an diesen eingeräumt.

Ist die Individualsoftware* bzw. die Individualsoftwarekomponente gemäß Ziffer 2.3.4.1 als Open Source Software* bereitzustellen, müssen auch sämtliche vorbestehenden Teile* derselben als Open Source Software* bereitgestellt werden, soweit der Auftraggeber nicht im Einzelfall ausnahmsweise ausdrücklich etwas anderes in Textform zulässt.

Für Open Source Software* gelten die nachfolgenden Regelungen dieser Ziffer 2.3.4.2 nicht.

Soweit vorbestehende Teile* der Individualsoftware bzw. Individualsoftwarekomponente nicht als Open Source Software* bereitgestellt werden, gilt folgendes:

- Die Verbreitung und Unterlizenzierung von vorbestehenden Teilen* ist zu vergüten, wenn der Auftragnehmer deren Verwendung im Angebot mitgeteilt, die Vergütung für die Einräumung dieser Rechte dort beziffert und der Auftraggeber auf dieses Angebot so auch den Zuschlag erteilt hat. Solange der Auftraggeber diese Rechte an den vorbestehenden Teilen* nicht ausübt, wird die Vergütung für deren Verbreitung oder Unterlizenzierung nicht fällig.



System-AGB

- Das Recht zur Bearbeitung der vorbestehenden Teile* ist ausgeschlossen, wenn die folgenden Voraussetzungen erfüllt sind:
 - o Der Auftragnehmer hat im bezuschlagten Angebot mitgeteilt, dass er statt des Quellcodes* der vorbestehenden Teile* nur deren Objektcode* überlassen werde und macht von diesem Recht Gebrauch.
 - o Der Auftragnehmer versetzt den Auftraggeber in die Lage, mit entsprechend qualifiziertem Personal aus den im Quellcode* überlassenen Teilen der Individualsoftware* und den nur im Objektcode* überlassenen vorbestehenden Teilen* die ausführbare Individualsoftware* zu erzeugen.
 - o Es besteht kein gesetzliches Bearbeitungsrecht.

Für den Einsatz von Werkzeugen* gilt Ziffer 2.3.4.4.

Die Verbreitung und Unterlizenzierung der vorbestehenden Teile* ist nur zusammen mit der Individualsoftware* in der überlassenen oder in abgeänderter, übersetzter, bearbeiteter oder umgestalteter Form zulässig.

2.3.4.3 Rückvergütung

Ist in Nummer 4.5.4 des EVB-IT Systemvertrages eine Rückvergütung an den Auftraggeber für die Einräumung von Rechten an der Individualsoftware* oder von Teilen der Individualsoftware* an Dritte vereinbart, gilt folgende Berichtspflicht- und Buchüberprüfungsvereinbarung:

- Der Auftragnehmer verpflichtet sich, dem Auftraggeber binnen eines Monats nach dessen Aufforderung in Textform eine aktuelle Übersicht über erfolgte bzw. vereinbarte Nutzungsrechtseinräumungen zu übermitteln (Abrechnung). Der Auftragnehmer ist vorbehaltlich einer anderen Vereinbarung zu maximal zwei Abrechnungen pro Vertragsjahr verpflichtet.
- Der Auftragnehmer ist verpflichtet, einem vom Auftraggeber beauftragten, zur Berufsverschwiegenheit verpflichteten Dritten einmal im Jahr zur Überprüfung der Abrechnungen zu den Bürozeiten des Auftragnehmers Einsicht in die für die Rückvergütung relevanten Unterlagen zu gewähren. Der Auftraggeber wird seinen Wunsch mit einer Frist von mindestens fünf Tagen in Textform ankündigen.

2.3.4.4 Rechte an Werkzeugen*

Für den Fall, dass der Auftragnehmer nicht am Markt erhältliche Werkzeuge* für die Erstellung der Individualsoftware* verwendet bzw. entwickelt hat und ohne diese Werkzeuge* die Bearbeitung und Umgestaltung der Individualsoftware* nicht oder nur mit unzumutbarem Aufwand möglich ist, übergibt er dem Auftraggeber ein Vervielfältigungsstück dieses Werkzeuges* spätestens bis zur Erklärung der Betriebsbereitschaft* und räumt ihm an diesem

- das nicht ausschließliche,
- örtlich unbeschränkte,
- in jeder beliebigen Hard- und Softwareumgebung ausübbarer,
- nur gemeinsam mit der Individualsoftware*, zu deren Bearbeitung bzw. Umgestaltung es dient, übertragbarer,
- dauerhafter, unwiderruflicher und unkündbarer
- Recht ein, das Werkzeug* im Original ausschließlich zum Zwecke der Fehlerbeseitigung und Weiterentwicklung zur Bearbeitung und Umgestaltung der Individualsoftware* einzusetzen und hierfür das Werkzeug*
- zu nutzen, das heißt insbesondere, es dauerhaft oder temporär zu speichern und zu laden, es anzuzeigen und ablaufen zu lassen, auch soweit hierfür Vervielfältigungen notwendig werden,
- durch Dritte nutzen oder für den Auftraggeber betreiben zu lassen,
- nicht nur für eigene Zwecke zu nutzen, sondern auch zur Erbringung von Leistungen an Dritte einzusetzen.

System-AGB

Der Auftraggeber ist darüber hinaus berechtigt, ein weiteres Vervielfältigungsstück herzustellen und dieses gemeinsam mit der jeweiligen Individualsoftware* zu verbreiten und dem Dritten die Rechte aus dieser Ziffer 2.3.4.4 mit Ausnahme des Unterlizenzierungs-, Verbreitungs- und Vervielfältigungsrechts einzuräumen. Statt des vom Auftragnehmer verwendeten Werkzeuges* kann dieser dem Auftraggeber eine reduzierte Version dieses Werkzeuges* übergeben und ihm die in dieser Ziffer 2.3.4.4 aufgeführten Rechte daran einräumen, wenn damit die Individualsoftware* ebenso gut bearbeitet und umgestaltet werden kann.

Der Auftragnehmer ist nicht zur Überlassung des Werkzeuges* verpflichtet, wenn er nachweisen kann, dass die Individualsoftware* mit einem am Markt erhältlichen anderen Werkzeug* ebenso gut bearbeitet und umgestaltet werden kann, wie mit dem von ihm verwendeten Werkzeug* und er dem Auftraggeber die Bezugsquelle nennt.

Die Regelungen in dieser Ziffer 2.3.4.4 gelten grundsätzlich auch in Bezug auf Werkzeuge, bei denen es sich um Open Source Software* handelt. Allerdings gelten in Bezug auf diese Werkzeuge die von den jeweiligen Rechteinhabern vorgegebenen Lizenzbedingungen und der Auftragnehmer hat dem Auftraggeber das Werkzeug unter Erfüllung der Pflichten, die für Open Source Software* gelten, zu übergeben. Der Auftragnehmer ist in diesem Fall insbesondere verpflichtet, dem Auftraggeber die Bezugsquelle zu nennen.

2.3.4.5 Rechte an Erfindungen

Soweit im EVB-IT Systemvertrag nichts anderes vereinbart ist, gilt für Erfindungen, die anlässlich der Vertragserfüllung gemacht werden, folgende Regelung:

- Der Auftragnehmer kann über die Erfindung und die daraus fließenden und damit in Zusammenhang stehenden Rechte frei verfügen und die Erfindung als Patent oder Gebrauchsmuster anmelden. Der Auftragnehmer räumt dem Auftraggeber bereits hiermit unentgeltlich ein einfaches, nicht ausschließliches, übertragbares, unterlizenzierbares und dinglich wirkendes Nutzungsrecht an jetzt und in Zukunft angemeldeten oder erteilten Patenten und Gebrauchsmustern in Verbindung mit der Nutzung der von der Erfindung betroffenen Systemkomponenten* ein. Soweit dies im Einzelfall nicht ausreichend ist, räumt der Auftragnehmer Nutzungsrechte in dem Umfang ein, der erforderlich ist, damit der Auftraggeber oder ein berechtigter Dritter die Rechte an der Systemkomponente* vertragsgemäß ausüben kann.
- Der Auftragnehmer hat auf seine Kosten sicherzustellen, dass die Ausübung der dem Auftraggeber zustehenden Nutzungsrechte an der Systemkomponente* weder durch ihn noch durch den Erfinder oder einen etwaigen Rechtsnachfolger beeinträchtigt werden kann. Insbesondere wird er zu diesem Zwecke etwaige Dienstserfindungen in Anspruch nehmen.

2.3.5 Multilizenzierung

Wenn der Auftragnehmer für die Erstellung von Individualsoftware* oder die Anpassung oder das Customizing* von Standardsoftware* vorbestehende Softwarekomponenten von Open Source Software* verwendet oder bearbeitet, die ihm unter mehreren Open Source Lizenzen zur Verfügung stehen, so muss der Auftragnehmer die Bearbeitungen dieser Softwarekomponenten unter all diesen Open Source Lizenzen lizenzieren und an den Auftraggeber weitergeben. Unabhängig davon kann der Auftragnehmer sich entscheiden, unter welcher dieser Lizenzen er die Softwarekomponenten in der Individualsoftware* bzw. Standardsoftware* verwendet.

2.4 Erstellung des Gesamtsystems und Herbeiführung der Betriebsbereitschaft*

Der Auftragnehmer ist verpflichtet, das Gesamtsystem entsprechend den vertraglichen Vereinbarungen zu erstellen und dessen Betriebsbereitschaft* herbeizuführen.

Dazu hat der Auftragnehmer die einzelnen von ihm zu liefernden oder zu erstellenden Systemkomponenten* sowie die durch den Auftraggeber beizustellenden Systemkomponenten* aufzustellen, zu installieren*, zu customizen* und zu integrieren*. Dies erfolgt jeweils nach Maßgabe der Leistungsbeschreibung bzw., sofern sich daraus nichts ergibt, soweit zur Herbeiführung der Betriebsbereitschaft* des Gesamtsystems erforderlich.

Der Auftragnehmer räumt dem Auftraggeber an den anlässlich der vorgenannten Tätigkeiten für den Auftraggeber insoweit erstellten Arbeitsergebnissen, insbesondere an den Ergebnissen der Installation*,



System-AGB

des Customizing* und der Integration* sowie an den Protokollen und sonstigen damit im Zusammenhang stehenden Materialien, Datenbankwerken und Datenbanken die Rechte gemäß Ziffern 2.3.3.1 und 2.3.3.4 ein. Soweit vorbestehende Materialien wie z.B. Vorlagen, Konzepte und Dokumentationen urheberrechtlich geschützt sind, erhält der Auftraggeber jedoch kein Bearbeitungsrecht sowie kein Recht zur Unterlizenzierung, es sei denn, dass einer dieser Ausschlüsse nach den gesetzlichen Vorschriften unzulässig ist. Sofern von den jeweiligen Rechteinhabern an vorbestehenden Materialien Rechte eingeräumt werden wie an Open Source Software*, gelten diese anstelle der Rechte gemäß Sätzen 1 und 2 dieser Ziffer 2.4.

2.5 Schulungen

Sind Schulungen vereinbart, führt der Auftragnehmer diese in eigener Verantwortung und insbesondere entsprechend den Vereinbarungen in Nummern 2 und 4 des EVB-IT Systemvertrages durch. Ist nichts anderes vereinbart, sind alle Schulungen in deutscher Sprache durchzuführen. Schulungen finden beim Auftraggeber statt, soweit nichts anderes vereinbart ist. Soweit Schulungen nicht beim Auftraggeber stattfinden, ist der Auftragnehmer für die Bereitstellung der Räumlichkeiten und der entsprechenden Schulungsinfrastruktur verantwortlich. Ein Schultag umfasst acht Unterrichtsstunden à 45 Minuten sowie angemessene Pausen. Die Schulungsvergütung beinhaltet die angemessene Vorbereitung der Schulung sowie die Einräumung der vereinbarten Nutzungsrechte an den Schulungsunterlagen. Die Schulungsunterlagen sind in deutscher Sprache geschuldet. Die vereinbarten Vervielfältigungsstücke gehen in das Eigentum des Auftraggebers über. Zu den Schulungsunterlagen gehören die elektronischen Präsentationsdateien.

An nicht für den Auftraggeber erstellten Schulungsunterlagen räumt der Auftragnehmer dem Auftraggeber das nicht ausschließliche, unwiderrufliche, dauerhafte und übertragbare Recht ein, die Schulungsunterlagen für eigene Zwecke des Rechteinhabers zu nutzen, soweit nichts anderes vereinbart ist.

Soweit Schulungsunterlagen oder Teile davon für den Auftraggeber erstellt wurden, räumt der Auftragnehmer diesem für Schulungen und im Übrigen allein für eigene Zwecke des Rechteinhabers die Rechte entsprechend Ziffer 2.3.4.1 in Verbindung mit Nummer 4.5.3 EVB-IT Systemvertrag ein, soweit nichts anderes vereinbart ist.

3 Mängelklassifizierung

3.1 Soweit im EVB-IT Systemvertrag, insbesondere in dessen Nummern 5.1.1.2, 13.5 oder 14.4.1 nicht anders vereinbart, wird zwischen folgenden drei Mängelklassen unterschieden:

3.1.1 Ein betriebsverhindernder Mangel liegt vor, wenn die Nutzung des Gesamtsystems unmöglich oder schwerwiegend eingeschränkt ist.

3.1.2 Ein betriebsbehindernder Mangel liegt vor, wenn die Nutzung des Gesamtsystems erheblich eingeschränkt ist.

3.1.3 Ein leichter Mangel liegt vor, wenn die Nutzung des Gesamtsystems ohne oder mit unwesentlichen Einschränkungen möglich ist.

3.2 Ein betriebsbehindernder Mangel liegt auch vor, wenn die leichten Mängel insgesamt zu einer nicht unerheblichen Einschränkung der Nutzung des Gesamtsystems führen.

4 Systemservice nach Abnahme

Sind Systemserviceleistungen vereinbart, erbringt der Auftragnehmer diese nach Maßgabe der Vereinbarungen im EVB-IT Systemvertrag sowie der folgenden Regelungen:

4.1 Wiederherstellung der Betriebsbereitschaft*

Ist die Wiederherstellung der Betriebsbereitschaft* des Gesamtsystems oder von Systemkomponenten* vereinbart, gehören hierzu alle für die Störungsbeseitigung notwendigen Maßnahmen des Auftragnehmers. Dies umfasst z.B. Instandsetzungsleistungen für Hardware und Pflegeleistungen für Software* zur Beseitigung von Störungen. Letztere beinhalten z.B. die Erstellung und Überlassung einer fehlerbereinigten Fassung der Individualsoftware* und die Überlassung eines für die Störungsbeseitigung notwendigen Programmstandes* für die Standardsoftware*; Ziffer 4.2.2.2 gilt entsprechend.

System-AGB

Liegt eine Störung in der Standardsoftware* vor und ist die Störungsbeseitigung für Standardsoftware* vereinbart, gilt Folgendes:

- Der Auftragnehmer ist während der Vertragslaufzeit verpflichtet, einen verfügbaren, die Störung beseitigenden Programmstand* bereitzustellen.
- Ist ein die Störung beseitigender Programmstand* nicht verfügbar, hat der Auftragnehmer eine Umkehrungslösung zur Verfügung zu stellen.
- Ist dies unzumutbar, hat er sich beim Hersteller der Standardsoftware* für die baldmögliche Überlassung eines die Störung beseitigenden Programmstandes* einzusetzen. Auf Verlangen des Auftraggebers wird der Auftragnehmer hierüber Auskunft erteilen.

Im Rahmen der Pflicht zur Bereitstellung einer Umkehrungslösung* kann der Auftraggeber in der Regel keinen Eingriff in den Objekt-* oder Quellcode* der Standardsoftware* verlangen.

4.1.1 Soweit nichts anderes vereinbart ist, ist eine neue Systemkomponente* vom Auftraggeber zu übernehmen, wenn sie der Beseitigung von Störungen dient. Zur Übernahme einer neuen Systemkomponente* ist der Auftraggeber nicht verpflichtet, wenn ihm dies nicht zuzumuten ist, weil die neue Systemkomponente* wesentlich von der vereinbarten Ausführung abweicht.

Übernimmt der Auftraggeber eine neue Systemkomponente* aus diesem Grunde nicht, wird der Auftragnehmer auf Wunsch des Auftraggebers eine andere Lösung vorschlagen, sofern eine solche möglich und zumutbar ist.

Übernimmt der Auftraggeber eine neue Systemkomponente*, gilt Folgendes:

- Enthält die neue Systemkomponente* mehr Funktionalität als die im EVB-IT Systemvertrag aufgeführte Systemkomponente* (Mehrleistung), ist der Auftraggeber zur Zahlung einer Mehrvergütung nur verpflichtet, wenn er diese Mehrleistung nutzen will. Dazu zählt auch der Fall, dass er die Mehrleistung nutzt, obwohl er die neue Systemkomponente* auch ohne die Mehrleistung vertragsgemäß nutzen könnte, nicht jedoch der Fall, dass er die bisherige Funktionalität nur zusammen mit der Mehrleistung nutzen kann. Eine Mehrvergütung entfällt, soweit die Überlassung der neuen Systemkomponente* bereits Gegenstand der Leistungsverpflichtung gemäß Ziffer 4.2 ist.
- Entstehen ihm durch die Nutzung der neuen Systemkomponente* höhere Kosten als zuvor, gehen diese zu Lasten des Auftragnehmers. Dies gilt nicht, soweit diese höheren Kosten darauf zurückzuführen sind, dass der Auftraggeber vorhandene Mehrleistungen nutzen will. Satz 2 des ersten Aufzählungspunktes dieser Ziffer 4.1.1 gilt entsprechend.

4.1.2 Sind keine Servicezeiten vereinbart, gelten die Zeiträume von Montag bis Freitag von 8:00 Uhr bis 17:00 Uhr (mit Ausnahme der gesetzlichen Feiertage am Erfüllungsort) als Servicezeiten. Sind keine Reaktionszeiten* vereinbart, ist mit den Arbeiten zur Wiederherstellung der Betriebsbereitschaft* des Gesamtsystems unverzüglich nach Zugang der Störungsmeldung innerhalb der Servicezeiten zu beginnen. Sind keine Wiederherstellungszeiten* vereinbart, sind die Arbeiten zur Wiederherstellung der Betriebsbereitschaft* des Gesamtsystems in angemessener Frist innerhalb der Servicezeiten abzuschließen. Hält der Auftragnehmer vereinbarte Reaktions- und/oder Wiederherstellungszeiten* nicht ein, gerät er nach deren Überschreitung auch ohne Mahnung in Verzug, es sei denn, dass er die Fristüberschreitung nicht zu vertreten hat.

Im Falle des Verzuges kann der Auftraggeber den Ausgleich des Verzögerungsschadens verlangen. Darüber hinaus kann er die Vereinbarung zum Systemservice gemäß Nummer 5 des EVB-IT Systemvertrages und – falls vereinbart – die Vereinbarung zur Weiterentwicklung und Anpassung des Gesamtsystems gemäß Nummer 6 des EVB-IT Systemvertrages kündigen und/oder Schadensersatz statt der Leistung verlangen, wenn er dem Auftragnehmer erfolglos eine angemessene Frist zur Leistung gesetzt hat. Tritt die gleiche Störung nach Erklärung der Betriebsbereitschaft* wieder auf und beruht die Störung auf der gleichen Ursache, gilt sie als nicht beseitigt. Hat der Auftraggeber die Störung vorsätzlich oder grob fahrlässig verursacht und ist eine Pauschalvergütung für den Systemservice vereinbart, kann der Auftragnehmer vom Auftraggeber eine angemessene Vergütung für die Störungsbeseitigung verlangen.

4.2 Aufrechterhaltung der Betriebsbereitschaft*



System-AGB

Ist die Aufrechterhaltung der Betriebsbereitschaft* des Gesamtsystems vereinbart, können hierzu je nach Vereinbarung die Wartung des Gesamtsystems oder von Systemkomponenten* und/oder die Überlassung von neuen Programmständen* der Standardsoftware* des Gesamtsystems gehören.

4.2.1 Wartung des Gesamtsystems

Ist die Wartung des Gesamtsystems (Systemwartung) vereinbart, sollen im vertraglich vereinbarten Umfang die Funktionsfähigkeit des Gesamtsystems oder von Systemkomponenten* gewährleistet und insbesondere vorausschauend Störungen vermieden werden.

4.2.2 Überlassung von neuen Programmständen*

4.2.2.1 Ist der Auftragnehmer zur Überlassung neuer Programmstände* verpflichtet, hat der Auftragnehmer diese zu installieren*, zu customizen* und in das Gesamtsystem zu integrieren*, soweit nichts anderes vereinbart ist. Für den Fall, dass Standardsoftware* für den Auftraggeber gemäß Ziffer 2.3.3 angepasst wurde, gehört dazu auch, diese Anpassungen in dem neuen Programmstand* für den Auftraggeber vorzunehmen. Enthalten neue Programmstände* wesentliche neue Funktionalitäten, sind das Customizing* und die Integration* in Bezug auf diese Funktionalitäten nur insoweit geschuldet, als dies zur Herstellung der Betriebsbereitschaft* erforderlich ist. Der Auftragnehmer ist jedoch verpflichtet, auf Wunsch des Auftraggebers das Customizing* und die Integration* in Bezug auf diese Funktionalitäten auch weitergehend vorzunehmen. Für diesen Fall gilt Ziffer 17. Im Übrigen darf eine Nutzung neuer Funktionalitäten durch das Customizing* nicht behindert werden. Die Verpflichtung zur Überlassung von Programmständen* umfasst auch die Verpflichtung zur Einräumung von Nutzungsrechten in Art und Umfang, wie sie für die zu pflegende Standardsoftware* bestehen.

4.2.2.2 Der Auftragnehmer gewährleistet, dass durch die Überlassung neuer Programmstände* keine Einschränkungen technischer, organisatorischer oder rechtlicher Art entstehen und die Nutzungsrechte auch an keine anderen Auflagen, Bedingungen oder Voraussetzungen geknüpft werden, als sie für die vorherige Fassung der Standardsoftware* bzw. den vorherigen Programmstand* bestanden.

