Leistungsbeschreibung

in dem Vergabeverfahren

Dialogmanagement und Kundenservice

Inhaltsverzeichnis

Inhaltsverzeichnis **2**

1. Ziele der Ausschreibung **3**
2. Leistungsumfang **3**

2.1 