Wenn ein neuer Programmstand eine Programmbibliothek* verlinkt, deren Lizenz (wie z.B. LGPL 2.1 oder 3.0) die Verpflichtung vorsieht, bei der Verbreitung, Vermietung, öffentlichen Wiedergabe und öffentlichen Zugänglichmachung der verlinkten Softwarekomponenten die Bearbeitung der Programmbibliothek* zu bestimmten Zwecken sowie das Reverse Engineering* der verlinkten Standardsoftware* zu bestimmten Zwecken zu erlauben, so verschafft der Auftragnehmer dem Auftraggeber die insoweit erforderlichen Nutzungsrechte.

Kann der Auftragnehmer mit dem neuen Programmstand* nicht die Verpflichtung aus dieser Ziffer erfüllen, z.B. weil der Ersteller der Standardsoftware* diese nur zu geänderten Nutzungsbedingungen anbietet, ist er verpflichtet, dem Auftraggeber vor der Überlassung die Lizenzbedingungen zu übergeben, die Nutzungsrechtseinschränkungen gegenüber dem vorherigen Programmstand* im Detail aufzuzeigen und etwaige Auflagen, Bedingungen bzw. Nutzungsvoraussetzungen zu erläutern.

Des Weiteren hat der Auftragnehmer die Konsequenzen für den praktischen Einsatz beim Auftraggeber zu erläutern, soweit wie der Auftragnehmer Kenntnis über die Systemumgebung des Auftraggebers erhält, in der die Standardsoftware* eingesetzt wird. Dies gilt entsprechend, wenn der neue Programmstand* gegenüber dem vorherigen Programmstand* Funktionseinschränkungen aufweist. Soweit technisch möglich und dem Auftragnehmer zumutbar, wird dieser dem Auftraggeber eine Ersatzlösung vorschlagen und vor weiteren diesbezüglichen Maßnahmen dessen Entscheidung abwarten. Weitere Ansprüche und Rechte des Auftraggebers bleiben unberührt.

Der Auftragnehmer ist verpflichtet, die Lizenzbedingungen bei der Leistungserbringung nach diesem Vertrag einzuhalten. Waren für die Standardsoftware* bestimmte Dokumente bzw. Informationen (z.B. Quellcode, NOTICE-Dateien, SBOM) aufgrund der Lizenzbedingungen oder aufgrund einer Vereinbarung mit dem Auftragnehmer zur Verfügung zu stellen, sind diese bei Bereitstellung eines neuen Programmstandes* dem Auftraggeber in entsprechend aktualisierter Fassung zur Verfügung zu stellen, damit der Auftraggeber die Lizenzbedingungen beim bestimmungsgemäßen Gebrauch ebenfalls einhalten kann.

4.3 Abnahme der Systemserviceleistungen

Nach Durchführung der Systemserviceleistungen erklärt der Auftragnehmer die Betriebsbereitschaft* des Gesamtsystems oder der vereinbarten Systemkomponente*. Systemserviceleistungen des



System-AGB

Auftragnehmers, die zu nicht unwesentlichen Eingriffen in das Gesamtsystem führen unterliegen der Abnahme. Bei unwesentlichen Eingriffen ist statt einer Abnahme die Erklärung der Betriebsbereitschaft* ausreichend. In diesem Fall steht die Erklärung der Abnahme gleich. Soweit Eingriffe einer Abnahme unterliegen, steht dem Auftraggeber das Recht zu, das Gesamtsystem oder die vereinbarte Systemkomponente* innerhalb einer angemessenen Frist nach Zugang der Betriebsbereitschaftserklärung einer Funktionsprüfung zu unterziehen. Für die Einhaltung der vereinbarten Wiederherstellungszeit* genügt bei erfolgreicher Beseitigung einer Störung der Zeitpunkt der Erklärung der Betriebsbereitschaft* für die Fristwahrung.

4.4 Mängelhaftung bei Systemserviceleistungen

Sind die Systemserviceleistungen mangelhaft erbracht, gilt Ziffer 13 entsprechend. An Stelle des Rücktritts nach Ziffer 13.11 tritt das Recht auf Kündigung der Systemservicevereinbarung gemäß Nummer 5 des EVB-IT Systemvertrages in Bezug auf die betroffene Leistung, es sei denn, dem Auftraggeber ist das Festhalten an der Systemservicevereinbarung insgesamt nicht zumutbar. In diesem Fall ist der Auftraggeber zur Kündigung der Systemservicevereinbarung insgesamt berechtigt.

4.5 Dokumentation der Systemserviceleistungen

Der Auftragnehmer dokumentiert die durchgeführten Systemserviceleistungen in angemessener Art und Weise, soweit nichts anderes vereinbart ist.

Der Auftragnehmer wird alle Anpassungen und Änderungen, die aufgrund von Maßnahmen zum Systemservice gemäß Ziffer 4 an den Dokumentationen erforderlich werden, in die Dokumentationen einarbeiten, soweit nichts anderes vereinbart ist. Soweit eine Einarbeitung dem Auftragnehmer rechtlich nicht möglich ist, wird er eine entsprechende Ergänzung der Dokumentation zur Verfügung stellen.

5 Dokumentation und Software Bill of Materials (SBOM)*

5.1 Der Auftragnehmer ist zur Dokumentation des Gesamtsystems verpflichtet.

5.2 Zu der Dokumentation des Gesamtsystems gehören insbesondere die Anwendungsdokumentation (Nutzerhinweise, Anleitungen und Hilfestellungen etc.) sowie Nutzungshandbücher für Hard- und Software* und Verfahrensbeschreibungen.

Die Dokumentation muss es dem für die Nutzung und Administration einzusetzenden Personal des Auftraggebers ermöglichen, das Gesamtsystem nach Durchführung der vereinbarten Schulung ordnungsgemäß zu bedienen, sofern das Personal ausreichende Vorbildung und Ausbildung aufweist.

Die Dokumentation muss darüber hinaus den technischen Aufbau und die technischen Abläufe des Gesamtsystems so umfassend beschreiben, dass es dem Auftraggeber bei Einsatz von Personal mit ausreichender Vorbildung und Ausbildung möglich ist, die Unterlagen auch ohne Inanspruchnahme des Auftragnehmers zu verwenden, insbesondere um das Gesamtsystem selbstständig einsetzen und, soweit die Gewährung entsprechender Rechte vereinbart ist, auch fortentwickeln zu können.

5.3 Soweit nichts anderes vereinbart ist, ist die Dokumentation spätestens mit Erklärung der Betriebsbereitschaft* in deutscher Sprache mindestens in zweifacher Ausfertigung oder in ausdrückbarer Form zu übergeben. Die Nutzung der gängigen englischen Fachbegriffe ist zulässig.

5.4 Der Auftragnehmer dokumentiert die im Rahmen der Mängelhaftung gemäß Ziffer 13 durchgeführten Maßnahmen, soweit nichts anderes vereinbart ist.

5.5 Der Auftragnehmer wird alle Anpassungen und Änderungen, die aufgrund von Maßnahmen im Rahmen der Mängelhaftung gemäß Ziffer 13 an den Dokumentationen erforderlich werden, in diese einarbeiten, soweit nichts anderes vereinbart ist. Soweit eine Einarbeitung dem Auftragnehmer rechtlich nicht möglich ist, wird er eine entsprechende Ergänzung der Dokumentation zur Verfügung stellen.

5.6 An für den Auftraggeber erstellten Dokumentationen räumt der Auftragnehmer diesem die Rechte entsprechend Ziffer 2.3.4.1 in Verbindung mit Nummer 4.5.3 EVB-IT Systemvertrag ein, soweit nichts anderes vereinbart ist. An allen anderen Dokumentationen räumt der Auftragnehmer dem Auftraggeber die Rechte entsprechend Ziffer 2.3.1 bzw. bei gemieteten Dokumentationen die Rechte gemäß Ziffer 2.3.2 ein, soweit nichts anderes vereinbart ist. Sofern von den jeweiligen Rechteinhabern an der Dokumentation Rechte eingeräumt werden wie an Open Source Software*, gelten diese anstelle der Rechte gemäß Sätzen 1 und 2 dieser Ziffer 5.6.

5.7 Soweit die Lieferung einer Software Bill of Materials (SBOM)* vereinbart ist, muss diese vom Auftragnehmer für jede Software* gemäß der Technischen Richtlinie BSI TR-03183-2 bereitgestellt werden. Die Software Bill of Materials (SBOM)* muss für jeden neuen Programmstand* aktualisiert werden, wenn Systemservice vereinbart ist.

6 Mitteilungspflichten des Auftragnehmers

6.1 Der Auftragnehmer wird dem Auftraggeber unverzüglich mitteilen, wenn Vorgaben des Auftraggebers in nicht unwesentlichem Umfang fehlerhaft, unvollständig, widersprüchlich oder objektiv nicht ausführbar oder beizustellende Systemkomponenten* nicht vertragsgemäß sind und er dies erkennt oder hätte erkennen müssen. Sofern mit zumutbarem Aufwand möglich, hat er dem Auftraggeber gleichzeitig die ihm erkennbaren Folgen schriftlich mitzuteilen und vor weiteren Maßnahmen dessen Entscheidung abzuwarten. Der Auftraggeber wird diese Entscheidung unverzüglich mitteilen. Der Auftragnehmer ist jedoch nicht verpflichtet, die Vorgaben und Beistellungen weitergehend zu untersuchen und zu prüfen, als dies für die Erstellung des Gesamtsystems erforderlich ist.

6.2 Erkennt der Auftragnehmer, dass die Datensicherungsmaßnahmen des Auftraggebers nicht einer ordnungsgemäßen Datensicherung entsprechen, hat er dies und die ihm erkennbaren Folgen dem Auftraggeber unverzüglich schriftlich mitzuteilen.

6.3 Treten Änderungen bei Normen (z. B. EN, DIN, ISO) ein, die mehr als nur unwesentliche Auswirkungen auf die Leistungsverpflichtungen des Auftragnehmers haben, oder ändern sich die ausdrücklich für die Leistungserbringung vereinbarten Normen, hat der Auftragnehmer dies und die ihm erkennbaren Folgen dem Auftraggeber in angemessener Frist in Textform mitzuteilen.

6.4 Der Auftragnehmer teilt dem Auftraggeber auf dessen Anforderung in angemessener Frist, unabhängig davon spätestens jedoch bis zur Erklärung der Abnahme mit, welche für die Bearbeitung und Umgestaltung der Individualsoftware* notwendigen Werkzeuge* er bei deren Erstellung verwendet bzw. entwickelt hat.

6.5 Ist die Störungsbeseitigung oder die Überlassung neuer Programmstände* in Bezug auf Open Source Software* vereinbart, so setzt der Auftragnehmer den Auftraggeber über das Erscheinen neuer Programmstände* in Kenntnis und berät ihn dazu, wann ein neuer Programmstand* übernommen werden sollte, sofern für die Überlassung neuer Programmstände* keine abweichende Vereinbarung getroffen wurde. Ziffer 4.1.1 Absatz 3 findet keine Anwendung.

6.6 Sofern eine Mitwirkung des Auftraggebers nicht in zwischen den Parteien abgestimmten Zeitplänen festgehalten ist, hat der Auftragnehmer den Auftraggeber so rechtzeitig auf die zu erbringende Mitwirkung hinzuweisen, dass die vereinbarte Leistungserbringung nicht gefährdet wird. Sofern eine Mitwirkung des Auftraggebers nach Auffassung des Auftragnehmers nicht oder nicht rechtzeitig oder nicht ordnungsgemäß erfolgt und diese für den Projekterfolg wesentlich ist, wird der Auftragnehmer den Auftraggeber hierauf hinweisen.

6.7 Der Auftragnehmer teilt dem Auftraggeber Kopier- oder Nutzungssperren* mit, die die vertragsgemäße Nutzung des Gesamtsystems beeinträchtigen könnten. Dies gilt nicht für vom Auftraggeber beigestellte Systemkomponenten*.

6.8 Der Auftragnehmer wird den Auftraggeber auf dessen Anfrage angemessen über den Stand der Erstellung des Gesamtsystems informieren. Der Auftraggeber kann in diesem Zusammenhang nach rechtzeitiger Vorankündigung zu den üblichen Geschäftszeiten Einsicht in alle für die Beurteilung des Projektstandes notwendigen fachlichen und technischen projektbezogenen Unterlagen des Auftragnehmers verlangen. Er kann zu diesem Zweck einen Dritten beauftragen. Soweit rechtlich zulässig und zumutbar, wird sich der Auftraggeber bemühen, einen Dritten zu beauftragen, der kein Konkurrent des Auftragnehmers ist. Der Auftraggeber ist zur Verschwiegenheit verpflichtet und wird Dritte, die er beauftragt, zur Verschwiegenheit verpflichten. Der Ort der Einsichtnahme wird einvernehmlich festgelegt. Jede Partei trägt die ihr entstehenden Kosten.

6.9 Ist im Rahmen des Projektfortschritts festzustellen, dass die Einhaltung von Terminen gemäß Termin- und Leistungsplan gefährdet ist, wird der Auftragnehmer den Auftraggeber hierüber unverzüglich informieren.

7 Personal des Auftragnehmers, Subunternehmer

7.1 Der Auftragnehmer erbringt die Leistung durch Personal, das entsprechend den vertraglichen Vereinbarungen für die Erbringung der vereinbarten Leistung qualifiziert ist. Die Kommunikation mit dem Auftraggeber erfolgt in deutscher Sprache, soweit nichts anderes vereinbart ist.

7.2 Der Auftragnehmer darf zur Erbringung von Leistungen, die qualitativ oder quantitativ für das Gesamtsystem wesentlich sind, Subunternehmer nur einsetzen oder eingesetzte Subunternehmer nur auswechseln, wenn der Auftraggeber dem ausdrücklich zustimmt. Er wird unverzüglich zustimmen, wenn sich unter Berücksichtigung des neuen Subunternehmers anstelle des alten Subunternehmers keine andere Zuschlagsentscheidung ergeben hätte. Die Einarbeitung des neuen Subunternehmers erfolgt auf Kosten des Auftragnehmers. Für die im Angebot des Auftragnehmers benannten Subunternehmer gilt die Zustimmung des Auftraggebers als erteilt.

7.3 Auftraggeber und Auftragnehmer werden durch organisatorische Maßnahmen gewährleisten, dass die jeweils von ihnen im Rahmen der Gesamtsystemerstellung gegenseitig abgestellten Mitarbeiter ausschließlich dem Direktionsrecht und der Disziplinargewalt des jeweiligen Arbeitgebers unterstehen. Weisungen erfolgen ausschließlich im Rahmen der vereinbarten Aufgabenverteilung.

7.4 Der Auftragnehmer darf Personen in vereinbarten Schlüsselpositionen nur mit Einwilligung des Auftraggebers auswechseln. Der Auftraggeber wird seine Einwilligung unverzüglich erklären, wenn die Ablösung zwingend erforderlich ist und der Auftragnehmer eine qualifizierte Ersatzperson anbietet. Zwingend erforderlich ist die Ablösung, wenn der weitere Einsatz unmöglich ist. Personal, das nicht auf Schlüsselpositionen eingesetzt ist, darf der Auftragnehmer auch ohne Einwilligung des Auftraggebers auswechseln, sofern das Ersatzpersonal über die vertraglich vorausgesetzte Eignung verfügt. Die Einarbeitung erfolgt auf Kosten des Auftragnehmers.

8 Vergütung

8.1 Der Pauschalfestpreis* ist die einseitig nicht änderbare Gesamtvergütung, die für die Leistung nach Ziffer 1.1 geschuldet ist, soweit nicht für einzelne Leistungen eine gesonderte ggf. pauschalierte Vergütung vereinbart ist. Materialkosten, Reisezeiten, Reisekosten und Nebenkosten* sind im Pauschalfestpreis* enthalten. Soweit die Vereinbarung einer Vergütung bei Open Source Software* gegen die dafür geltenden Lizenzbedingungen verstößt, umfasst die vereinbarte Vergütung die Rechteverschaffung an solcher Standardsoftware* nicht; die Verpflichtung des Auftragnehmers zur Rechteverschaffung auch an solcher Standardsoftware* bleibt unberührt. Nachforderungen durch den Auftragnehmer sind ausgeschlossen, soweit die Parteien keine Änderung der Leistungen vereinbaren.

8.2 Eine im EVB-IT Systemvertrag vereinbarte Vergütung nach Aufwand ist das Entgelt für den Zeitaufwand, soweit nichts anderes vereinbart ist. Materialkosten, Reisezeiten, Reisekosten und Nebenkosten* werden entsprechend der vertraglichen Vereinbarung vergütet. Vom Auftraggeber zu vertretende Wartezeiten des Auftragnehmers werden wie Arbeitszeiten vergütet. Der Auftragnehmer muss sich jedoch anrechnen lassen, was er durch die Nichterbringung seiner Leistung erspart oder durch anderweitige Verwendung seiner Dienste erwirbt oder zu erwerben böswillig unterlässt. Ist bei Vergütung nach Aufwand eine Obergrenze vereinbart, ist der Auftragnehmer auch bei Überschreitung dieser Grenze zur vollständigen Erbringung der vereinbarten Leistung verpflichtet. Dies gilt nicht, wenn der Auftragnehmer die Überschreitung nicht zu vertreten hat. Der Auftragnehmer ist jedoch in diesem Fall verpflichtet, die vereinbarte Leistung gegen zusätzliche Vergütung nach Aufwand zu den vereinbarten Sätzen vollständig zu erbringen, sofern der Auftraggeber dies verlangt.

8.3 Die Vergütung für die Erstellung des Gesamtsystems wird nach der Gesamtabnahme fällig, soweit nicht im Zahlungsplan in Nummer 9 des EVB-IT Systemvertrages Zahlungen nach Teilabnahmen vereinbart sind. Anspruch auf Vorauszahlungen bzw. Abschlagszahlungen* hat der Auftragnehmer nur, soweit diese im EVB-IT Systemvertrag vereinbart sind. Das Recht, bei Vorliegen der Voraussetzungen des § 632a BGB Abschlagszahlungen* zu verlangen, bleibt jedoch unberührt.

8.4 Eine fällige Vergütung ist innerhalb von 30 Tagen nach Zugang einer prüffähigen Rechnung zu zahlen, soweit nichts anderes vereinbart ist. Dieser sind bei Vergütung nach Aufwand vom Auftragnehmer unterschriebene Nachweise über die Leistungen und die weiteren geltend gemachten Kosten, z.B. entsprechend Muster 2 - Leistungsnachweis Systemvertrag - beizufügen. Voraussetzung für die Fälligkeit

der Vergütung bei vereinbarter Vergütung nach Aufwand für Systemserviceleistungen gemäß Ziffer 4 ist darüber hinaus, soweit eine solche vereinbart ist, die Abnahme der jeweiligen Leistung.

8.5 Je Kalendertag wird pro Person nicht mehr als ein Tagessatz vergütet, soweit nichts anderes vereinbart ist. Ein vereinbarter Tagessatz kann nur dann in Rechnung gestellt werden, wenn mindestens 8 Zeitstunden geleistet wurden. Werden weniger als 8 Zeitstunden pro Tag geleistet, sind diese anteilig in Rechnung zu stellen. Ist ein Stundensatz vereinbart, werden angefangene Stunden anteilig vergütet. Pausen sind auszuweisen und werden nicht vergütet. Werden mehr als sechs Zeitstunden geleistet, wird vermutet, dass der Auftragnehmer eine halbstündige Pause eingelegt hat. Dies gilt nicht, wenn der Auftragnehmer nachweist, keine Pause gemacht zu haben.

8.6 Ist eine Preisanpassung für Leistungen vereinbart, die nicht im Pauschalfestpreis* enthalten sind, gilt, falls keine anderweitige Regelung vorgesehen ist, Folgendes: Eine Erhöhung der Vergütung kann erstmalig 12 Monate nach Abnahme des Gesamtsystems, weitere Erhöhungen frühestens jeweils 12 Monate nach Wirksamwerden der vorherigen Erhöhung angekündigt werden. Eine Erhöhung wird drei Monate nach der Ankündigung wirksam. Die Erhöhung hat angemessen und marktüblich zu sein und darf maximal 3 % der zum Zeitpunkt der Ankündigung der Erhöhung geltenden Vergütung betragen.

8.7 Alle Preise verstehen sich rein netto und, soweit Umsatzsteuerpflicht besteht, zuzüglich der gesetzlichen Umsatzsteuer.

9 Verzug

9.1 Der Vertragserfüllungstermin*, Teilabnahmetermine - soweit solche vereinbart wurden - und einzelne Meilensteine sind im Termin- und Leistungsplan gem. Nummer 8 des EVB-IT Systemvertrages festgelegt. Soweit nicht anders vereinbart, sind diese Termine verbindlich einzuhalten. Bei Verzögerungen, die der Auftragnehmer nicht zu vertreten hat, verschieben sich die von der Verzögerung betroffenen im Termin- und Leistungsplan genannten Ausführungsfristen angemessen; die gesetzlichen Ansprüche der Parteien bleiben hiervon unberührt.

9.2 Wenn der Auftragnehmer den Vertragserfüllungstermin* oder Teilabnahmetermine nicht einhält, kommt er ohne Mahnung in Verzug. Dies gilt nicht, wenn der Auftragnehmer die Verzögerung nicht zu vertreten hat. Der Auftraggeber kann im Fall des Verzuges den Verzögerungsschaden verlangen. Ferner kann der Auftraggeber vom EVB-IT Systemvertrag zurücktreten und Schadensersatz statt der Leistung verlangen, wenn er dem Auftragnehmer erfolglos eine angemessene Frist zur Leistung gesetzt hat. Anstelle des Schadensersatzes statt der Leistung kann der Auftraggeber Ersatz vergeblicher Aufwendungen im Sinne von § 284 BGB verlangen. Die Fristsetzung ist in den gesetzlich genannten Fällen gem. §§ 281 Abs. 2, 323 Abs. 2 BGB entbehrlich.

9.3 Des Weiteren ist der Auftraggeber für den Fall der Überschreitung des vereinbarten Vertragserfüllungstermins* um mehr als sieben Kalendertage berechtigt, für jeden Kalendertag, an dem sich der Auftragnehmer mit der Einhaltung des Vertragserfüllungstermins* in Verzug befindet, eine Vertragsstrafe in Höhe von 0,2 % des Auftragswertes* zu verlangen. Satz 1 gilt auch für Überschreitungen von vereinbarten Teilabnahmetermen. In diesem Fall berechnet sich die Vertragsstrafe nach dem auf die Teilleistung entfallenden Anteil am Auftragswert*. Insgesamt darf die Summe der aufgrund dieser Regelung zu zahlenden Vertragsstrafen jedoch nicht mehr als 5 % des Auftragswertes* betragen.

9.4 § 341 Abs. 3 BGB wird dahingehend abgeändert, dass die Strafe bis zur Schlusszahlung geltend gemacht werden kann. Dies gilt nicht, wenn sich der Auftraggeber bei der Abnahme die Vertragsstrafe trotz Aufforderung durch den Auftragnehmer nicht vorbehalten hat. Die Vertragsstrafen werden auf Schadensersatzansprüche angerechnet.

10 Projektmanagement

10.1 Das vereinbarte Vorgehensmodell ergibt sich aus Nummer 2.3 des EVB-IT Systemvertrages. Soweit dort nichts anderes vereinbart ist, ist der Auftragnehmer verantwortlich für

- Planung, Steuerung und Kontrolle des Projektes unter Einhaltung der Faktoren Zeit, Qualität und, soweit kein Festpreis vereinbart ist, Budget,
- Festlegung der Rahmenbedingungen für die Projektorganisation,
- Kontrolle und Einhaltung der vertraglichen Abmachungen,



System-AGB

- Organisation und Dokumentation eventueller Änderungsverfahren,
- Problem- und Konfliktlösung bei der Projektplanung, bei der Projektabwicklung und beim Projektabschluss,
- Überwachung des Projektfortschrittes und Einleitung von eventuell notwendigen Krisenmaßnahmen,
- Gewährleistung der Projektberichterstattung und -kommunikation,
- Berichterstattung an den Auftraggeber über den Projektverlauf.

10.2 Jeder Vertragspartner benennt in Nummer 10 des EVB-IT Systemvertrages einen oder mehrere Ansprechpartner (z.B. Projektleiter oder Projektmanager), die befugt sind, die im Projekt erforderlichen Entscheidungen entweder selbst zu treffen oder herbeizuführen. Hat ein Vertragspartner die Rolle des Projektleiters nicht besetzt, übernimmt diese Rolle dessen Projektmanager.

10.3 Sofern eine Vergütung nach Aufwand vereinbart ist, werden projektbezogene interne Abstimmungen des Auftragnehmers sowie Schulungen und Qualifizierungen des Auftragnehmers nicht vergütet.

11 Mitwirkung des Auftraggebers

11.1 Dem Auftraggeber obliegen die in Nummer 12 des EVB-IT Systemvertrages aufgeführten Mitwirkungsleistungen sowie die gemäß Nummer 3 des EVB-IT Systemvertrages vereinbarten Beistellungsleistungen. Er wird dem Auftragnehmer die erforderlichen Informationen und Unterlagen aus seiner Sphäre zur Verfügung stellen. Der Auftraggeber wird den Mitarbeitern des Auftragnehmers Zugang zu seinen Räumlichkeiten und der dort vorhandenen informationstechnischen Infrastruktur gewähren, soweit dies zur Erbringung der Leistung erforderlich ist und die vertraglich vereinbarten persönlichen Voraussetzungen (z.B. Sicherheitsüberprüfungen nach Sicherheitsüberprüfungsgesetz - SÜG) erfüllt sind. Kommt der Auftraggeber seinen Mitwirkungsleistungen trotz Aufforderung des Auftragnehmers nicht, nicht rechtzeitig oder unvollständig nach, kann der Auftragnehmer ein Angebot unterbreiten, diese Leistungen selbst anstelle des Auftraggebers zu erbringen. Sonstige Ansprüche des Auftragnehmers bleiben unberührt.

11.2 Verlangt der Auftragnehmer eine über die geschuldete Mitwirkung des Auftraggebers hinausgehende Leistung des Auftraggebers, kann der Auftraggeber es übernehmen, diese anstelle des Auftragnehmers als eigene Mitwirkungsobliegenheit zu erbringen; die für die Erstellung des Gesamtsystems zu zahlende Vergütung reduziert sich entsprechend. Der Auftragnehmer ist jedoch verpflichtet, diesen Beitrag des Auftraggebers zu prüfen, ggf. zu korrigieren und in das Gesamtsystem zu integrieren*. Die vertraglichen und gesetzlichen Ansprüche des Auftraggebers bleiben unberührt.

11.3 Der Auftraggeber hat Störungen bzw. Mängel unter Angabe der ihm bekannten und für deren Erkennung zweckdienlichen Informationen zu melden. Soweit keine andere Form der Störungsmeldung vereinbart ist, wird er diese in der Regel auf dem Störungsmeldeformular entsprechend Muster 1 vornehmen. Auf Nachfrage des Auftragnehmers hat er im Rahmen des Zumutbaren bestimmte, in seine Sphäre fallende Maßnahmen zu treffen, die eine Feststellung und Analyse der Störung bzw. des Mangels ermöglichen, z.B. notwendige, mit zumutbarem Aufwand von ihm beschaffbare einzelne technische Informationen aus seiner Sphäre bereit zu stellen.

11.4 Dem Auftraggeber obliegt, den Auftragnehmer über von ihm veranlasste Änderungen an der Systemumgebung* oder Beistellungen zu informieren, sofern sich diese auf die vertraglichen Leistungen des Auftragnehmers auswirken. Bei vereinbartem Systemservice obliegt es dem Auftraggeber, den Auftragnehmer rechtzeitig über nicht vom Auftragnehmer vorgenommene oder initiierte Änderungen an den Systemkomponenten* zu informieren, sofern sich diese auf die Erbringung der vertraglichen Leistungen des Auftragnehmers auswirken. Diese Obliegenheit gilt unabhängig davon, ob der Auftraggeber zu einer solchen Änderung berechtigt ist.

Der Auftragnehmer wird den Auftraggeber über ihm bekannte nachteilige Auswirkungen dieser Änderungen unverzüglich unterrichten. Jeder Vertragspartner kann verlangen, dass der Vertrag entsprechend der Änderungen angepasst wird.

Der Auftraggeber wird bei auszutauschenden Systemkomponenten* oder Teilen von diesen die Datenträger entnehmen, sofern nichts anderes vereinbart ist.



System-AGB

11.5 Bei vereinbartem Teleservice* wird der Auftraggeber entsprechend den Festlegungen in einer Teleservicevereinbarung die notwendigen technischen Einrichtungen beim Auftraggeber bereitstellen und den Zugriff auf das System ermöglichen.

11.6 Die ordnungsgemäße Datensicherung obliegt dem Auftraggeber, soweit die Datensicherung nicht Bestandteil der vom Auftragnehmer zu erbringenden Leistungen ist.

12 Abnahme

12.1 Abnahmegegenstand ist das Gesamtsystem und - soweit vereinbart - teilabnahmefähige Leistungen.

12.2 Der Auftragnehmer hat die Betriebsbereitschaft* des Gesamtsystems zum vereinbarten Termin zu erklären und das Gesamtsystem zur Funktionsprüfung zur Verfügung zu stellen. Wenn im EVB-IT Systemvertrag dafür kein Termin vereinbart ist, hat dies so rechtzeitig vor dem vereinbarten Vertragserfüllungstermin* zu erfolgen, dass dem Auftraggeber mindestens die vereinbarte Funktionsprüfungszeit vor dem Vertragserfüllungstermin* zur Verfügung steht. Die Erklärung der Betriebsbereitschaft* setzt voraus, dass der Auftragnehmer das Gesamtsystem vertragsgemäß hergestellt hat und die zur Durchführung der Funktionsprüfung vereinbarten Schulungen durchgeführt wurden. Abweichend davon kann der Auftragnehmer die Betriebsbereitschaft* auch ohne vorherige Schulung erklären, sofern der Auftraggeber dem Auftragnehmer trotz Aufforderung nicht ausreichend Gelegenheit dazu gegeben hat.

12.3 Soweit nichts anderes vereinbart ist, steht dem Auftraggeber das Recht zu, das Gesamtsystem innerhalb von 30 Tagen nach dem Zugang der Betriebsbereitschaftserklärung einer Funktionsprüfung zu unterziehen (Funktionsprüfungszeit). Für teilabzunehmende Leistungen gilt davon abweichend eine Funktionsprüfungszeit von 14 Tagen, soweit nichts anderes vereinbart ist.

12.4 Die Funktionsprüfung erfolgt nach der Erklärung der Betriebsbereitschaft* in der vertraglich vereinbarten Systemumgebung* beim Auftraggeber, soweit nichts anderes vereinbart ist. In der Funktionsprüfung werden das Gesamtsystem oder die teilabzunehmenden Leistungen auf Mangelfreiheit überprüft. Der Auftragnehmer wird den Auftraggeber bei der Vorbereitung und Durchführung der Funktionsprüfung in angemessenem Umfang unterstützen.

12.5 Werden betriebsverhindernde und/oder betriebsbehindernde Mängel festgestellt, kann der Auftraggeber die Funktionsprüfung abbrechen. Sofern lediglich betriebsbehindernde Mängel festgestellt werden, darf der Auftraggeber die Funktionsprüfung jedoch nur abbrechen, wenn deren Fortsetzung aufgrund der Mängel nicht mehr sinnvoll erscheint. Der Auftraggeber teilt dem Auftragnehmer nach Abschluss oder Abbruch der Funktionsprüfung bei der Funktionsprüfung festgestellte Mängel entsprechend der vereinbarten Mängelklassifizierung mit.

12.6 Hat der Auftraggeber die Funktionsprüfung gemäß Ziffer 12.5 Satz 1 abgebrochen, setzt er dem Auftragnehmer eine angemessene Frist, die Mängel zu beseitigen. Nach deren Beseitigung hat der Auftragnehmer erneut die Betriebsbereitschaft* des Gesamtsystems oder der teilabzunehmenden Leistungen zu erklären. Der Auftraggeber hat das Recht zur erneuten Funktionsprüfung. Soweit nichts anderes vereinbart ist, beträgt der dafür vereinbarte Zeitrahmen 14 Tage.

12.7 Ziffer 12.6 gilt auch, wenn die Funktionsprüfung trotz betriebsverhindernder Mängel und betriebsbehindernder Mängel vollständig durchgeführt wird.

12.8 Der Auftraggeber erklärt nach Ende der Funktionsprüfungszeit die Abnahme des Gesamtsystems, wenn dieses lediglich leichte Mängel aufweist und diese in ihrer Summe auch nicht gemäß Ziffer 3.2 als betriebsbehindernde Mängel gelten. Diese werden in der Abnahmeerklärung als Mängel festgehalten und vom Auftragnehmer im Rahmen seiner Haftung für Sach- und Rechtsmängel gemäß Ziffern 13 und 14 unverzüglich beseitigt, soweit nicht eine Frist für die Beseitigung vereinbart ist.

12.9 Teilabnahmen finden nur statt, wenn sie ausdrücklich vereinbart sind; in diesem Fall erfolgt die Erklärung der Betriebsbereitschaft* für die vereinbarten einzelnen Teile des Gesamtsystems. Soweit nicht anders vereinbart, ist Gegenstand der Teilabnahme die Funktionsfähigkeit der Teilleistung isoliert betrachtet, das heißt sie umfasst grundsätzlich weder systemübergreifende Funktionalitäten noch die Interoperabilität der Teilleistung mit anderen Teilen des Gesamtsystems. Systemübergreifende Funktionalitäten und die Interoperabilität der Teilleistungen sind dann Gegenstand der Teilabnahme, soweit die Nutzung dieser Teilleistungen vor der Gesamtabnahme vereinbart ist und diese Nutzung deren

Interoperabilität vereinbarungsgemäß voraussetzt. Nach Erklärung der Abnahme der letzten Teilleistung erfolgt eine Gesamtabnahme. Gegenstand der Gesamtabnahme ist insbesondere die Prüfung der systemübergreifenden Funktionalitäten sowie der Interoperabilität aller Teile des Gesamtsystems. Die Erklärung der Gesamtabnahme bleibt erforderlich. Die Erfüllung des EVB-IT Systemvertrages richtet sich ausschließlich danach, ob das Gesamtsystem wie vertraglich vereinbart insgesamt abnahmefähig im Sinne von Ziffer 12.8 ist. Hierfür bleibt der Auftragnehmer nachweispflichtig. Im Übrigen gelten die Regelungen zur Abnahme des Gesamtsystems entsprechend.

12.10 Kann der Auftragnehmer zum Vertragserfüllungstermin* kein abnahmefähiges Gesamtsystem übergeben, kommt er mit der Erfüllung des EVB-IT Systemvertrages in Verzug. Es gilt Ziffer 9. Vorgenannte Sätze gelten nicht, wenn der Auftragnehmer die Verzögerung nicht zu vertreten hat.

12.11 Die Abnahme hat förmlich zu erfolgen. Der Abnahme steht es aber gleich, wenn der Auftraggeber das Gesamtsystem nicht innerhalb einer ihm vom Auftragnehmer bestimmten angemessenen Frist abnimmt, obwohl er dazu verpflichtet ist.

13 Rechte des Auftraggebers bei Mängeln des Gesamtsystems (Gewährleistung)

13.1 Der Auftragnehmer verpflichtet sich, das Gesamtsystem frei von Sach- und Rechtsmängeln zu erstellen.

13.2 Für die zum Zeitpunkt der Abnahme beiden Parteien bekannten und nicht behobenen Mängel gelten die Mängelansprüche als vorbehalten.

13.3 Die Verjährungsfrist für Sach- und Rechtsmängelansprüche beträgt grundsätzlich 24 Monate, für Rechtsmängelansprüche an der Individualsoftware* 36 Monate jeweils ab der Erklärung der Gesamtabnahme, soweit nichts anderes vereinbart ist. Nach Ablauf von 12 Monaten der Verjährungsfrist ist, sofern sich der Auftragnehmer darauf beruft, ein Rücktritt vom EVB-IT Systemvertrag bezogen auf Standardsoftware* gleich aus welchem Grund ausgeschlossen. Hinsichtlich aller weiteren Leistungen bleibt das Recht zum Rücktritt unberührt, auch wenn der Rücktrittsgrund in einem Mangel der Standardsoftware* liegt. Abweichend von Satz 1 und 2 verjähren die Ansprüche in der regelmäßigen Verjährungsfrist, wenn der Auftragnehmer den Mangel arglistig verschwiegen hat. Die Verjährungsfrist endet in diesem Falle jedoch nicht vor den Fristen gemäß Satz 1 und 2.

13.4 Soweit Leistungen teilabgenommen wurden, beginnt die Verjährungsfrist mit dem Zeitpunkt der jeweiligen Teilabnahme und endet zwei Jahre nach der jeweiligen Teilabnahme, frühestens aber neun Monate nach der Gesamtabnahme. Soweit sich die Gesamtabnahme aus Gründen verzögert, die der Auftraggeber zu vertreten hat, beginnt die Neunmonatsfrist zu dem Zeitpunkt, zu dem die Gesamtabnahme ohne diese Verzögerung hätte erfolgen müssen.

13.5 Für alle Mängel an teilabgenommen Leistungen, die gleichzeitig Mängel des Gesamtsystems sind, beginnt die Verjährungsfrist mit der Teilabnahme, endet jedoch erst mit dem Ablauf der Verjährungsfrist für Mängel des Gesamtsystems.

13.6 Die Mängelansprüche erstrecken sich nicht auf beigestellte Systemkomponenten* und solche Systemkomponenten*, die der Auftraggeber oder ein Dritter ohne Zustimmung des Auftragnehmers ändert. Dies gilt nicht, wenn der Auftraggeber nachweist, dass diese Änderung für den gemeldeten Mangel nicht ursächlich und nicht auf eine zuvor durchgeführte Selbstvornahme gemäß Ziffer 13.11 zurückzuführen ist. Darüber hinaus erstrecken sich die Mängelansprüche nicht auf Software*, die der Auftraggeber nicht in der vereinbarten Systemumgebung* einsetzt, es sei denn, der Auftraggeber weist nach, dass dieser Einsatz für den gemeldeten Mangel nicht ursächlich war.

13.7 Die Rechtsmängelhaftung erstreckt sich nicht auf Ansprüche wegen Patentverletzungen und Gebrauchsmusterverletzungen im Sinne der deutschen Rechtsordnung, die Dritte gegen den Auftraggeber geltend machen, wegen dessen Nutzung von Systemkomponenten* außerhalb der Mitgliedsstaaten von EU und EFTA.

13.8 Meldet der Auftraggeber vor Ablauf der Verjährungsfrist Mängel und verhandeln die Parteien im Sinne des § 203 BGB, ist die Verjährung gehemmt, bis der Auftragnehmer oder der Auftraggeber die Fortsetzung der Verhandlungen verweigert. Die Verjährung tritt frühestens drei Monate nach dem Ende der Hemmung ein.

13.9 Eine neue Systemkomponente* ist vom Auftraggeber zu übernehmen, wenn sie der Vermeidung oder Beseitigung von Mängeln dient und der Auftragnehmer aus der Übernahme resultierende nachteilige Folgen für den Auftraggeber ebenfalls ausgleicht, wobei Ziffer 13.9 Anwendung findet. Zur Übernahme der neuen Systemkomponente* ist der Auftraggeber nicht verpflichtet, wenn ihm dies nicht zuzumuten ist, z.B. weil die neue Systemkomponente* wesentlich von der vereinbarten Ausführung oder im Hinblick auf ihre Bedienung abweicht. An neuen Programmständen* räumt der Auftragnehmer dem Auftraggeber Nutzungsrechte in Art und Umfang ein, wie sie für die gelieferte Software* bestehen.

Übernimmt der Auftraggeber eine neue Systemkomponente*, gilt Folgendes:

- Enthält die neue Systemkomponente* mehr Funktionalität als die im EVB-IT Systemvertrag aufgeführte Systemkomponente* (Mehrleistung), ist der Auftraggeber zur Zahlung einer Mehrvergütung nur verpflichtet, wenn er diese Mehrleistung nutzen will. Dazu zählt auch der Fall, dass er die Mehrleistung nutzt, obwohl er die neue Systemkomponente* auch ohne die Mehrleistung vertragsgemäß nutzen könnte, nicht jedoch der Fall, dass er die bisherige Funktionalität nur zusammen mit der Mehrleistung nutzen kann.
- Entstehen ihm durch die Nutzung der neuen Systemkomponente* höhere Kosten als zuvor gehen diese zu Lasten des Auftragnehmers. Dies gilt nicht, soweit diese höheren Kosten darauf zurückzuführen sind, dass der Auftraggeber vorhandene Mehrleistungen nutzen will; Satz 2 des ersten Aufzählungspunktes dieser Ziffer 13.9 gilt entsprechend.

13.10 Der Auftragnehmer hat ihm bekannte Mängel unverzüglich, spätestens innerhalb einer vom Auftraggeber gesetzten angemessenen Frist nach seiner Wahl durch Nachbesserung oder Neulieferung zu beheben. Handelt es sich um einen Mangel in der Standardsoftware*, kann der Auftragnehmer bis zur Überlassung eines den Mangel beseitigenden Programmstandes* eine Umgehungslösung* zur Verfügung stellen, soweit und solange dies für den Auftraggeber zumutbar ist. Die Verpflichtung des Auftragnehmers, den Mangel unverzüglich zu beseitigen, bleibt unberührt. Bei der Verletzung von Schutzrechten Dritter gilt vorrangig Ziffer 14. Der Auftragnehmer hat die zum Zwecke der Nacherfüllung erforderlichen Kosten, insbesondere Transport-, Wege-, Arbeits- und Materialkosten zu tragen. Erfolgt die Nacherfüllung durch Neuerstellung oder Neulieferung, entfällt der Nutzungsherausgabeanspruch des Auftragnehmers.

13.11 Schließt der Auftragnehmer die Mängelbehebung nicht innerhalb einer ihm gesetzten Frist erfolgreich ab, kann der Auftraggeber dem Auftragnehmer entweder

- eine weitere angemessene Nachfrist verbunden mit der Ankündigung setzen, nach deren fruchtlosem Ablauf den Mangel selbst zu beseitigen. Läuft diese Frist fruchtlos ab, ist der Auftraggeber berechtigt, den Mangel selbst zu beseitigen und Ersatz der erforderlichen Aufwendungen zu verlangen.
- oder eine weitere angemessene Nachfrist setzen und nach deren fruchtlosem Ablauf die Vergütung angemessen herabsetzen oder vom EVB-IT Systemvertrag ganz oder teilweise zurücktreten. Ein Rücktritt wegen eines unerheblichen Mangels ist jedoch ausgeschlossen.

Der Auftraggeber kann darüber hinaus bei Vorliegen der gesetzlichen Voraussetzungen Schadens- oder Aufwendungsersatz gem. § 634 Nr. 4 BGB im Rahmen der Ziffer 15 verlangen.

14 Schutzrechte Dritter

Macht ein Dritter gegenüber dem Auftraggeber Ansprüche wegen der Verletzung von Schutzrechten durch die Nutzung des erstellten Gesamtsystems oder sonstige Leistungen des Auftragnehmers geltend und wird deren Nutzung hierdurch beeinträchtigt oder untersagt, haftet der Auftragnehmer unbeschadet der Rechte des Auftraggebers gemäß Ziffern 8.1 und 13 wie folgt:

14.1 Der Auftragnehmer kann im Rahmen des Wahlrechts gemäß Ziffer 13.10 auf seine Kosten entweder die Leistungen so ändern oder ersetzen, dass sie das Schutzrecht nicht verletzen, aber im Wesentlichen doch den vereinbarten Funktions- und Leistungsmerkmalen in für den Auftraggeber zumutbarer Weise entsprechen, oder den Auftraggeber von Ansprüchen gegenüber dem Schutzrechtsinhaber freistellen.

14.2 Ist die Nacherfüllung dem Auftragnehmer unmöglich oder nur zu unverhältnismäßigen Bedingungen möglich, hat er das Recht, die betroffenen Leistungen gegen Erstattung der entrichteten Vergütung zurückzunehmen. Der Auftragnehmer hat dem Auftraggeber dabei eine angemessene Auslauffrist zu



System-AGB

gewähren, es sein denn, dies ist nur zu unzumutbaren rechtlichen oder sonstigen Bedingungen möglich. Die sonstigen Ansprüche des Auftraggebers z.B. auf Rücktritt, Minderung und Schadensersatz bleiben unberührt.

14.3 Ziffern 14.1 und 14.2 gelten entsprechend, soweit sich für die vertragsgemäße Ausübung der in Bezug auf die für die Software* vereinbarten Rechte weitere Vergütungspflichten gegenüber Dritten ergeben, z.B. für Patentlizenzen oder die Ausübung bestimmter Nutzungsrechte.

14.4 Die Parteien werden sich unverzüglich wechselseitig über geltend gemachte Ansprüche Dritter verständigen. Der Auftraggeber wird die behauptete Schutzrechtsverletzung nicht anerkennen und jegliche Auseinandersetzung einschließlich etwaiger außergerichtlicher Regelungen entweder dem Auftragnehmer überlassen oder nur im Einvernehmen mit dem Auftragnehmer führen. Der Auftragnehmer erstattet dem Auftraggeber notwendige Verteidigungskosten und sonstige Schäden, soweit dem Auftraggeber aus Rechtsgründen die geeigneten Abwehrmaßnahmen und Vergleichsverhandlungen vorbehalten bleiben bzw. bleiben müssen. Der Auftraggeber hat in diesem Fall Anspruch auf einen Vorschuss in Höhe der geschätzten Verteidigungskosten.

14.5 Soweit der Auftraggeber die Schutzrechtsverletzung selbst zu vertreten hat, sind Ansprüche gegen den Auftragnehmer ausgeschlossen.

15 Haftungsbeschränkung

Sofern keine andere vertragliche Haftungsvereinbarung vorliegt, gelten für alle gesetzlichen und vertraglichen Schadens-, Freistellungs- und Aufwendungsersatzansprüche des Auftraggebers folgende Regelungen:

15.1 Bei leicht fahrlässigen Pflichtverletzungen wird die Haftung für den Vertrag insgesamt grundsätzlich auf den Auftragswert* beschränkt. Davon abweichend gilt:

15.2 Beträgt der Auftragswert* weniger als 25.000,- €, wird die Haftung auf 50.000,- € beschränkt.

15.3 Beträgt der Auftragswert* 25.000,- € oder mehr und weniger als 100.000,- €, wird die Haftung auf 100.000,- € beschränkt.

15.4 Die Haftungsobergrenze für leicht fahrlässige Pflichtverletzungen beim Systemservice ist die Summe der Vergütungen, die für die Vertragslaufzeit für den Systemservice zu zahlen ist. Sie beträgt jedoch insgesamt minimal das Doppelte und maximal das Vierfache der Vergütung, die für das erste Vertragsjahr des Systemservice zu zahlen ist.

15.5 Bei der Bestimmung der vorgenannten Vergütungen bleibt eine etwaige vereinbarte Reduktion wegen Mängelansprüchen unberücksichtigt.

15.6 Bei Verlust von Daten haftet der Auftragnehmer nur für denjenigen Aufwand, der bei ordnungsgemäßer und regelmäßiger Datensicherung durch den Auftraggeber für die Wiederherstellung der Daten erforderlich gewesen wäre. Die Beschränkung gilt nicht, wenn und soweit die Datensicherung Bestandteil der vom Auftragnehmer zu erbringenden Leistungen ist.

15.7 Die Haftungsbeschränkungen gelten nicht für Ansprüche wegen Vorsatz und grober Fahrlässigkeit, bei der Verletzung des Lebens, des Körpers oder der Gesundheit, bei Arglist, soweit das Produkthaftungsgesetz zur Anwendung kommt sowie bei einem Garantieverprechen, soweit bzgl. letzterem nichts anderes geregelt ist.

15.8 Ansprüche aus entgangenem Gewinn sind ausgeschlossen, soweit in Nummer 15.4 des EVB-IT Systemvertrages nichts anderes vereinbart ist.

15.9 Soweit einbezogene Lizenzbedingungen Haftungsbeschränkungen zugunsten des Auftragnehmers vorsehen, gelten diese nicht gegenüber dem Auftraggeber. Satz 1 gilt entsprechend für den Ausschluss von Ansprüchen wegen Mängeln.

16 Laufzeit und Kündigung

16.1 Vertragliche Regelungen für Dauerschuldverhältnisse (die Leistungsteile Vermietung von Hardware, zeitweilige Überlassung von Standardsoftware*, Systemservice sowie Weiterentwicklung und Anpassung des Gesamtsystems) beginnen mit der Erklärung der Abnahme des Gesamtsystems, soweit nichts anderes vereinbart ist.



System-AGB

16.1.1 Ist für Dauerschuldverhältnisse kein Ende der jeweiligen Laufzeit im EVB-IT Systemvertrag vereinbart, kann der jeweilige Leistungsteil mit einer Frist von drei Monaten zum Ablauf eines Kalendermonats gekündigt werden, frühestens jedoch zum Ende einer im EVB-IT Systemvertrag vereinbarten Mindestvertragsdauer. Im EVB-IT Systemvertrag kann eine andere Kündigungsfrist vereinbart werden.

16.1.2 Eine Kündigung gemäß Ziffer 16.2 oder 16.3 erfasst auch die Dauerschuldverhältnisse. Der Auftraggeber ist aber berechtigt, einzelne oder alle Dauerschuldverhältnisse aus der Kündigung auszunehmen. Für die ausgenommenen Dauerschuldverhältnisse findet der EVB-IT Systemvertrag weiter Anwendung. Den Parteien bleibt es unbenommen, für die verbleibende Vertragslaufzeit stattdessen die Einbeziehung der jeweils einschlägigen EVB-IT bzw. BVB zu vereinbaren.

16.1.3 Ein wichtiger Grund für die Kündigung eines Dauerschuldverhältnisses über die zeitweilige Überlassung von Standardsoftware* durch den Auftragnehmer ist die schwerwiegende Verletzung von Nutzungsrechten des Rechteinhabers, die der Auftraggeber trotz schriftlicher Abmahnung aufrechterhält. Das Recht zur Kündigung auch ohne eine schriftliche Abmahnung gemäß § 543 Abs. 3 Satz 2 BGB bleibt für die dort genannten Fälle unberührt.

16.2 Der Auftraggeber hat das Recht, den EVB-IT Systemvertrag gemäß § 648 BGB zu kündigen. Soweit nichts anderes vereinbart ist, hat der Auftragnehmer im Falle der Kündigung aufgrund dieser Regelung die gesetzlichen Rechte, ist jedoch verpflichtet, auf der Basis der durch die Kündigung ersparten Aufwendungen die von ihm beanspruchte Vergütung nachvollziehbar darzulegen. Des Weiteren ist er verpflichtet darzulegen, welche Systemkomponente* er als fertig gestellt bzw. begonnen ansieht bzw. welche Systemkomponente* er bereits von Dritten erworben hat.

Der Auftragnehmer unterstützt den Auftraggeber auf dessen Wunsch gegen angemessene Vergütung in angemessener Weise so, dass der Auftraggeber oder ein Dritter das nach dem EVB-IT Systemvertrag vereinbarte Gesamtsystem fertig stellen kann, sofern dies für den Auftragnehmer nicht unzumutbar ist. Diese Unterstützungsleistung gilt als „Füllauftrag“ im Sinne von § 648 BGB, soweit dies für den Auftragnehmer nicht unzumutbar ist.

16.3 Im Übrigen kann der EVB-IT Systemvertrag von jedem Vertragsteil nur bei Vorliegen eines wichtigen Grundes - ohne Einhaltung einer Kündigungsfrist - innerhalb einer angemessenen Zeit ab Kenntnis des Kündigungsgrundes gekündigt werden. Ein wichtiger Grund liegt vor, wenn Tatsachen gegeben sind, aufgrund derer dem Kündigenden unter Berücksichtigung aller Umstände des Einzelfalles und unter Abwägung der Interessen der Vertragsteile die Fortsetzung des Vertrages nicht mehr zugemutet werden kann. Besteht der wichtige Grund in der Verletzung einer vertraglichen Pflicht, ist die Kündigung erst nach erfolglosem Ablauf einer zur Abhilfe gesetzten Frist oder nach erfolgloser Abmahnung zulässig, soweit nicht gemäß § 323 Abs. 2 BGB eine Fristsetzung entbehrlich ist.

16.3.1 Hat der Auftragnehmer die Kündigung zu vertreten, ist die tatsächlich fertig gestellte bzw. begonnene Leistung abzurechnen, soweit der Auftraggeber für sie Verwendung hat. Soweit noch nicht erfolgt, liefert der Auftragnehmer diese Leistung und überträgt dem Auftraggeber die vereinbarten Nutzungs- und Eigentumsrechte daran. Die Abrechnung erfolgt anteilig nach den vereinbarten Preisen. Die nicht verwendbare Leistung wird dem Auftragnehmer zurückgewährt. Die mit der Rückgewähr verbundenen Kosten trägt der Auftragnehmer. Die sonstigen gesetzlichen Rechte und Ansprüche bleiben unberührt.

16.3.2 Im Falle von Ziffer 16.3.1 unterstützt der Auftragnehmer den Auftraggeber auf dessen Wunsch gegen angemessene Vergütung in angemessener Weise so, dass der Auftraggeber oder ein Dritter das nach dem EVB-IT Systemvertrag vereinbarte Gesamtsystem fertig stellen kann, sofern dies für den Auftragnehmer nicht unzumutbar ist.

17 Änderung der Leistung nach Vertragsschluss

17.1 Der Auftraggeber kann nach Vertragsschluss jederzeit Änderungen des Leistungsumfangs des Gesamtsystems im Rahmen der Leistungsfähigkeit des Auftragnehmers verlangen, es sei denn, dies ist für den Auftragnehmer unzumutbar. Das Änderungsverfahren ist auf einem Formular gemäß Muster 3 - Änderungsverfahren EVB-IT Systemvertrag - zu dokumentieren, soweit nichts anderes vereinbart ist.



System-AGB

17.2 Der Auftragnehmer hat das Änderungsverlangen des Auftraggebers zu prüfen und wird dem Auftraggeber in angemessener Frist, insbesondere unter Berücksichtigung von Art und Umfang des Änderungsverlangens mitteilen, ob es zumutbar und falls nicht, warum es unzumutbar ist.

17.3 Hat das zumutbare Änderungsverlangen keinen Einfluss auf die vereinbarte Vergütung oder Termine, hat der Auftragnehmer unverzüglich mit der Umsetzung des Änderungsverlangens zu beginnen und dies dem Auftraggeber mitzuteilen.

17.4 Hat das zumutbare Änderungsverlangen Einfluss auf die vereinbarte Vergütung oder Termine, wird der Auftragnehmer ein Realisierungsangebot unter Angabe von Terminen und den Auswirkungen auf die vereinbarte Vergütung unterbreiten. Der Auftraggeber wird das Realisierungsangebot des Auftragnehmers in angemessener Frist annehmen oder ablehnen.

17.5 Bedarf die Erstellung des Realisierungsangebotes einer umfangreichen technischen Planung, kann der Auftragnehmer dieses von der Zahlung einer angemessenen Vergütung abhängig machen. Er wird in diesem Fall ein entsprechendes Planungsangebot mit Angabe der Vergütung unterbreiten. Der Auftraggeber wird das Planungsangebot des Auftragnehmers in angemessener Frist annehmen oder ablehnen.

17.6 Kommt eine Vereinbarung über die Änderung der Leistung zustande, ist der EVB-IT Systemvertrag, insbesondere die Leistungsbeschreibung, entsprechend anzupassen. Kommt keine Vereinbarung zustande, werden die Arbeiten auf der Grundlage des geltenden EVB-IT Systemvertrages weitergeführt. Ist das Änderungsverlangen dem Auftragnehmer zumutbar und kommt keine Vereinbarung zustande, weil sich die Parteien wegen Mehrleistungen nicht über die Anpassung der Vergütung einigen können, kann der Auftraggeber die Durchführung der Änderung gleichwohl verlangen. Die Vergütung wird in diesem Fall angemessen erhöht. Kommt keine Vereinbarung zustande, weil sich die Parteien wegen Mehrleistungen nicht über die Anpassung des Termin- und Leistungsplanes einigen können, kann der Auftraggeber die Durchführung der Änderung gleichwohl verlangen. In diesem Fall verschieben sich die von der Änderung betroffenen im Termin- und Leistungsplan genannten Ausführungsfristen angemessen.

18 Quellcodeübergabe und Quellcodehinterlegung

18.1 Soweit nichts anderes vereinbart ist, hat der Auftragnehmer den jeweils aktuellen Stand des Quellcodes* der Individualsoftware* und etwaiger Anpassungen der Standardsoftware* auf Quellcodeebene gemäß Ziffer 2.3.3 mit der Abnahme des Gesamtsystems und nach der Abnahme bei jeder Übergabe eines neuen Programmstandes* der Individualsoftware* bzw. der betroffenen Standardsoftware* an den Auftraggeber zu übergeben. Zum Quellcode* gehören dessen fachgerechte Kommentierung und die Beschreibung der notwendigen Systemparameter sowie sonstige notwendige Informationen, die den Auftraggeber in die Lage versetzen, mit Fachpersonal den Quellcode* zu bearbeiten, um eine selbstständige Weiterentwicklung der Individualsoftware* bzw. der Anpassungen der Standardsoftware* auf Quellcodeebene vorzunehmen. Die Übergabe soll in elektronischer Form auf einem Datenträger erfolgen und wird protokolliert.

18.2 Die Pflicht zur Übergabe des Quellcodes bei jeder Übergabe eines neuen Programmstandes nach Ziffer 18.1 besteht nicht, wenn der Auftragnehmer gemäß Ziffer 2.3.3 erklärt, er werde die Anpassungen in den Standard übernehmen und dies auch vertragsgemäß umsetzt. Der Auftraggeber erhält an allen Fassungen des Quellcodes* und der Dokumentationen im Zeitpunkt der jeweiligen Erstellung ein Nutzungsrecht gemäß Ziffer 2.3.4.1. Der Auftraggeber wird den Quellcode* wie eigene vertrauliche Informationen behandeln und Dritten nur im Rahmen der bestimmungsgemäßen Nutzung zugänglich machen und diese ebenfalls zur Vertraulichkeit verpflichten. Auf Open Source Software* findet diese Ziffer 18.2 keine Anwendung.

18.3 Ist die Hinterlegung des Quellcodes* bestimmter Software* vereinbart, erfolgt diese aufgrund der im EVB-IT Systemvertrag aufgeführten Hinterlegungsvereinbarung bei der vereinbarten Hinterlegungsstelle. Die Hinterlegungsverpflichtung bezieht sich auf die vom Auftragnehmer auf der Grundlage des EVB-IT Systemvertrages jeweils letzte geänderte Fassung des Quellcodes* eines überlassenen Programmstandes* einschließlich von Fehlerbeseitigungen. An sämtlichen Fassungen des Quellcodes* von Individualsoftware* stehen dem Auftraggeber die Rechte gemäß Ziffer 2.3.4.1 zu. An sämtlichen zu hinterlegenden Fassungen des Quellcodes* von Standardsoftware* steht dem Auftraggeber das für den Fall der Herausgabe aufschiebend bedingte Recht zu, diese zum Zwecke der Fehlerbeseitigung und zur Aufrechterhaltung der Nutzungsmöglichkeit, insbesondere im Gesamtsystem zu bearbeiten und daraus



System-AGB

ausführbare neue Programmstände* zu erzeugen, an denen dem Auftraggeber wiederum dieselben Rechte wie an dem ursprünglich überlassenen Stand der Standardsoftware* zustehen. Die vorgenannten Rechteeinräumungen erfolgen bei Quellcodes* von Individualsoftware* mit der jeweiligen Entstehung derselben und bei Quellcodes* von Standardsoftware* mit Überlassung der ausführbaren Programmstände*.

18.4 Ist für die hinterlegte Standardsoftware* die Lieferung neuer Programmstände* in Nummer 5.1.3 des EVB-IT Systemvertrages vereinbart, bezieht sich die Hinterlegungsverpflichtung ebenfalls auf den jeweiligen Quellcode* der überlassenen Programmstände*.

18.5 Die Kosten der Hinterlegung trägt der Auftraggeber.

18.6 Die Regelungen dieser Ziffer 18 beschränken nicht etwaige Rechte des Auftraggebers an Open Source Software*.

19 Haftpflichtversicherung

19.1 Soweit vereinbart, weist der Auftragnehmer bei Abschluss des EVB-IT Systemvertrages dem Auftraggeber nach, dass er über eine in Rahmen und Umfang marktübliche Industriehaftpflichtversicherung oder eine vergleichbare Versicherung aus einem Mitgliedsstaat der EU verfügt.

19.2 Der Auftragnehmer wird diesen Versicherungsschutz bis zum Ende des EVB-IT Systemvertrages aufrechterhalten, mindestens aber bis zur Verjährung der Mängelansprüche. Kommt der Auftragnehmer dieser Verpflichtung nicht nach, ist der Auftraggeber nach erfolgloser angemessener Fristsetzung zum Rücktritt vom EVB-IT Systemvertrag berechtigt, wenn ihm ein Festhalten am Vertrag nicht mehr zuzumuten ist. Weitergehende Ansprüche des Auftraggebers, insbesondere Schadensersatzansprüche, bleiben hiervon unberührt. Nach Gesamtabnahme tritt an die Stelle des Rücktrittsrechts das Recht zur Kündigung des Systemservices.

20 Vorauszahlungsbürgschaft, Vertragserfüllungs- und Mängelhaftungssicherheit

20.1 Sind im EVB-IT Systemvertrag Sicherheiten vereinbart, gilt Folgendes:

20.1.1 Ist der Auftraggeber mit Abschluss des EVB-IT Systemvertrages zu einer Vorauszahlung verpflichtet, leistet er diese Zug um Zug gegen Übergabe einer unbefristeten, selbstschuldnerischen Bürgschaft eines deutschen Kreditinstituts oder eines vergleichbaren Kreditinstituts aus einem Mitgliedsstaat der EU in Höhe der vereinbarten Vorauszahlung. Eine Hinterlegung eines Geldbetrages als Sicherheit für den Auftraggeber durch den Auftragnehmer ist ausgeschlossen. Die Bürgschaft dient als Sicherheit für Ansprüche des Auftraggebers auf Rückzahlung der Vorauszahlung. Die Vorauszahlungsbürgschaftsurkunde ist unverzüglich zurückzugeben, wenn der Auftragnehmer Leistungen im Wert der Vorauszahlung erbracht hat.

20.1.2 Ist eine Vertragserfüllungssicherheit vereinbart, hinterlegt der Auftragnehmer bei Abschluss des EVB-IT Systemvertrages den im EVB-IT Systemvertrag als Sicherheit vereinbarten Geldbetrag gemäß § 18 Nr. 5 VOL/B oder übergibt dem Auftraggeber eine unbefristete, selbstschuldnerische Bürgschaft eines deutschen Kreditinstituts oder eines vergleichbaren Kreditinstituts aus einem Mitgliedsstaat der EU in der vereinbarten Höhe. Die Sicherheit dient der Absicherung sämtlicher Ansprüche des Auftraggebers aus der Erstellung des Gesamtsystems bis zur Abnahme, insbesondere für Ansprüche wegen Pflichtverletzungen des Auftragnehmers, aus Vertragsstrafe und ungerechtfertigter Bereicherung. Die Vertragserfüllungssicherheit beträgt 10 % des Erstellungspreises*, sofern nichts anderes vereinbart ist. Der Auftraggeber kann eine Anpassung verlangen, wenn sich der Auftragswert* gegenüber dem Erstellungspreis* erhöht. Eine Anpassung ist erstmalig bei einer Erhöhung um 10 % und im Übrigen in angemessenen Schritten möglich. Die Vertragserfüllungssicherheit ist unverzüglich zurückzugeben, wenn der Auftragnehmer das Gesamtsystem vertragsgemäß erstellt hat, die etwa vereinbarte Sicherheit für die Erfüllung der Mängelansprüche geleistet ist und bis dahin erhobene Ansprüche auf Schadensersatz oder Erstattung von Überzahlungen befriedigt sind. Soweit Teilabnahmen durchgeführt wurden, erfolgt eine teilweise Rückgabe der Vertragserfüllungssicherheit.

20.1.3 Ist eine Mängelhaftungssicherheit vereinbart, hinterlegt der Auftragnehmer zum Zeitpunkt der Gesamtabnahme den vereinbarten Geldbetrag gemäß § 18 Nr. 5 VOL/B oder übergibt dem Auftraggeber eine unbefristete, selbstschuldnerische Bürgschaft eines deutschen Kreditinstituts oder eines



System-AGB

vergleichbaren Kreditinstituts aus einem Mitgliedsstaat der EU in der vereinbarten Höhe. Die Mängelhaftungssicherheit beträgt 5 % des Auftragswertes*, soweit nichts anderes vereinbart ist. Die Sicherheit dient der Absicherung sämtlicher Mängelansprüche aus der Erstellung des Gesamtsystems. Die bei Gesamtabnahme zu stellende Sicherheit ist unverzüglich nach Ablauf der Verjährungsfristen für Mängelansprüche des Gesamtsystems und nach Erfüllung der bis dahin erhobenen Mängelansprüche an den Auftragnehmer zurückzugeben.

20.1.4 Ist eine kombinierte Vertragserfüllungs- und Mängelhaftungssicherheit vereinbart, hinterlegt der Auftragnehmer bei Abschluss des EVB-IT Systemvertrages den als Sicherheit vereinbarten Geldbetrag gemäß § 18 Nr. 5 VOL/B oder übergibt dem Auftraggeber eine unbefristete, selbstschuldnerische Bürgschaft eines deutschen Kreditinstituts oder eines vergleichbaren Kreditinstituts aus einem Mitgliedsstaat der EU in der vereinbarten Höhe. Die kombinierte Vertragserfüllungs- und Mängelhaftungssicherheit beträgt hinsichtlich der Vertragserfüllung 10 % und hinsichtlich der Mängelhaftung 5 % des Erstellungspreises*, soweit nichts anderes vereinbart ist. Der Auftraggeber kann eine Anpassung verlangen, wenn sich der Auftragswert* gegenüber dem Erstellungspreis* erhöht. Eine Anpassung ist erstmalig bei einer Erhöhung um 10 % und im Übrigen in angemessenen Schritten möglich. Die Sicherheit dient als Vertragserfüllungssicherheit der Absicherung sämtlicher Ansprüche des Auftraggebers aus der Erstellung des Gesamtsystems bis zur Abnahme, insbesondere für Ansprüche wegen Pflichtverletzungen des Auftragnehmers, aus Vertragsstrafe und ungerechtfertigter Bereicherung. Ist eine Teilabnahme oder die Gesamtabnahme erfolgt, dient die Sicherheit auch der Absicherung sämtlicher Mängelansprüche aus der Erstellung des Gesamtsystems. Die Sicherheit ist unverzüglich nach Ablauf der Verjährungsfristen für Mängelansprüche des Gesamtsystems und nach Erfüllung der bis dahin erhobenen Ansprüche auch auf Erstattung von Überzahlungen und Schadensersatz an den Auftragnehmer zurückzugeben.

20.2 Bürgschaften können auch durch andere Bürgen als deutsche Kreditinstitute oder vergleichbare Kreditinstitute aus einem Mitgliedsstaat der EU gestellt werden, sofern der Auftraggeber den Bürgen zuvor als tauglich anerkannt hat.

21 Datenschutz, Geheimhaltung und Sicherheit

21.1 Der Auftraggeber gibt dem Auftragnehmer alle relevanten, über die gesetzlichen Regelungen hinausgehenden Sachverhalte bekannt, deren Kenntnis für ihn aus Gründen des Datenschutzes und der Geheimhaltung erforderlich ist.

21.2 Vor Übergabe eines Datenträgers an den Auftragnehmer stellt der Auftraggeber die Löschung schutzwürdiger Inhalte sicher, soweit nichts anderes vereinbart ist.

21.3 Der Auftragnehmer sorgt dafür, dass alle Personen, die von ihm mit der Bearbeitung oder Erfüllung des EVB-IT Systemvertrages betraut sind, die gesetzlichen Bestimmungen über den Datenschutz beachten. Die nach Datenschutzrecht erforderliche Verpflichtung auf das Datengeheimnis ist spätestens vor der erstmaligen Aufnahme der Tätigkeit vorzunehmen und dem Auftraggeber auf Verlangen schriftlich zu bestätigen.

21.4 Der Auftraggeber kann ganz oder teilweise vom EVB-IT Systemvertrag zurücktreten, wenn der Auftragnehmer seine Pflichten gemäß Ziffer 21.3 unter Berücksichtigung der Sachverhalte gemäß Ziffer 21.1 schuldhaft innerhalb einer gesetzten angemessenen Frist nicht nachkommt oder Datenschutzvorschriften vorsätzlich oder grob fahrlässig verletzt. Betreffen vorgenannte Pflichtverletzungen ausschließlich den Systemservice, tritt an die Stelle des Rücktrittsrechts das Recht zur Kündigung des Systemservices.

21.5 Auftraggeber und Auftragnehmer sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten vertraulichen Informationen, Geschäfts- und Betriebsgeheimnisse vertraulich zu behandeln, insbesondere nicht an Dritte weiterzugeben oder anders als zu vertraglichen Zwecken zu verwenden. Dies gilt auch für den Erfahrungsaustausch innerhalb der öffentlichen Hand.

21.6 Vertrauliche Informationen sind Informationen, die ein verständiger Dritter als schützenswert ansehen würde oder die als vertraulich gekennzeichnet sind; dies können auch solche Informationen sein, die während einer mündlichen Präsentation oder Diskussion bekannt werden. Vertrauliche Informationen dürfen ausschließlich zum Zweck der Erfüllung der Verpflichtungen aus dem EVB-IT Systemvertrag eingesetzt werden. Die Verpflichtung zur Vertraulichkeit gilt nicht für Informationen, die den Parteien



System-AGB

bereits rechtmäßig bekannt sind oder außerhalb des EVB-IT Systemvertrages ohne Verstoß gegen eine Vertraulichkeitsverpflichtung bekannt werden.

22 Zurückbehaltungsrechte

Zurückbehaltungs- und Leistungsverweigerungsrechte des Auftragnehmers sind ausgeschlossen, es sei denn, der Auftraggeber bestreitet die zugrunde liegenden Gegenansprüche nicht oder diese sind rechtskräftig festgestellt.

23 Schlichtungsverfahren

Die Parteien können vereinbaren, bei Meinungsverschiedenheiten aus oder im Zusammenhang mit der Vertragserfüllung, die sie nicht untereinander bereinigen können, eine Schlichtungsstelle anzurufen, um den Streit nach deren Schlichtungsordnung ganz oder teilweise vorläufig oder endgültig zu bereinigen. Sofern die Parteien im EVB-IT Systemvertrag eine Schlichtung vereinbart haben, ist dies nur wirksam, wenn die Schlichtungsstelle dort konkret bezeichnet ist und diese in Bezug auf derartige Meinungsverschiedenheiten auch tatsächlich tätig wird. Zur Ermöglichung der Schlichtung verzichten die Parteien wechselseitig auf die Einrede der Verjährung für alle Ansprüche aus dem streitigen Sachverhalt ab Schlichtungsantrag bis einen Monat nach Ende des Schlichtungsverfahrens. Der Verzicht bewirkt eine Hemmung der Verjährung.

24 Textform

Soweit nichts anderes geregelt ist, bedürfen vertragliche Mitteilungen und Erklärungen mindestens der Textform. Für Mängelrügen ist der Eintrag in ein Ticketsystem ausreichend.

25 Anwendbares Recht

Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss der Normen, die in eine andere Rechtsordnung verweisen, und des Übereinkommens der Vereinten Nationen über Verträge über den internationalen Warenkauf (CISG*).

Begriffsbestimmungen

Begriff	Definition
Abschlagszahlung	Anteilige Zahlung der vereinbarten Vergütung vor deren Fälligkeit. Ein Anspruch auf Abschlagszahlungen kann im EVB-IT Systemvertrag vereinbart werden.
Angebotspreis	Dient der Ermittlung des wirtschaftlichsten Angebots für die einzelnen Leistungen des Vertrages, z.B. Systemserviceleistungen, Weiterentwicklung des Gesamtsystems.
Auftragswert	Summe aus Erstellungspreis* und aller im Rahmen des Projektes bis zur Gesamtabnahme vereinbarten Vergütungserhöhungen oder -verringerungen, insbesondere aufgrund von Änderungsverlangen (Change Requests).
Beizustellende Systemkomponenten	Die vom Auftraggeber beizustellenden Systemkomponenten* bilden mit den vom Auftragnehmer zu liefernden und/oder herzustellenden Systemkomponenten* das

System-AGB

Begriff	Definition
	Gesamtsystem. Die beizustellenden Systemkomponenten* können sowohl Teile der beim Auftraggeber zum Zeitpunkt des Vertragsschlusses vorhandenen Systemumgebung* sein als auch später hinzukommende neue Komponenten, die der Auftraggeber zur Erfüllung seiner Mitwirkungsleistungen vereinbarungsgemäß beschafft oder erstellt.
Betriebsbereitschaft	Das Gesamtsystem ist vertragsgemäß erstellt.
CISG	United Nations Convention on Contracts for the international Sales of Goods (Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenkauf).
Copyleft	Eine Lizenzbedingung, die für die Nutzung, Änderung oder Verbreitung der lizenzierten Software* oder Softwarekomponente verlangt, dass die Software*, Softwarekomponente oder davon abgeleitete Werke unter inhaltsgleichen (Copyleft)Lizenzbedingungen kostenlos und in Quellcode*form zur Verfügung gestellt werden.
Customizing	Anpassen von Systemkomponenten* an die Anforderungen des Auftraggebers zur Erstellung des Gesamtsystems und zur Herbeiführung der Betriebsbereitschaft*, das nicht auf Quellcodeebene erfolgt.
Erstellungspreis	Angebotspreis* für die Erstellung des Gesamtsystems.
Gesamtangebotspreis	Dient der Ermittlung des wirtschaftlichsten Angebots und ist die Summe aller Angebotspreise*, die vereinbart sind oder abgerufen werden können.
Individualsoftware	Softwareprogramme, Programm-Module, Tools etc., die zur Vertragserfüllung für die Bedürfnisse des Auftraggebers vom Auftragnehmer erstellt wurden einschließlich der zugehörigen Dokumentation. Hierzu gehören auch die Anpassungen von Standard- oder Individualsoftware* auf Quellcodeebene. Nicht hierzu gehören jedoch Customizing* und die Anpassungen von Standardsoftware*, die gemäß Ziffer 2.3.1.3 in den Standard übernommen wurden.
Installation	Alle notwendigen Maßnahmen für das Einbringen der Software* in die vereinbarte Systemumgebung* sowie die Herbeiführung der vereinbarten

System-AGB

Begriff	Definition
	Ablauffähigkeit der Software* einschließlich aller notwendigen Prüfungen und Kontrollen zur Erstellung des Gesamtsystems und zur Herbeiführung der Betriebsbereitschaft*.
Integration	Einbetten von Hardware und/oder Software* in das Gesamtsystem innerhalb der vereinbarten Systemumgebung* zum Zwecke der Erstellung des Gesamtsystems und zur Herbeiführung der Betriebsbereitschaft*.
Kopier- oder Nutzungssperre	Maßnahmen zur Einschränkung der Kopierbarkeit und/oder Nutzungsmöglichkeit einer Systemkomponente*.
Nebenkosten	Aufwendungen des Auftragnehmers, die zur Leistungserbringung notwendig, aber weder Reisekosten noch Materialkosten sind.
Objektcode	Zwischenergebnis eines Compiler- bzw. Übersetzungsvorgangs des Quellcodes* eines Programms.
openCode	openCode ist die gemeinsame Plattform der Öffentlichen Verwaltung für den Austausch von Open Source Software.
Open Source Software	Die Standardsoftware* bzw. Softwarekomponente liegt vollständig im Quellcode* vor und an der Standardsoftware* bzw. Softwarekomponente werden Nutzungsrechte eingeräumt, die es jedermann, jederzeit, an jedem Ort und zu jedem Zweck, unentgeltlich und inhaltlich unbeschränkt gestatten, die Standardsoftware* bzw. Softwarekomponente ohne Auflagen, Bedingungen oder weitere Voraussetzungen im Objekt- und Quellcode* zu benutzen und zu verwenden, insbesondere zu analysieren, dauerhaft und vorübergehend in unveränderter oder veränderter Form ganz oder in Teilen zu vervielfältigen, zu übersetzen, zu bearbeiten, zu arrangieren, zu verändern oder anderweitig umzuarbeiten und im Original, als Vervielfältigungsstück in Quellcode*- oder Objektcodeform zu verbreiten und zu vermieten, öffentlich wiederzugeben und öffentlich zugänglich zu machen, ohne dass es notwendig ist, eine zusätzliche Lizenz zu erwerben. Solche Standardsoftware* oder Softwarekomponenten werden gewöhnlich auch Open Source Software (OSS), Freie Software / Free Software oder Free, Libre and Open Source Software (FLOSS) genannt.

System-AGB

Begriff	Definition
	Die Verbreitung, Vermietung, öffentliche Wiedergabe und öffentliche Zugänglichmachung einer solchen Standardsoftware* bzw. Softwarekomponente darf entgegen der vorstehenden Regelung weder eingeschränkt noch an andere Auflagen, Bedingungen oder Voraussetzungen geknüpft werden, als an die folgenden: • Weitergabe des Lizenztextes • Ausschluss der Erweiterung der jeweiligen Lizenz um zusätzliche Bedingungen • Copyleft*-Pflicht • Verbreitung, Vermietung, öffentliche Wiedergabe und öffentliche Zugänglichmachung der Standardsoftware* bzw. Softwarekomponente frei von Entgelten für die Einräumung von Nutzungsrechten („Lizenzgebühren“, „License Fees“) • Weitergabe unter anderen Lizenzbedingungen kann von weiteren Voraussetzungen abhängig gemacht werden • Pflicht zur Weitergabe oder sonstigen Bereitstellung des Quellcodes* und ggf. Pflicht zur Weitergabe oder sonstigen Bereitstellung weiterer Materialien • Pflicht zur Angabe von Urheber- oder Markenhinweisen und ähnlichen Hinweisen oder Material (z. B. NOTICE-Dateien) und Pflicht zu ähnlichen Angaben • Pflicht zu Hinweisen auf die Verwendung der Standardsoftware* bzw. Softwarekomponente in einer anderen Software, z. B. in der Dokumentation oder der Standardsoftware* selbst • Angaben zu Änderungen an der Standardsoftware* bzw. Softwarekomponente. Die Lizenz kann vorschreiben, dass abgeleitete Werke einen anderen Namen oder eine andere Versionsnummer als die Originalsoftware tragen müssen • Weitergabe oder Anzeige eines Haftungsausschlusses • Mitliefern von Installationsinformationen* in bestimmten Fällen • bei der Weitergabe zusammen mit Drittsoftware: Eine Verpflichtung zur Klarstellung in den Lizenzbedingungen der Drittsoftware, dass die Lizenzbedingungen der

System-AGB

Begriff	Definition
	Standardsoftware* bzw. Softwarekomponente unberührt bleiben. Die unter evb-it.gov.de verfügbare „Open Source Lizenzliste“ enthält Lizenzen, die dieser Definition entsprechen.
Patch	Behebung eines Mangels und/oder einer Störung in der Standardsoftware* ohne Eingriff in den Quellcode*.
Pauschalpreis	Umfasst den Erstellungspreis*, den Angebotspreis* für Systemserviceleistungen, den Angebotspreis* für die Weiterentwicklung und Anpassung des Gesamtsystems sowie den Angebotspreis* für sonstige Leistungen, jeweils sofern diese zum Festpreis vereinbart sind.
Programmbibliothek	Eine Programmbibliothek, auch als Softwarebibliothek oder Codebibliothek bezeichnet, ist eine Sammlung von wiederverwendbaren Softwareressourcen, die Funktionen, Routinen, Klassen, Datenstrukturen und andere Elemente enthält, die in der Softwareentwicklung verwendet werden können.
Programmstand	Oberbegriff für Patch*, Update*, Upgrade* und neue(s) Release/Version*.
Quellcode	Code eines Programms in der Fassung der Programmiersprache.
Reaktionszeit	Zeitraum, innerhalb dessen der Auftragnehmer mit den Störungs- bzw. Mängelbehebungsarbeiten zu beginnen hat. Der Zeitraum beginnt mit dem Zugang der Störungs- bzw. Mängelmeldung innerhalb der vereinbarten Servicezeiten und läuft während der vereinbarten Servicezeiten.
Release/Version	Neue Entwicklungsstufe einer Software*, die sich gegenüber dem vorherigen Release bzw. der Version im Funktions- und/oder Datenspektrum erheblich unterscheidet (z.B. 4.5.7 à 5.0.0).
Reverse Engineering	Reverse Engineering von Software* bezieht sich auf den Prozess, bei dem die Software* analysiert wird, um ihre Funktionsweise, Struktur oder andere wichtige Informationen zu verstehen.
Schaden stiftende	Software mit vom Auftraggeber unerwünschter, nicht vereinbarter Funktion, die zumindest auch den Zweck hat, die Verfügbarkeit von Daten, Ressourcen oder Dienstleistungen, die

System-AGB

Begriff	Definition
	Vertraulichkeit von Daten oder die Integrität von Daten, zu gefährden bzw. zu beeinträchtigen, z.B. Viren, Würmer, Trojanische Pferde.
Software	Oberbegriff für Standardsoftware* und Individualsoftware*.
Software Bill of Materials (SBOM)	Eine formale, strukturierte Aufzeichnung, die die Softwarekomponenten einer Software* identifiziert und ihre Beziehungen untereinander und zu anderer Software*/anderen Softwarekomponenten beschreibt. Anwendung findet hierbei BSI TR-03183-2.
Standardsoftware	Softwareprogramme, Programm-Module, Tools etc., die für die Bedürfnisse einer Mehrzahl von Kunden am Markt und nicht speziell vom Auftragnehmer für den Auftraggeber entwickelt wurden, einschließlich der zugehörigen Dokumentation.
Systemkomponente	Teil des Gesamtsystems, z.B. Hard- oder Software*. Hierzu gehören auch auf der Grundlage des EVB-IT Systemsvertrages überlassene neue Programmstände*.
Systemumgebung	Technische, räumliche und fachlich organisatorische Umgebung, in die das zu liefernde System zu integrieren ist.
Teleservice	Leistungen unter Inanspruchnahme von technischen Einrichtungen zur Fernkommunikation von einem Standort außerhalb des Einsatzortes des Gesamtsystems.
Umgehungslösung	Temporäre Überbrückung eines Mangels und/oder einer Störung in der Software*.
Update	Bündelung mehrerer Mängelbehebungen und/oder Störungsbeseitigungen sowie ggf. geringfügige funktionale Verbesserungen und/oder Anpassungen der Software* (z.B. 4.1.3 à 4.1.4).
Upgrade	Bündelung mehrerer Mängelbehebungen und/oder Störungsbeseitigungen und mehr als geringfügige funktionale Verbesserungen und/oder Anpassungen der Software* (z.B. 4.1.3 à 4.2.0).
Version/Release	siehe Release/Version.
Vertragserfüllungstermin	Termin, zu dem der Auftragnehmer alles Vereinbarte getan haben muss, damit der

System-AGB

Begriff	Definition
	Auftraggeber die Abnahme erklären kann. Dazu gehört insbesondere, dass der Auftragnehmer das Gesamtsystem bereits zum Termin der Erklärung der Betriebsbereitschaft* vertragsgemäß und im Wesentlichen mangelfrei bereitstellt, damit der Auftraggeber in der Zeit bis zum Vertragserfüllungstermin die Funktionsprüfung durchführen kann.
Vorbestehende Teile	Alle Bestandteile • der Individualsoftware* und • der auf der Quellcodeebene vorgenommenen, jedoch nicht gemäß Ziffer 2.3.1.3 in den Standard aufgenommenen Anpassungen an Standardsoftware*, die der Auftragnehmer oder ein Dritter unabhängig von diesem Vertrag entwickelt hat.
V-Modell XT	Das V-Modell XT ist ein Vorgehensmodell zum Planen und Durchführen von Projekten. Einzelheiten unter www.cio.bund.de .
Werkzeug	Hilfsmittel für die Entwicklung, Bearbeitung und Pflege von Software*.
Wiederherstellungszeit	Zeitraum, innerhalb dessen der Auftragnehmer die Störungs- bzw. Mängel- behebungsarbeiten erfolgreich abzuschließen hat. Der Zeitraum beginnt mit dem Zugang der Störungs- bzw. Mängelmeldung und läuft ausschließlich während der vereinbarten Servicezeiten.

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen dem

Universitätsklinikum Frankfurt (Anstalt des öffentlichen Rechts),

vertreten durch den Vorstand

Theodor - Stern - Kai 7

60590 Frankfurt am Main

Ausführende Stellen, Verantwortliche nach Art. 4 DS-GVO

- Verantwortliche - nachstehend Auftraggeber genannt -

und dem/der

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

Präambel

Die Parteien sind sich über die Bedeutung des Schutzes des Persönlichkeitsrechts beim Umgang mit personenbezogenen Daten bewusst und ihnen sind die dazu bestehenden rechtlichen, insbesondere datenschutzrechtlichen Vorschriften bekannt. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien, die sich aus bestehenden oder künftigen Verträgen über Lieferungen und Leistungen ergeben, soweit diese eine Verarbeitung von personenbezogenen Daten des Auftraggebers oder seiner Patienten, insbesondere im Sinne der Datenschutzgrundverordnung (DS-GVO), durch den Auftragnehmer zum Gegenstand haben.

Inhalt

Präambel	2
1. Gegenstand und Dauer des Auftrags	3
2. Konkretisierung des Auftragsinhalts	3
3. Technisch-organisatorische Maßnahmen	4
4. Berichtigung, Einschränkung und Löschung von Daten	4
5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers	5
6. Unterauftragsverhältnisse	6
7. Kontrollrechte des Auftraggebers	7
8. Mitteilung bei Verstößen des Auftragnehmers	7
9. Weisungsbefugnis des Auftraggebers	8
10. Löschung und Rückgabe von personenbezogenen Daten	8
11. Informationspflichten, Schriftformklausel	8
12. Verpflichtung zur Geheimhaltung von Berufsgeheimnissen (§ 203 StGB)	9
13. Haftung	10
14. Salvatorische Klausel	10
15. Rechtswahl, Gerichtsstand	10
Anlage 1 – Technisch-organisatorische Maßnahmen nach Art. 25	Fehler! Textmarke nicht definiert.
Anlage 2 – Kontaktdaten des Auftragnehmers	14
1. Datenschutzbeauftragte(r)	14
2. Ansprechpartner (wenn kein(e) Datenschutzbeauftragte(r) erforderlich ist)	14
3. ständiger Vertreter gemäß Art. 27 DS-GVO	14
Anlage 3 – Liste der Unterauftragnehmer des Auftragnehmers	15
Anlage 4 – Weisungsberechtigte Personen	16
1. beim Auftraggeber	16
2. beim Auftragnehmer	16

1. Gegenstand und Dauer des Auftrags

- (1) Gegenstand
- Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:für das Universitätsklinikum Frankfurt
- (2) Dauer

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist gemäß Hauptbeauftragung gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

- Auftragsinhalt ist die Durchführung von: für das Universitätsklinikum Frankfurt.
- (1) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):

- ☐ Patientendaten / Personenstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Adressdaten
- ☐ Gesundheitsdaten
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Interessenten
- ☐ Besucher
- ☐ Bewerber
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben
(von Dritten, z.B. Auskunftsteilen, oder aus öffentlichen Verzeichnissen)
- ☐

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Patienten
- ☐ Spender
- ☐ Interessenten
- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐ Abonnenten
- ☐

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung, sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [**Anlage 1**].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer

wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Der Auftragnehmer unterstützt angesichts der Art der Verarbeitung den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DS-GVO genannten Rechte der betroffenen Person nachzukommen.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) ☐ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt.
- ☐ Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
- ☐ Als Datenschutzbeauftragte(r) ist beim Auftragnehmer bestellt: **[Anlage 2]**. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
- ☐ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
- b) ☐ oder: Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird benannt: **[Anlage 2]**.
- c) ☐ oder: Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union: **[Anlage 2]**.
- d) ☒ Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- e) ☒ Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen ist gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO **[Anlage 1]** sicherzustellen.
- f) ☒ Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- g) ☒ Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits-

oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

- h) ☒ Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- i) ☒ Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse, sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- j) ☒ Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers, auch bei ausgelagerten Nebenleistungen, angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) wie folgt beauftragen:

- ☐ Eine Unterbeauftragung ist unzulässig
- ☐ nach vorheriger ausdrücklicher schriftlicher Zustimmung des Auftraggebers
- ☐ Der Auftraggeber stimmt der Beauftragung der Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO.
[Anlage 3]

(3) Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und der Auftraggeber nicht innerhalb einer Frist von 14 Tagen, gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(4) Die Weitergabe von personenbezogenen Daten des Auftragnehmers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(5) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen. Eine weitere Auslagerung durch den Unterauftragnehmer

- ☐ ist nicht gestattet;
- ☐ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);
- ☐ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch (optional durch Auftragnehmer zu belegen):

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artt. 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

- b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
- e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer wird Daten des Auftraggebers nur zur Erfüllung der vertraglich vereinbarten Leistungen und nach Weisung des Auftraggebers verarbeiten. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Weisungsberechtigte Personen des Auftraggebers sind in der **[Anlage 4]** benannt und sind mit den weisungsberechtigten Personen des Auftragnehmers zu vervollständigen.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Informationspflichten, Schriftformklausel

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Daten beim Auftraggeber liegt.

(2) Es gelten ausschließlich diese Bedingungen; Nebenabreden, Änderungen oder Ergänzungen dieser Bedingungen bedürfen für Ihre Wirksamkeit der Schriftform. Dieses gilt auch für die Abbedingung der Schriftformklausel.

12. Verpflichtung zur Geheimhaltung von Berufsgeheimnissen (§ 203 StGB)

(1) Im Rahmen dieses Auftrages werden auch Daten verarbeitet, die unter ein Berufsgeheimnis (im Sinne von § 203 StGB) fallen.

Der Auftragnehmer verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist.

Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, strafbar machen nach § 203 Abs. 4 S. 1 StGB.

Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Geheimnis offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

(2) Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggebers befassten Beschäftigten und andere für den Auftragnehmer tätigen Personen (z.B. Subunternehmer), die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar macht, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Geheimnis offenbart, und die mitwirkende Person nicht dafür Sorge getragen hat, dass die weitere mitwirkende Person zur Geheimhaltung verpflichtet wurde

(3) Der Auftragnehmer wird darauf hingewiesen, dass Daten, die er im Auftrag eines Berufsgeheimnisträgers verarbeitet u.U. dem Zeugnisverweigerungsrecht von sogenannten mitwirkenden Personen unterliegt (§ 53a Strafprozessordnung (StPO)). Entsprechend § 53a StPO entscheidet jedoch der Berufsgeheimnisträger über die Ausübung des Schweigerechts. Im Falle einer Befragung wird der Auftragnehmer unter Hinweis auf § 53a StPO dieser widersprechen und unverzüglich den Auftraggeber informieren, der daraufhin bzgl. der Wahrnehmung des Schweigerechts entscheidet.

(4) Der Auftragnehmer wird darauf hingewiesen, dass die sich in seinem Gewahrsam befindenden Geheimnisschutzdaten dem Beschlagnahmeverbot gemäß § 97 Abs. 2 StPO unterliegen. Die Daten dürfen nicht ohne das Einverständnis des Auftraggebers (Berufsgeheimnisträger) herausgegeben werden. Im Falle einer Beschlagnahme wird der Auftragnehmer dieser widersprechen und unverzüglich den Auftraggeber informieren.

13. Haftung

Die Haftung richtet sich nach den allgemeinen Gesetzen insbesondere nach Artikel 82 DS-GVO.

14. Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Vertrages ganz oder teilweise unwirksam oder unanwendbar sein oder werden, oder sollte sich in dem Vertrag eine Lücke befinden, so soll hierdurch die Gültigkeit der übrigen Bestimmungen nicht berührt werden. Anstelle der unwirksamen oder unanwendbaren Bestimmung oder zur Ausfüllung der Lücke soll eine angemessene Regelung treten, die, soweit rechtlich möglich, dem am nächsten kommt, was die Vertragsparteien gewollt haben oder nach dem Sinn und Zweck dieses Vertrages gewollt haben würden, wenn sie den Punkt bedacht hätten.

15. Rechtswahl, Gerichtsstand

Für etwaige Streitigkeiten aus den Verträgen oder damit im Zusammenhang stehenden Rechtsbeziehungen wird Frankfurt als Gerichtsstand vereinbart.

Für den Auftraggeber:

Name, Funktion:

Ort, Datum, Unterschrift:

Für den Auftragnehmer:

Name, Funktion: (*mindestens ppa.*)

Ort, Datum, Unterschrift:

Universitätsklinikum Frankfurt

Anlage 1 – Technisch-organisatorische Maßnahmen nach Art. 32 DSGVO

Diese Anlage ergänzt den Vertrag zwischen dem Auftraggeber und dem Auftragnehmer. Ziel dieser Anlage ist die Festlegung und Einhaltung technischer und organisatorischer Maßnahmen (TOMs) nach dem aktuellen Stand der Technik, zum Schutz personenbezogener Daten und insbesondere zum Schutz besonders schutzwürdiger personenbezogener Daten, gemäß den geltenden Datenschutzgesetzen. Es handelt sich hierbei um Mindestanforderungen, die in jedem Fall mindestens vorliegen müssen. Technische- und organisatorische Maßnahmen die über die hier genannten hinausgehen bzw. im Rahmen der angegebenen Services näher spezifiziert werden sind beizufügen. Erweiterungen der Maßnahmen die dem Schutz der personenbezogenen Daten dienen und diese nicht gefährden, können zu jedem Zeitpunkt in einvernehmlicher Rücksprache eingesetzt werden.

1. Technische Maßnahmen:

1.1 Verschlüsselung:

- **Datenverschlüsselung:** Alle besonders schutzwürdigen personenbezogenen Daten müssen sowohl bei der Übertragung als auch bei der Speicherung mittels starker Verschlüsselungsverfahren (z.B. AES-256) geschützt werden.
- **Schlüsselspeicherung:** Verschlüsselungsschlüssel müssen sicher gespeichert und verwaltet werden.

1.2 Transportverschlüsselung:

- **TLS/SSL:** Alle Datenübertragungen müssen mindestens durch TLS (Transport Layer Security) in der aktuellen Version (z.B. TLS 1.3 oder höher) geschützt werden. Auf eigenes Risiko des Auftragnehmers kann auch TLS 1.2 verwendet werden. Der Auftragnehmer übernimmt hierbei das Risiko.
- **VPN:** Bei der Übertragung über unsichere Netzwerke ist der Einsatz von Virtual Private Networks (VPNs) erforderlich.
- **End-to-End-Verschlüsselung:** Bei besonders schutzwürdigen personenbezogenen Daten ist eine End-to-End-Verschlüsselung zu implementieren, um sicherzustellen, dass Daten nur von autorisierten Endpunkten entschlüsselt werden können.
- **E-Mail-Verschlüsselung:** E-Mails, die besonders schutzwürdige personenbezogenen Daten enthalten, müssen z.B. mit S/MIME oder PGP verschlüsselt werden.

1.3 Zutrittskontrolle:

- Physische Zugangskontrollen zu den Räumlichkeiten, in denen besonders schutzwürdige personenbezogenen Daten verarbeitet werden, z.B. durch elektronische Zugangssysteme, Sicherheitspersonal, Videoüberwachung.
- Protokollierung aller Zutrittsaktivitäten.

1.4 Zugangskontrolle:

- Implementierung von Multi-Faktor-Authentifizierung (MFA), insbesondere für den Zugang zu besonders schutzwürdigen personenbezogene Daten und zentraler Rechnerstruktur.
- Verwendung von rollenbasierter Berechtigungsvergabe zur Sicherstellung, dass nur autorisierte Personen Zugriff auf personenbezogene Daten haben.
- Regelmäßige Überprüfung und Aktualisierung von Benutzerrechten.
- Sachkundiger Einsatz von Schutzprogrammen (u.a. Virens Scanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).

1.5 Zugriffskontrolle:

- Implementierung von Mechanismen zur Protokollierung und Überwachung von Zugriffen auf besonders schutzwürdige personenbezogene Daten.

1.6 Trennungskontrolle

- Einzelne Mandanten sind streng voneinander physisch und/oder logisch getrennt.
- Daten, auf die sich diese Zusatzvereinbarung bezieht, werden physisch und/oder logisch von anderen Daten getrennt gespeichert.
- Die Datensicherung (Backups) erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.

1.7 Datensicherung:

- Regelmäßige, automatisierte Backups.
- Backup- und Recovery-Konzept ist vorhanden und wird regelmäßig getestet.
- Sicherstellung, dass Backups ebenfalls verschlüsselt und sicher gespeichert werden.

1.8 Standards für Rechenzentren:

- Rechenzentren sollten mindestens die Anforderungen der ISO 27001 erfüllen.
- Rechenzentren sollten idealerweise auch die ISO 27701 erfüllen.
- Cloudservices von Rechenzentren sollten idealerweise auch die C5-Kriterien erfüllen.
- Physische Sicherheitsmaßnahmen wie u.a. Zugangskontrollen, Videoüberwachung und Brandschutzsysteme müssen implementiert sein.

2. Organisatorische Maßnahmen:

2.1 Schulung und Sensibilisierung:

- Regelmäßige Schulungen und Sensibilisierungsmaßnahmen für alle Mitarbeiter, die mit personenbezogenen Daten arbeiten, insbesondere, wenn sie mit besonders schutzwürdigen personenbezogenen Daten arbeiten.
- Dokumentation und Nachverfolgung der Teilnahme an Schulungen.

2.2 Vertraulichkeitserklärungen:

- Alle Mitarbeiter des Auftragnehmers, die Zugang zu besonders schutzwürdigen personenbezogenen Daten haben, müssen Vertraulichkeitserklärungen/Verschwiegenheitserklärungen unterzeichnen, insbesondere mit Bezug auf §203 StGB.

2.3 Datenschutzmanagement:

- Ernennung eines Datenschutzbeauftragten, der für die Einhaltung der Datenschutzbestimmungen und die Umsetzung dieser Vereinbarung verantwortlich ist.
- Durchführung regelmäßiger Datenschutz-Audits und Risikoanalysen.
- Vorhandensein eines Datenschutzmanagements, sowie mindestens gängiger Richtlinien und Policies der Informationssicherheit

2.4 Vorfallmanagement:

- Implementierung eines Verfahrens zur Erkennung, Meldung und Behandlung von Sicherheitsvorfällen.
- Verpflichtung zur unverzüglichen Benachrichtigung des Auftraggebers im Falle eines Datenschutzvorfalls.

2.5 Unterauftragnehmer:

- Eine Liste der aktuellen Unterauftragnehmer ist im Rahmen des AV-Vertrags aufzuführen.
- Der Auftragnehmer ist verpflichtet, vor der Einschaltung von Unterauftragnehmern Rücksprache mit dem Auftraggeber zu halten.
- Sicherstellung, dass Unterauftragnehmer die gleichen Datenschutz- und Sicherheitsmaßnahmen einhalten wie in dieser Vereinbarung festgelegt.
- Regelmäßige Überprüfung der Datenschutzkonformität und Sicherheitsmaßnahmen der Unterauftragnehmer.

2.6 Datenträgerentsorgung:

- Datenschutzkonforme Löschung/Vernichtung von Daten bzw. Datenträgern und Dokumenten entsprechend der Sicherheitsstufe der Daten, z.B. durch physische Zerstörung oder sichere Datenlöschung (vgl. DIN 66399, ISO/IEC 21964)
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.

Anlage 2 – Kontaktdaten des Auftragnehmers

1. Datenschutzbeauftragte(r)

Herr / Frau	
Name, Vorname	
Straße	
PLZ, Ort	
Telefon	
E-Mail-Adresse	

oder

2. Ansprechpartner (wenn kein(e) Datenschutzbeauftragte(r) erforderlich ist)

Herr / Frau	
Name, Vorname	
Straße	
PLZ, Ort	
Telefon	
E-Mail-Adresse	

oder

3. ständiger Vertreter gemäß Art. 27 DS-GVO

Herr / Frau	
Name, Vorname	
Straße	
PLZ, Ort	
Telefon	
E-Mail-Adresse	

Anlage 3 – Liste der Unterauftragnehmer des Auftragnehmers

Alternativ in freier Form zur Verfügung stellen.

Sollten keine Unterauftragnehmer im Einsatz sein, bitte diese Seite entwerten.

Firma Unterauftragnehmer	Anschrift/Land	Leistung

Anlage 4 – Weisungsberechtigte Personen

1. beim Auftraggeber

Als weisungsberechtigte Personen im Sinne dieser Vereinbarung gelten die jeweiligen hauptverantwortlichen Fachbereichsleiter*innen am Universitätsklinikum Frankfurt oder deren stellvertretenden Personen. Das Weisungsrecht beschränkt sich auf die Hauptvereinbarung oder SLA des jeweils verantwortlichen Fachbereichs am Universitätsklinikum Frankfurt im Sinne der DSGVO mit dem Auftragnehmer.

2. beim Auftragnehmer

Herr / Frau	
Name, Vorname	
Straße	
PLZ, Ort	
Telefon	
E-Mail-Adresse	



UNIVERSITÄTSKLINIKUM



CODE OF CONDUCT

für Lieferanten des
Universitätsklinikum Frankfurt



Markus Jones, Prof. Dr. Jürgen Graf, Birgit Roelfsema, Prof. Dr. Stefan Zeuzem (v.l.)

I. Einleitung

Als Maximalversorger in Deutschland, vor allem aber im Rhein/Main-Gebiet, ist sich das Universitätsklinikum seiner Verantwortung gegenüber seinen Patientinnen und Patienten, gegenüber seinen Beschäftigten und gegenüber seinem Umfeld, explizit der Umwelt bewusst. Das Universitätsklinikum Frankfurt bekennt sich zur Einhaltung der Menschenrechte und zum Schutz der Umwelt. Es ist das erklärte Ziel der Unternehmensleitung, die Menschenrechte und die Umwelt entlang der gesamten Wertschöpfungskette zu achten, zu schützen und zu fördern.

Ebenso erwarten wir die Einhaltung der Menschenrechte und umweltbezogener Schutzpflichten von unseren Lieferanten.

Dieser Lieferanten Code of Conduct stützt sich auf nationale Gesetze und Vorgaben sowie auf internationale Übereinkommen.

Prof. Dr. Jürgen Graf
*Ärztlicher Direktor und
Vorstandsvorsitzender*

Markus Jones
*Kaufmännischer Direktor und
stellvertretender Vorstandsvorsitzender*

Birgit Roelfsema
Pflegedirektorin

Prof. Dr. Stefan Zeuzem
Dekan

INHALT

I. Einleitung	01
II. Anforderungen an Lieferanten des Universitätsklinikum Frankfurt	04
III. Anforderungen an Lieferanten des Universitätsklinikum Frankfurt	08
IV. Kenntnisnahme und Einverständnis des Lieferanten	08



II. Anforderungen an Lieferanten des Universitätsklinikum Frankfurt

1. Menschenrechtsbezogene Verantwortung

1.1 Menschenrechte



Der Lieferant respektiert die persönliche Würde, Privatsphäre und die Menschenrechte eines jeden. Auf den Schutz der international anerkannten Menschenrechte ist angemessen hinzuwirken. Die Mitwirkung an Menschenrechtsverletzung ist durch den Lieferanten zu verhindern.

1.2 Verbot von Kinderarbeit



In keiner Phase der Produktion darf Kinderarbeit eingesetzt werden. Die Lieferanten sind aufgefordert, sich an die Empfehlungen aus den ILO-Konventionen zum Mindestalter für die Beschäftigung von Kindern zu halten. Demnach soll das Alter nicht geringer sein als das Alter, mit dem die allgemeine Schulpflicht endet und in jedem Fall nicht unter 15 Jahre.

1.3 Ausschluss von Zwangsarbeit



Es darf keine Zwangsarbeit, Sklavenarbeit oder derart vergleichbare Arbeit eingesetzt werden. Jede Arbeit muss freiwillig sein und die Mitarbeitenden müssen jederzeit die Arbeit oder das Beschäftigungsverhältnis beenden können. Außerdem darf keine inakzeptable Behandlung von Arbeitskräften, wie etwas psychische Härte, sexuelle und persönliche Belästigung stattfinden.

1.4 Einhaltung von angemessenem Arbeits- und Gesundheitsschutz



Der Lieferant sorgt für angemessene Sicherheitsmaßnahmen zum wirksamen Schutz seiner Beschäftigten vor Unfällen, chemischen, biologischen und physikalischen Gefahren sowie Berufskrankheiten, einschließlich Mitarbeiterunterweisungen und persönlicher Schutzausrüstung. Der Lieferant identifiziert und verhindert



wirksam relevante Risiken und Notfallsituationen am Arbeitsplatz, in der öffentlichen Umgebung und in den vom Unternehmen zur Verfügung gestellten Wohnräumen und stellt geeignete Notfallpläne, regelmäßige Sicherheitsschulungen und Reaktionsverfahren sicher.

1.5 Einhaltung der Vereinigungsfreiheit / Koalitionsfreiheit



Der Lieferant respektiert das Recht der Arbeitskräfte auf Vereinigungsfreiheit, auf Beitritt zu Gewerkschaften, auf Anruf der Arbeitskräftevertretung oder auf Mitgliedschaft in Betriebsräten/Personalräten in Übereinstimmung mit den vor Ort geltenden Gesetzen. Den Arbeitskräften muss es möglich sein, mit der Unternehmensleitung offen und ohne Angst vor Repressalien oder Belästigung zu kommunizieren.

1.6 Gleichbehandlung in der Beschäftigung



Die Diskriminierung von Beschäftigten in jeglicher Form ist unzulässig. Dies gilt z.B. für Benachteiligungen aufgrund von Geschlecht, Rasse, Kaste, Hautfarbe, Behinderung, politischer Überzeugung, Herkunft, Religion, Alter, Schwangerschaft oder sexueller Orientierung. Die persönliche Würde, Privatsphäre und Persönlichkeitsrechte jedes Einzelnen werden respektiert. Der Lieferant fördert die Chancengleichheit am Arbeitsplatz und die Gleichbehandlung seiner Mitarbeiter unabhängig von Hautfarbe, Nationalität, sozialer Herkunft, möglicher Behinderung, sexueller Orientierung, politischer oder religiöser Überzeugung sowie Geschlecht und Alter.



1.7 Faire Entlohnung



Der Lieferant vergütet seine Beschäftigten angemessen und gewährleistet die Zahlung der gesetzlich festgelegten nationalen Mindestlöhne. Die Arbeitszeiten haben den geltenden Gesetzen oder den Branchenstandards zu entsprechen.

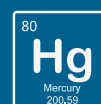
1.8 Schutz der natürlichen Lebensgrundlagen



Der Lieferant hat schädliche Bodenveränderungen, Gewässer- und Luftverunreinigungen, Lärmemissionen sowie übermäßiger Wasserverbrauch zu unterlassen, wenn dadurch die Gesundheit von Personen schädigt, die natürliche Grundlage zur Produktion von Nahrung erheblich beeinträchtigt wird oder der Zugang von Personen zu Trinkwasser bzw. Sanitäranlagen verhindert wird. Der Lieferant darf nicht unter Verstoß gegen legitime Rechte Land, Wälder oder Gewässer entziehen, deren Nutzung die Lebensgrundlage von Personen sichert.

2. Umweltschutzbezogene Verantwortung

2.1 Verbote im Kontext von Quecksilber



Die Verwendung von Quecksilber hat lediglich unter Beachtung der Verbote bzw. im Einklang mit dem Übereinkommen von Minamata in seiner aktuellen Fassung zu erfolgen.

2.2 Persistente organische Schadstoffe



Die Verwendung von persistenten organischen Schadstoffen hat lediglich unter Beachtung der Verbote bzw. im Einklang mit dem Stockholmer Übereinkommen in seiner aktuellen Fassung zu erfolgen.

2.3 Gefahrenabfall und Abfallentsorgung



Im Zusammenhang mit Festabfall hat der Lieferant einer systematischen Herangehensweise zu folgen was die Ermittlung, die Handhabung, Reduktion, verantwortungsvolle Entsorgungen bzw. Recycling dessen anbelangt. Des Weiteren sind entsprechende Verbote hinsichtlich der Ausfuhr von gefährlichen Abfällen gemäß des Basler Übereinkommen in seiner aktuellen Fassung zu beachten. Chemikalien und weitere Materialien, welche im Falle von Freisetzung in die Umwelt eine Gefahr mit sich ziehen, sind in solcher Weise zu ermitteln bzw. zu handhaben, dass die Sicherheit bei Umgang mit diesen Stoffen (Beförderung, Lagerung, Nutzung, Recycling, Wiederverwendung oder Entsorgung) gewährleistet ist.



3. Compliance & ethisches Verhalten

3.1 Integrität / Anti-Korruption



Der Lieferant wirkt stets darauf hin, dass bei allen Geschäftsaktivitäten angemessene Integritätsstandards zugrunde gelegt werden. Der Lieferant duldet keine Art von Korruption, Bestechung oder Erpressung, noch beteiligt er sich daran. Verfahren zur Prävention, Überwachung und letztlich zu Durchsetzung der anwendbaren Normen sind zu implementieren, um die Einhaltung der entsprechenden Anti-Korruptions-Gesetzgebung zu gewährleisten.

3.2 Datenschutz/ Vertraulichkeit



Der Lieferant verwaltet und schützt alle bei ihm liegende personenbezogenen Daten in Übereinstimmung mit der geltenden Rechtsordnung, insb. der europäischen Datenschutzgrundverordnung (DSGVO). Des Weiteren achtet der Lieferant die Vertraulichkeit von Geschäftsinformationen anderer und schützt entsprechende Rechte. Rechte an geistigem Eigentum sind zu respektieren. Technologie- und Wissenstransfer haben so zu erfolgen, dass die geistigen Eigentumsrechte sowie Kunden-/Patienteninformationen stets geschützt sind.

3.3 Fairer Wettbewerb



Die Regeln für einen fairen Wettbewerb sind unabdingbare Voraussetzung für eine leistungsorientierte Marktwirtschaft, um wirtschaftliche Effizienz, Entwicklung und Innovationen zu fördern. Daher achtet und fördert der Lieferant den fairen Wettbewerb und agiert in Übereinstimmung mit allen geltenden Wettbewerbs- bzw. Kartellgesetzen.

III. Anforderungen an Lieferanten des Universitätsklinikum Frankfurt

Das Universitätsklinikum Frankfurt behält sich entsprechend § 6 Abs. 4 Nr. 4 LkSG vor, in begründeten Fällen beim Lieferanten angemessene risikobasierte Kontrollmaßnahmen hinsichtlich der Einhaltung aller anwendbaren Gesetze und Rechtsvorschriften, einschließlich dieses Code of Conduct für Lieferanten, durchzuführen. Gegenüber Lieferanten, welche die obenstehenden Anforderungen/ Sorgfaltspflichten/ Verbote nicht beachten, behält sich das Universitätsklinikum Frankfurt vor, geeignete Maßnahmen zu ergreifen, welche letztlich auch zu einem Aussetzen oder Beenden der Lieferbeziehung führen können.

IV. Kenntnisnahme und Einverständnis des Lieferanten

Ein Lieferant des Universitätsklinikum Frankfurt verpflichtet sich, mit der Annahme und Umsetzung des Vertrages, entsprechend der in diesem Dokument aufgeführten Aspekte, verantwortungsvoll zu handeln sowie die enthaltenen Anforderungen einzuhalten.



Verfahren: 20261023 - Security Managed Services

EIGNUNGSKRITERIEN

1 Hinweis zum Wettbewerbsregister

Ab einer Auftragssumme von 30.000 Euro wird der Auftraggeber von den Bewerbern, welche zur Angebotsabgabe aufgefordert werden sollen bzw. von dem Bieter, auf dessen Angebot der Zuschlag erteilt werden soll, einen Auszug aus dem Wettbewerbsregister gem. Wettbewerbsregistergesetz beim Bundeskartellamt anfordern.

2 Wichtige Hinweise zu den Eignungskriterien [Mussangabe]

Der Auftraggeber hat öffentliche Aufträge an fachkundige und leistungsfähige (geeignete) Unternehmen zu vergeben (§ 122 GWB und § 31 UVgO).

Ein Unternehmen (Bewerber/Bieter/Unterauftragnehmer) ist geeignet, wenn die im Nachfolgenden festgelegten Kriterien im Hinblick auf die Befähigung und Erlaubnis der Berufsausübung, wirtschaftliche und finanzielle Leistungsfähigkeit sowie technische und berufliche Leistungsfähigkeit erfüllt bzw. beantwortet sind.

Als vorläufigen Beleg der Eignung eines Unternehmens hat der Auftraggeber grundsätzlich die Vorlage von Eigenerklärungen zu akzeptieren (§ 48 Abs. 2 VgV und § 35 Abs. 2 UVgO). Die Eigenerklärungen werden durch Beantwortung des Kriterienkatalogs abgegeben. Dabei ist folgendes zu beachten:

- Ausschlusskriterien (K.O.-Kriterium: Ja) müssen erfüllt werden. Angebote, die ein oder mehrere Ausschlusskriterien nicht erfüllen (Fragen mit "Nein" beantwortet), werden ausgeschlossen.

- Pflichtangaben (Mussangabe) sind zwingend erforderliche Angaben. Fragen können auch mit "Nein" beantwortet werden, ohne dass dies zwingend zum Ausschluss des Angebotes führt. Angebote deren Angaben jedoch nicht erkennen lassen, dass das Unternehmen über die erforderliche Eignung für die ordnungsgemäße Ausführung des Auftrags verfügt, können gleichwohl ausgeschlossen werden.

- Falls mit Angebotsabgabe vom Unternehmen gesonderte Nachweise vorzulegen sind, wird darauf im Kriterium/in der Frage hingewiesen.

Der Auftraggeber behält sich das Recht vor, noch im Vergabeverfahren (vor Zuschlagserteilung) und auch während der Vertragslaufzeit aktuelle Nachweise, Bestätigungen und Bescheinigungen für die vom Unternehmen bzw. Auftragnehmer mit seinem Angebot abgegebenen Erklärungen unter einer Fristsetzung einzufordern. Eine wesentliche falsche Angabe der Erklärungen kann den Ausschluss von diesem und weiterer Vergabeverfahren zur Folge haben.

☐ Ich erkläre/Wir erklären, dass ich/wir die vorgenannten Hinweise zu den Eignungskriterien zur Kenntnis genommen haben.

Mehrere Antworten wählbar

3 Erklärungen zum Unternehmensprofil

Gewichtung: 0,00%

3.1 Bewerber-/Bieterstruktur [Mussangabe]

Ich/Wir beabsichtige/n am Vergabeverfahren als Einzelbewerber/-bieter teilzunehmen:

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

Nur eine Antwort wählbar

3.2 Bieter-/Arbeitsgemeinschaft [Mussangabe]

Ich/Wir beabsichtige/n als Bieter-/Arbeitsgemeinschaft am Vergabeverfahren teilzunehmen:
(Falls Ja, ist das Formblatt "Anlage EBG - Eigenerklärung zur Bietergemeinschaft" ausgefüllt mit dem Angebot einzureichen)

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

Nur eine Antwort wählbar

3.3 Unterauftragnehmer/Nachunternehmer [Mussangabe]

Ich/Wir beabsichtige/n zur Erfüllung des Auftrags Unterauftragnehmer bzw. Nachunternehmer einzusetzen:
(Falls Ja, ist das Formblatt "Anlage EN1-Eigenerklärung Nachunternehmerinsatz" und das Formblatt "Anlage EN2-Verpflichtungserklärung Nachunternehmer" mit dem Angebot einzureichen)

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

3.4 Eintragung im Berufs-/Handelsregister [Mussangabe]

Ich/Wir bin/sind im Berufs-/Handelsregister eingetragen:

(Hinweis: Auf Verlangen der Vergabestelle ist ein aktueller Handelsregisterauszug -nicht älter als sechs Monate- vom Unternehmen vorzulegen)

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

Nur eine Antwort wählbar

3.5 Angaben zum Berufs-/Handelsregistereintrag [Mussangabe]

Falls Ihr Unternehmen im öffentlichen Berufs-/Handelsregister eingetragen ist, sind die folgenden Angaben in der vorgegebenen Reihenfolge zu tätigen:

- Rechtsform des Unternehmens
- Registernummer
- Amtsgericht
- Sitz des Unternehmens (Straße Nr., PLZ, Ort)
- USt.ID-Nr.

3.6 informative Abfrage [Mussangabe]

Bitte geben Sie, in dieser Reihenfolge, an:

- Name der Ansprechperson im Unternehmen mit e-Mail Adresse und Telefonnummer
- E-Mail Adresse für Bestellaufträge
- Bank-Name
- IBAN
- ggf. SWIFT

3.7 KMU-Eigenschaft [Mussangabe]

Angabe für statistische Zwecke (VergStatVO)

Ich/Wir bin/sind ein kleines oder mittleres Unternehmen (KMU):

Hinweis: Ihr Unternehmen erfüllt die KMU-Eigenschaft, wenn weniger als 250 Personen beschäftigt sind und ein Jahresumsatz von höchstens 50 Mio. EUR oder eine Jahresbilanzsumme von höchstens 43 Mio. EUR erzielt wird.

- ☐ Keine Angabe (0)
☐ Kleinunternehmen (0)
☐ Kleines Unternehmen (0)
☐ Mittleres Unternehmen (0)
☐ Großes Unternehmen (kein KMU) (0)

Nur eine Antwort wählbar

4 Erklärungen zur Zuverlässigkeit, Fachkunde und Leistungsfähigkeit

Gewichtung: 100,00%

4.1 Verpflichtungserklärung Tariftreue und Mindestlohn [Mussangabe]

Verpflichtungserklärung zu Tariftreue und Mindestentgelt bei öffentlichen Aufträgen nach dem Hessischen Vergabe- und Tariftreuegesetz (HVTG) vom 19. Dezember 2014, GVBl. S. 354

Es wird darauf hingewiesen, dass sich die Verpflichtungserklärung zu Tariftreue und Mindestentgelt entsprechend den Vorgaben der §§ 4 und 6 des Hessischen Vergabe- und Tariftreuegesetzes (HVTG) zur Zahlung des Mindestlohns gemäß § 20 des Mindestlohngesetzes (MiLoG) bzw. des Tariflohns nach dem Arbeitnehmer-Entsendegesetz (AEntG) nicht auf Beschäftigte bezieht, die bei einem Bieter oder Nachunternehmer im EU-Ausland beschäftigt sind und die Leistung im EU-Ausland erbringen.

Ich/Wir erkläre/n:

1. Ich/wir nehme/n zur Kenntnis, dass ich/wir gemäß § 4 Abs. 1 HVTG die für mich/uns geltenden gesetzlichen, aufgrund eines Gesetzes festgesetzten und unmittelbar geltenden tarifvertraglichen Leistungen zu gewähren habe/n. Ich/wir nehme/n weiterhin zur Kenntnis, dass bei Vorliegen von Anhaltspunkten dafür, dass gegen diese Regelung verstoßen wird, auf Anforderung dem öffentlichen Auftraggeber oder dem Besteller die Einhaltung dieser Verpflichtung nachzuweisen ist.
2. Ich/wir verpflichte/n mich/uns, gemäß § 4 Abs. 2 HVTG meinen/unseren Beschäftigten bei der Ausführung der Leistung diejenigen Arbeitsbedingungen einschließlich des Entgelts zu gewähren, die nach Art und Höhe mindestens den Vorgaben desjenigen Tarifvertrags entsprechen, an den mein/unser Unternehmen aufgrund des AEntG gebunden ist.
3. Ich/wir verpflichte/n mich/uns, gemäß § 4 Abs. 3 und § 6 HVTG meinen/unseren Beschäftigten bei der Ausführung der Leistung ein Entgelt zu zahlen, das den Vorgaben des MiLoG entspricht. Im Falle der Auftragsausführung durch Nachunternehmer oder Verleihunternehmen sind im Angebot, soweit diese bereits bei Angebotsabgabe bekannt sind, spätestens jedoch vor Beginn der Ausführung der Leistung durch das Nachunternehmen oder Verleihunternehmen die entsprechenden Erklärungen in Textform abzugeben und vorzulegen.
 - Die Erklärung kann entfallen, soweit sie bereits in einem Präqualifizierungsregister hinterlegt ist.
 - Die Einhaltung der nach Bundesrecht oder aufgrund von Bundesrecht für mich/uns geltenden Regelungen von besonders festgesetzten Mindestentgelten (Mindestlohn) als Mindeststandard im Angebot entfällt, soweit nach § 4 HVTG Tariftreue gefordert werden kann und die danach maßgebliche tarifliche Regelung für die Beschäftigten günstiger ist als die für sie nach Bundesrecht geltenden Bestimmungen.
4. Ich/wir erkläre/n, dass ich/wir nicht wegen eines Verstoßes gegen § 21 MiLoG (Bußgeldvorschriften) mit einer Geldbuße von wenigstens 2.500 Euro belegt worden bin/sind und damit nicht die Voraussetzungen für einen Ausschluss von der Auftragsvergabe

nach § 19 Abs. 1 und 3 MiLoG vorliegen.

5. Ich/wir verpflichte/n mich/uns für den Fall der Ausführung vertraglich übernommener Leistungen durch Nachunternehmen, die Erfüllung der Verpflichtungen nach den §§ 4 und 6 HVTG durch die Nachunternehmen sicherzustellen und dem öffentlichen Auftraggeber Tariftreue- und sonstige Verpflichtungs- sowie Mindestlohnklärungen der Nachunternehmen nach Auftragserteilung, spätestens vor Beginn der Ausführung der Leistung durch das Nachunternehmen, vorzulegen. Gleiches gilt, wenn ich/wir oder ein beauftragtes Nachunternehmen zur Ausführung des Auftrags Arbeitskräfte eines Verleihunternehmens einsetze(n)/einsetzt. Diese Verpflichtung gilt entsprechend auch für alle weiteren Nachunternehmen und Verleihunternehmen.

☐ Ich/ Wir bestätige/n, dass vorstehende Angaben von meinem/ unserem Unternehmen bei der Angebotenen Leistung erfüllt sind.

Mehrere Antworten wählbar

4.2 Eigenerklärung bzgl. Sanktionen gegen Russland [Mussangabe]

Die nachfolgende Erklärung gebe/n ich/wir verbindlich ab (ggf. zugleich in Vertretung für die lt. Teilnahmeantrag / Angebot Vertretenen auch für diese):

1.Der / die Bewerber / Bieter gehört / gehören nicht zu den in Artikel 5 k) Absatz 1 der Verordnung (EU) Nr. 833/2014 in der Fassung des Art. 1 Ziff. 23 der Verordnung (EU) 2022/576 des Rates vom 8. April 2022 über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren, genannten Personen oder Unternehmen, die einen Bezug zu Russland im Sinne der Vorschrift aufweisen,

a)durch die russische Staatsangehörigkeit des Bewerbers/Bieters oder die Niederlassung des Bewerbers/Bieters in Russland,

b)durch die Beteiligung einer natürlichen Person oder eines Unternehmens, auf die eines der Kriterien nach Buchstabe a zutrifft, am Bewerber/Bieter über das Halten von Anteilen im Umfang von mehr als 50%,

c)durch das Handeln der Bewerber/Bieter im Namen oder auf Anweisung von Personen oder Unternehmen, auf die die Kriterien der Buchstaben a und/oder b zutrifft.

2.Die am Auftrag als Unterauftragnehmer, Lieferanten oder Unternehmen, deren Kapazitäten im Zusammenhang mit der Erbringung des Eignungsnachweises in Anspruch genommen werden, beteiligten Unternehmen, auf die mehr als 10 % des Auftragswerts entfällt, gehören ebenfalls nicht zu dem in der Vorschrift genannten Personenkreis mit einem Bezug zu Russland im Sinne der Vorschrift.

3.Es wird bestätigt und sichergestellt, dass auch während der Vertragslaufzeit keine als Unterauftragnehmer, Lieferanten oder Unternehmen, deren Kapazitäten im Zusammenhang mit der Erbringung des Eignungsnachweises in Anspruch genommen werden, beteiligten Unternehmen eingesetzt werden, auf die mehr als 10 % des Auftragswerts entfällt.

☐ Ich/ wir bestätigt, dass das auf mein/ unser Unternehmen zutrifft.

Mehrere Antworten wählbar

4.3 Artikel 5k der Verordnung (EU) Nr. 833/2014

Artikel 5k der Verordnung (EU) Nr. 833/2014 in der Fassung des Art. 1 Ziff. 23 der Verordnung (EU) 2022/576 des Rates vom 8. April 2022 lautet wie folgt:

(1)Es ist verboten, öffentliche Aufträge oder Konzessionen, die in den Anwendungsbereich der Richtlinien über die öffentliche Auftragsvergabe sowie unter Artikel 10 Absatz 1, Absatz 3, Absatz 6 Buchstaben a bis e, Absatz 8, Absatz 9 und Absatz 10 und die Artikel 11, 12, 13 und 14 der Richtlinie 2014/23/EU, unter die Artikel 7 und 8, Artikel 10 Buchstaben b bis f und h bis j der Richtlinie 2014/24/EU, unter Artikel 18, Artikel 21 Buchstaben b bis e und g bis i, Artikel 29 und Artikel 30 der Richtlinie 2014/25/EU und unter Artikel 13 Buchstaben a bis d, f bis h und j der Richtlinie 2009/81/EG fallen, an folgende Personen, Organisationen oder Einrichtungen zu vergeben bzw. Verträge mit solchen Personen, Organisationen oder Einrichtungen weiterhin zu erfüllen:

a)russische Staatsangehörige oder in Russland niedergelassene natürliche oder juristische Personen, Organisationen oder Einrichtungen,

b)juristische Personen, Organisationen oder Einrichtungen, deren Anteile zu über 50 % unmittelbar oder mittelbar von einer der unter Buchstabe a genannten Organisationen gehalten werden, oder

c)natürliche oder juristische Personen, Organisationen oder Einrichtungen, die im Namen oder auf Anweisung einer der unter Buchstabe a oder b genannten Organisationen handeln,

auch solche, auf die mehr als 10 % des Auftragswerts entfällt, Unterauftragnehmer, Lieferanten oder Unternehmen, deren Kapazitäten im Sinne der Richtlinien über die öffentliche Auftragsvergabe in Anspruch genommen werden.

(2)Abweichend von Absatz 1 können die zuständigen Behörden die Vergabe oder die Fortsetzung der Erfüllung von Verträgen genehmigen, die bestimmt sind für

a)den Betrieb ziviler nuklearer Kapazitäten, ihre Instandhaltung, ihre Stilllegung, die Entsorgung ihrer radioaktiven Abfälle, ihre Versorgung mit und die Wiederaufbereitung von Brennelementen und die Weiterführung der Planung, des Baus und die Abnahmetests für die Indienstellung ziviler Atomanlagen und ihre Sicherheit sowie die Lieferung von Ausgangsstoffen zur Herstellung medizinischer Radioisotope und ähnlicher medizinischer Anwendungen, kritischer Technologien zur radiologischen Umweltüberwachung sowie für die zivile nukleare Zusammenarbeit, insbesondere im Bereich Forschung und Entwicklung,

b)die zwischenstaatliche Zusammenarbeit bei Raumfahrtprogrammen,

c)die Bereitstellung unbedingt notwendiger Güter oder Dienstleistungen, wenn sie ausschließlich oder nur in ausreichender Menge von den in Absatz 1 genannten Personen bereitgestellt werden können,

d)die Tätigkeit der diplomatischen und konsularischen Vertretungen der Union und der Mitgliedstaaten in Russland, einschließlich Delegationen, Botschaften und Missionen, oder internationaler Organisationen in Russland, die nach dem Völkerrecht Immunität genießen.

e)den Kauf, die Einfuhr oder die Beförderung von Erdgas und Erdöl, einschließlich raffinierter Erdölerzeugnisse, sowie von Titan, Aluminium, Kupfer, Nickel, Palladium und Eisenerz aus oder durch Russland in die Union, oder

f)den Kauf, die Einfuhr oder die Beförderung von Kohle und anderen festen fossilen Brennstoffen, die in Anhang XXII aufgeführt sind, bis 10. August 2022.

(3)Der betreffende Mitgliedstaat unterrichtet die anderen Mitgliedstaaten und die Kommission über jede nach diesem Artikel erteilte Genehmigung innerhalb von zwei Wochen nach deren Erteilung.

(4)Die Verbote gemäß Absatz 1 gelten nicht für die Erfüllung — bis zum 10. Oktober 2022 — von Verträgen, die vor dem 9. April 2022 geschlossen wurden.

4.4 Berufsgenossenschaft [Mussangabe]

Ich/Wir bin/sind Mitglied der Berufsgenossenschaft:

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

Nur eine Antwort wählbar

4.5 Insolvenz und Liquidation [Mussangabe]

Ich/Wir erkläre/n, dass ein Insolvenzverfahren oder ein vergleichbares gesetzlich geregeltes Verfahren weder beantragt noch eröffnet wurde, ein Antrag auf Eröffnung nicht mangels Masse abgelehnt wurde und sich mein/unser Unternehmen nicht in Liquidation befindet.

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

Nur eine Antwort wählbar

4.6 Strafrechtliche Ermittlungen [Mussangabe]

Ich/Wir erkläre/n, dass keine aktuellen strafrechtlichen Ermittlungen gegen Mitglieder der Geschäftsleitung/Objektleitung anhängig sind.

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

Nur eine Antwort wählbar

4.7 Steuern, Abgaben und Sozialbeiträge [Mussangabe]

Ich/Wir erkläre/n, dass ich/wir meine/unsere Verpflichtung zur Zahlung von Steuern und Abgaben sowie der Beiträge zur gesetzlichen Sozialversicherung, soweit sie der Pflicht zur Beitragszahlung unterfallen, ordnungsgemäß erfüllt habe/n.

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

Nur eine Antwort wählbar

4.8 Betriebs-/Berufshaftpflichtversicherung [Mussangabe]

Ich/Wir erkläre/n, dass ich/wir über eine Betriebs-/Berufshaftpflichtversicherung verfüge/n, die mindestens die nachstehenden Schäden mit folgenden Deckungssummen abdeckt:

- Für Personen-, Sach- und Vermögensschäden mindestens 2.500.000 EUR pauschal je Schadensfall einfach maximiert pro Jahr und ich/wir diese während der gesamten Vertragslaufzeit aufrechterhalten werde/n
- oder
- im Auftragsfalle eine entsprechende Versicherung abschließen werde/n bzw. eine entsprechende Anpassung der Versicherungsdeckungssumme vornehmen werde/n und ich/wir diese während der gesamten Vertragslaufzeit aufrechterhalten werde/n.

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

Nur eine Antwort wählbar

4.9 Nichtvorliegen von Ausschlussgründen (§ 123 GWB) [Mussangabe]

Ausschlusskriterium

Ich/Wir erkläre/n, dass keine der nach § 123 GWB genannten und nachfolgende abgedruckten Ausschlussgründe vorliegen:

Nach § 123 Abs. 1 GWB ist ein Unternehmen von der Teilnahme an einem Vergabeverfahren wegen Unzuverlässigkeit auszuschließen, wenn der Auftraggeber Kenntnis davon hat, dass eine Person, deren Verhalten dem Unternehmen zuzurechnen ist, rechtskräftig verurteilt ist wegen:

1. § 129 des Strafgesetzbuchs (Bildung krimineller Vereinigungen), § 129a des Strafgesetzbuchs (Bildung terroristischer Vereinigungen) oder § 129b des Strafgesetzbuchs (Kriminelle und terroristische Vereinigungen im Ausland),
2. § 89c des Strafgesetzbuchs (Terrorismusfinanzierung) oder wegen der Teilnahme an einer solchen Tat oder wegen der Bereitstellung oder Sammlung finanzieller Mittel in Kenntnis dessen, dass diese finanziellen Mittel ganz oder teilweise dazu verwendet werden oder verwendet werden sollen, eine Tat nach § 89a Absatz 2 Nummer 2 des Strafgesetzbuchs zu begehen,
3. § 261 des Strafgesetzbuchs (Geldwäsche),
4. § 263 des Strafgesetzbuchs (Betrug), soweit sich die Straftat gegen den Haushalt der Europäischen Union oder gegen Haushalte richtet, die von der Europäischen Union oder in ihrem Auftrag verwaltet werden,
5. § 264 des Strafgesetzbuchs (Subventionsbetrug), soweit sich die Straftat gegen den Haushalt der Europäischen Union oder gegen Haushalte richtet, die von der Europäischen Union oder in ihrem Auftrag verwaltet werden,
6. § 299 des Strafgesetzbuchs (Bestechlichkeit und Bestechung im geschäftlichen Verkehr), §§ 299a und 299b des Strafgesetzbuchs (Bestechlichkeit und Bestechung im Gesundheitswesen),
7. § 108e des Strafgesetzbuchs (Bestechlichkeit und Bestechung von Mandatsträgern) oder § 108f des Strafgesetzbuchs

(unzulässige Interessenwahrnehmung),
 8. den §§ 333 und 334 des Strafgesetzbuchs (Vorteilsgewährung und Bestechung), jeweils auch in Verbindung mit § 335a des Strafgesetzbuchs (Ausländische und internationale Bedienstete),
 9. Artikel 2 § 2 des Gesetzes zur Bekämpfung internationaler Bestechung (Bestechung ausländischer Abgeordneter im Zusammenhang mit internationalem Geschäftsverkehr) oder
 10. den §§ 232, 232a Absatz 1 bis 5, den §§ 232b bis 233a des Strafgesetzbuchs (Menschenhandel, Zwangsprostitution, Zwangsarbeit, Ausbeutung der Arbeitskraft, Ausbeutung unter Ausnutzung einer Freiheitsberaubung).

Einem Verstoß gegen diese Vorschriften gleichgesetzt sind Verstöße gegen entsprechende Strafnormen anderer Staaten. Ein Verhalten einer rechtskräftig verurteilten Person ist einem Unternehmen zuzurechnen, wenn sie für dieses Unternehmen bei der Führung der Geschäfte selbst verantwortlich gehandelt hat oder ein Aufsichts- oder Organisationsverschulden gemäß § 130 des Gesetzes über Ordnungswidrigkeiten (OWiG) einer Person im Hinblick auf das Verhalten einer anderen für das Unternehmen handelnden, rechtskräftig verurteilten Person vorliegt.

- ☐ Keine Angabe
☐ Ja
☐ Nein

Nur eine Antwort wählbar

4.10 Nichtvorliegen von Ausschlussgründen (§ 124 GWB) [Mussangabe]

Ich/Wir erkläre/n, dass keine der nach § 124 GWB genannten und nachfolgende abgedruckten Ausschlussgründe vorliegen:

Nach § 124 GWB können öffentliche Auftraggeber unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit ein Unternehmen zu jedem Zeitpunkt des Vergabeverfahrens von der Teilnahme an einem Vergabeverfahren ausschließen, wenn

1. das Unternehmen bei der Ausführung öffentlicher Aufträge nachweislich gegen geltende umwelt-, sozial- oder arbeitsrechtliche Verpflichtungen verstoßen hat,
2. das Unternehmen zahlungsunfähig ist, über das Vermögen des Unternehmens ein Insolvenzverfahren oder ein vergleichbares Verfahren beantragt oder eröffnet worden ist, die Eröffnung eines solchen Verfahrens mangels Masse abgelehnt worden ist, sich das Unternehmen im Verfahren der Liquidation befindet oder seine Tätigkeit eingestellt hat,
3. das Unternehmen im Rahmen der beruflichen Tätigkeit nachweislich eine schwere Verfehlung begangen hat, durch die die Integrität des Unternehmens infrage gestellt wird; § 123 Absatz 3 ist entsprechend anzuwenden,
4. der öffentliche Auftraggeber über hinreichende Anhaltspunkte dafür verfügt, dass das Unternehmen Vereinbarungen mit anderen Unternehmen getroffen hat, die eine Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs bezwecken oder bewirken,
5. ein Interessenkonflikt bei der Durchführung des Vergabeverfahrens besteht, der die Unparteilichkeit und Unabhängigkeit einer für den öffentlichen Auftraggeber tätigen Person bei der Durchführung des Vergabeverfahrens beeinträchtigen könnte und der durch andere, weniger einschneidende Maßnahmen nicht wirksam beseitigt werden kann,
6. eine Wettbewerbsverzerrung daraus resultiert, dass das Unternehmen bereits in die Vorbereitung des Vergabeverfahrens einbezogen war, und diese Wettbewerbsverzerrung nicht durch andere, weniger einschneidende Maßnahmen beseitigt werden kann,
7. das Unternehmen eine wesentliche Anforderung bei der Ausführung eines früheren öffentlichen Auftrags oder Konzessionsvertrags erheblich oder fortdauernd mangelhaft erfüllt hat und dies zu einer vorzeitigen Beendigung, zu Schadensersatz oder zu einer vergleichbaren Rechtsfolge geführt hat,
8. das Unternehmen in Bezug auf Ausschlussgründe oder Eignungskriterien eine schwerwiegende Täuschung begangen oder Auskünfte zurückgehalten hat oder nicht in der Lage ist, die erforderlichen Nachweise zu übermitteln, oder
9. das Unternehmen
 - a) versucht hat, die Entscheidungsfindung des öffentlichen Auftraggebers in unzulässiger Weise zu beeinflussen,
 - b) versucht hat, vertrauliche Informationen zu erhalten, durch die es unzulässige Vorteile beim Vergabeverfahren erlangen könnte, oder
 - c) fahrlässig oder vorsätzlich irreführende Informationen übermittelt hat, die die Vergabeentscheidung des öffentlichen Auftraggebers erheblich beeinflussen könnten, oder versucht hat, solche Informationen zu übermitteln.

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

Nur eine Antwort wählbar

4.11 Lieferkettensorgfaltspflichten gesetz [Mussangabe]

Wir erklären, dass uns keine Verstöße gegen menschrechtliche (gem. § 2 Abs. 2 Nr. 1-12 LkSG) und umweltbezogene Pflichten (gem. § 2 Abs. 3 Nr. 1-8 LkSG) innerhalb unseres Unternehmens und der Unternehmen unserer Zulieferer bekannt sind. Sollten wir Kenntnis darüber erlangen, dass in unserem Unternehmen oder in einem Unternehmen unserer Zulieferer eine Verletzung menschenrechtlicher oder umweltbezogener Pflichten stattfindet/stattgefunden hat, so werden wir das UKF hierüber unverzüglich informieren.

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

Nur eine Antwort wählbar

4.12 Abfragen zur Eignung

4.12.1 1. Vorbemerkungen

Dieses Dokument legt die Eignungsanforderungen für den Teilnahmewettbewerb im Vergabeverfahren Cybersecurity Managed Services des Universitätsklinikums Frankfurt (UKF) fest. Die Eignungsprüfung erfolgt vorgelagert zur Angebotswertung. Nur Bewerber, die sämtliche K.O.-Kriterien erfüllen, werden zur Angebotsabgabe zugelassen.

Die Eignungskriterien unterteilen sich in zwei Kategorien:

- K.O.-Kriterien (Typ A): Ausschlusskriterien. Nichterfüllung führt zum Ausschluss vom Verfahren.
- Bewertungskriterien (Typ B): Gehen in die qualitative Bewertung der Bewerbungsunterlagen ein; Nichterfüllung führt nicht zum Ausschluss, wirkt sich jedoch auf die Rangbildung im Teilnahmewettbewerb aus.

Alle Nachweise sind in Form der jeweils bezeichneten Dokumente, Zertifikate oder Eigenerklärungen mit dem Teilnahmeantrag einzureichen. Soweit Nachweise durch Eignungsleihe von Nachunternehmern erbracht werden, sind die Nachunternehmer und die

Art der Eignungsleihe explizit zu benennen.

Hinweise:

In der Phase des Teilnahmewettbewerbs sind keine Lösungskonzepte (vgl. Anlagen D3 + D4) einzureichen und keine Preise (vgl. Anlage D5) zu kalkulieren. Dies ist erst erforderlich, wenn die zugelassenen Teilnehmer zur Abgabe eines Angebotes aufgefordert werden. Gleiches gilt für den beiliegenden EVB-IT System sowie für die Anlage-AVV (Auftragsdatenverarbeitung) [jeweils blanko]. Sind mehr als 4 (vier) Teilnehmer geeignet, dann entscheidet die Summe der Punkte aus den Bewertungskriterien über die weitere Teilnahme. Das Verfahren wird mit den Rängen 1 – 4 (höchste Punktzahl absteigend) fortgesetzt. Haben mehrere Teilnehmer die gleiche Punktzahl erreicht, dann entscheidet das Los.

4.12.2 3. K.O.-Kriterien (Typ A) – Mindestanforderungen

Die nachfolgenden Kriterien sind Ausschlusskriterien. Bewerber, die ein oder mehrere Kriterien nicht erfüllen, werden vom weiteren Verfahren ausgeschlossen. Die Nichterfüllung kann nicht durch besondere Leistungen bei Bewertungskriterien (Typ B) kompensiert werden.

4.12.3 (1) ISO 27001 – Informationssicherheits-Maßnahmen [Mussangabe]

Der Bewerber verfügt über eine gültige Zertifizierung nach ISO/IEC 27001 in der aktuellen Normfassung. Der Nachweis kann mittels Eignungsleihe von einem an der Leistungserbringung beteiligten Nachunternehmer erbracht werden.

☐ Gültiges Zertifikat ist als Anlage hochgeladen!

Mehrere Antworten wählbar

4.12.4 (2) ISO 9001 – Qualitätsmanagementsystem [Mussangabe]

Der Bewerber verfügt über eine gültige Zertifizierung nach ISO 9001 in der aktuellen Normfassung. Der Nachweis kann mittels Eignungsleihe erbracht werden.

☐ Gültiges Zertifikat ist als Anlage hochgeladen!

Mehrere Antworten wählbar

4.12.5 (2a) ISO/IEC 20000-1 – IT-Service-Management-System [Mussangabe]

Gewichtung: 0,00%
Maximalpunktzahl: 10

Der Bewerber verfügt über eine gültige Zertifizierung nach ISO/IEC 20000-1 in der aktuellen Normfassung. Der Nachweis kann mittels Eignungsleihe erbracht werden, sofern der eignungsleihende Nachunternehmer an der Leistungserbringung beteiligt ist.

- ☐ Keine Angabe (0)
☐ Gültiges Zertifikat ist als Anlage hochgeladen! (10)
☐ Zertifikat nicht vorhanden. (0)

Nur eine Antwort wählbar

4.12.6 (3) BSI C5 Typ 2 – Cloud-Sicherheit [Mussangabe]

Die angebotene Gesamtlösung enthält Cloud-Bestandteile?

Antwort JA:

Der Bewerber oder der Cloud-Dienstleister muss über ein gültiges Testat nach BSI C5 Typ 2 verfügen. Der Nachweis ist verpflichtend, sofern die Lösung Cloud-basierte Verarbeitungen vorsieht.

Bitte Nachweis in der Anlage hochladen.

Antwort NEIN:

Bei reinen On-Premises-Lösungen entfällt dieses Kriterium.

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

Nur eine Antwort wählbar

4.12.7 (4) EU-Firmensitz und EU-Datenhoheit [Mussangabe]

Der Bewerber hat seinen Firmensitz innerhalb der Europäischen Union. Sämtliche im Rahmen der Leistungserbringung verarbeiteten und gespeicherten Daten werden ausschließlich innerhalb der Europäischen Union verarbeitet und gespeichert. Dies gilt auch für etwaige Sub-Auftragsverarbeitung.

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

Nur eine Antwort wählbar

4.12.8 (5) DSGVO-Konformität [Mussangabe]

Der Bewerber stellt sicher, dass alle angebotenen Leistungen vollständig DSGVO-konform erbracht werden und die einschlägigen nationalen sowie europäischen Datenschutz- und Sicherheitsanforderungen eingehalten werden.

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

Nur eine Antwort wählbar

4.12.9 (6) Deutschsprachiger SOC-Betrieb [Mussangabe]

Der SOC-Betrieb des Bewerbers muss vollständig in deutscher Sprache erfolgen. Sämtliche Kommunikations-, Eskalations- und Berichtspflichten gegenüber dem Auftraggeber sind in deutscher Sprache sicherzustellen.

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

Nur eine Antwort wählbar

4.12.10 (7) BSI-Qualifizierung APT-Response-Dienstleister [Mussangabe]

Gewichtung: 0,00%
Maximalpunktzahl: 10

Für den Nachweis einer BSI-Listung als qualifizierter APT-Response-Dienstleister oder eines gleichwertigen Befähigungsnachweises werden Punkte vergeben. Bewertet wird die nachgewiesene strukturierte Handlungsfähigkeit bei hochentwickelten Bedrohungen, APT-/Incident-Response-Lagen und vergleichbaren Cyberkrisen.

Der Nachweis kann durch den Bewerber selbst oder durch einen benannten, an der Leistungserbringung beteiligten Nachunternehmer im Wege der Eignungsleihe erbracht werden.

BSI-Listungsnachweis oder gleichwertiger Befähigungsnachweis
Bitte Nachweis in der Anlage hochladen!

- ☐ Keine Angabe (0)
☐ BSI-Listung als qualifizierter APT-Response-Dienstleister oder nachvollziehbar gleichwertiger Befähigungsnachweis (10)
☐ Kein Nachweis oder Gleichwertigkeit nicht nachvollziehbar belegt (0)

Nur eine Antwort wählbar

4.12.11 (8) Referenz 1 – SOC/MDR-Betrieb im KRITIS-KH [Mussangabe]

Der Bewerber weist mindestens eine Referenz über die Implementierung und den Betrieb eines Security Operations Centers (SOC) bzw. Managed Detection and Response Service (MDR)

- in einem KRITIS-Krankenhaus
- mit mindestens 1.000 Betten
- Der Service muss 24/7-Betrieb umfassen.

Es müssen folgende Angaben in der vorgegebenen Reihenfolge getätigt werden:

- Benennung Referenzauftraggeber (mit Name und Anschrift)
- Benennung Ansprechpartner (mit Name, Telefonnummer und E-Mail)
- Bezeichnung des Auftragsgegenstandes
- Anzahl vollstationäre Behandlungsfälle/Jahr
- Anzahl Betten
- Service umfasst 24/7 JA oder NEIN
- Ausführungszeitraum (von Datum bis Datum)

Ich/Wir erkläre/n mich/uns durch die Angabe der Referenz mit einer Nachfrage des Auftraggebers beim jeweiligen Referenzauftraggeber einverstanden. Die Einreichung einer Bescheinigung der Referenzauftraggeber ist daher nicht erforderlich.

4.12.12 (9a21) Referenz 2 – SOC/MDR-Betrieb Krankenhaus 1 [Mussangabe]

Für jede eingereichte Referenz über die Implementierung und den Betrieb eines SOC/MDR-Service in einem Krankenhaus werden Punkte vergeben.

- Krankenhaus mit mindestens 500 Betten; eine KRITIS-Einstufung ist nicht erforderlich.
- 24/7-SOC-Betrieb muss Teil der Referenzleistung sein.

Es müssen folgende Angaben in der vorgegebenen Reihenfolge getätigt werden:

- Krankenhaus 1
- Benennung Referenzauftraggeber (mit Name und Anschrift)
 - Benennung Ansprechpartner (mit Name, Telefonnummer und E-Mail)
 - Bezeichnung des Auftragsgegenstandes
 - Anzahl Betten
 - Service umfasst 24/7 JA oder NEIN
 - Ausführungszeitraum (von Datum bis Datum)

Ich/Wir erkläre/n mich/uns durch die Angabe der Referenz mit einer Nachfrage des Auftraggebers beim jeweiligen Referenzauftraggeber einverstanden. Die Einreichung einer Bescheinigung der Referenzauftraggeber ist daher nicht erforderlich.

4.12.13 (9b22) Referenz 2 – Bewertung SOC/MDR-Betrieb KH 1

Gewichtung: 0,00%
Maximalpunktzahl: 10

Für jede eingereichte Referenz über die Implementierung und den Betrieb eines SOC/MDR-Service in einem Krankenhaus werden Punkte vergeben.

- Krankenhaus mit mindestens 500 Betten; eine KRITIS-Einstufung ist nicht erforderlich.
- 24/7-SOC-Betrieb muss Teil der Referenzleistung sein.

Bewertung zu Referenz 2 - Krankenhaus 1

- [☐] Keine Angabe (0)
[☐] Referenz genügt den Kriterien (10)
[☐] Referenz genügt NICHT den Kriterien (0)

Nur eine Antwort wählbar

4.12.14 (9a31) Referenz 3 – SOC/MDR-Betrieb Krankenhaus 2 [Mussangabe]

Für jede eingereichte Referenz über die Implementierung und den Betrieb eines SOC/MDR-Service in einem Krankenhaus werden Punkte vergeben.

- Krankenhaus mit mindestens 500 Betten; eine KRITIS-Einstufung ist nicht erforderlich.
- 24/7-SOC-Betrieb muss Teil der Referenzleistung sein.

Es müssen folgende Angaben in der vorgegebenen Reihenfolge getätigt werden:

Krankenhaus 2

- Benennung Referenzauftraggeber (mit Name und Anschrift)
- Benennung Ansprechpartner (mit Name, Telefonnummer und E-Mail)
- Bezeichnung des Auftragsgegenstandes
- Anzahl Betten
- Service umfasst 24/7 JA oder NEIN
- Ausführungszeitraum (von Datum bis Datum)

Ich/Wir erkläre/n mich/uns durch die Angabe der Referenz mit einer Nachfrage des Auftraggebers beim jeweiligen Referenzauftraggeber einverstanden. Die Einreichung einer Bescheinigung der Referenzauftraggeber ist daher nicht erforderlich.

4.12.15 (9b32) Referenz 3 – Bewertung SOC/MDR-Betrieb KH 2

Gewichtung: 0,00%
Maximalpunktzahl: 10

Für jede eingereichte Referenz über die Implementierung und den Betrieb eines SOC/MDR-Service in einem Krankenhaus werden Punkte vergeben.

- Krankenhaus mit mindestens 500 Betten; eine KRITIS-Einstufung ist nicht erforderlich.
- 24/7-SOC-Betrieb muss Teil der Referenzleistung sein.

Bewertung zu Referenz 3 - Krankenhaus 2

- [☐] Keine Angabe (0)
[☐] Referenz genügt den Kriterien (10)
[☐] Referenz genügt NICHT den Kriterien (0)

Nur eine Antwort wählbar

4.12.16 (10) Referenz 4 – IoMT-Security-Plattform [Mussangabe]

Der Bewerber weist mindestens eine Referenz über die Implementierung und den Betrieb einer IoMT-Security-Plattform nach,

- bei der mindestens 1.000 vernetzte Medizingeräte überwacht werden
- Passive, nicht-invasive Überwachung der Medizingeräte muss Teil der Referenzleistung sind

Es müssen folgende Angaben in der vorgegebenen Reihenfolge getätigt werden:

- Benennung Referenzauftraggeber (mit Name und Anschrift)
- Benennung Ansprechpartner (mit Name, Telefonnummer und E-Mail)
- Bezeichnung des Auftragsgegenstandes
- Anzahl der vernetzten überwachten Medizingeräte
- Passive, nicht-invasive Überwachung der Medizingeräte sind Teil der Referenzleistung JA oder NEIN
- Ausführungszeitraum (von Datum bis Datum)

Ich/Wir erkläre/n mich/uns durch die Angabe der Referenz mit einer Nachfrage des Auftraggebers beim jeweiligen Referenzauftraggeber einverstanden. Die Einreichung einer Bescheinigung der Referenzauftraggeber ist daher nicht erforderlich.

4.12.17 (11) Anzahl festang. Mitarbeiter MDR/SOC und IoMT [Mussangabe]

Gewichtung: 0,00%
Maximalpunktzahl: 10

Anzahl festangestellter Mitarbeiter im direkten MDR/SOC- und IoMT-Betrieb

Anzugeben ist die Zahl der festangestellten Mitarbeiter, die direkt im MDR/SOC-Betrieb sowie im IoMT-Security-Betrieb eingesetzt werden (keine Stabsfunktionen, keine Vertrieb/Presales).

- ☐ Keine Angabe (0)
- ☐ größer/gleich 25 Mitarbeiter (10)
- ☐ größer/gleich 10 Mitarbeiter (5)
- ☐ kleiner 10 Mitarbeiter (0)

Nur eine Antwort wählbar

4.12.18 (12a) Jahresumsatz aus Cybersecurity Managed Servi [Mussangabe]

Anzugeben ist der Jahresumsatz, der in jedem der letzten drei abgeschlossenen Geschäftsjahre aus Cybersecurity Managed Services (SOC, MDR, SIEM, Endpoint Security, IoMT Security) erzielt wurde.

4.12.19 (12b) Bewertung Jahresumsatz [Mussangabe]

Gewichtung: 0,00%

Maximalpunktzahl: 15

Bewertung Jahresumsatz

Maßgeblich ist der niedrigste Umsatz in einem der drei Jahre

- ☐ Keine Angabe (0)
- ☐ größer/gleich 10 Mio. €/Jahr (15)
- ☐ größer/gleich 5 Mio. €/Jahr (10)
- ☐ größer/gleich 1 Mio. €/Jahr (5)
- ☐ kleiner 1 Mio. €/Jahr (0)

Nur eine Antwort wählbar

4.12.20 Eigenerklärung Business Continuity / Notbetrieb [Mussangabe]

Der Bieter bestätigt, dass er für die angebotenen Cybersecurity Managed Services angemessene Regelungen zur Business Continuity, zum Notbetrieb und zur Wiederherstellung kritischer Servicefunktionen vorhält. Die Regelungen berücksichtigen insbesondere Sicherheitsvorfälle beim Bieter selbst, Ransomware-Angriffe, Ausfälle zentraler Betriebsplattformen, Kommunikationsstörungen sowie eingeschränkte Verfügbarkeit der SOC-Organisation. Der Bieter bestätigt, dass im Auftragsfall spätestens im Rahmen der Transition ein geeigneter Nachweis, z. B. Management Summary, Auditnachweis, Testnachweis oder vergleichbarer Nachweis, vorgelegt wird.

- ☐ Keine Angabe (0)
- ☐ Ja (0)
- ☐ Nein (0)

Nur eine Antwort wählbar

Typ	Dateiname	Größe	MIME-Type
Dateianlage	Preismatrix SOC-SIEM final.xlsx	34,90 KB	xlsx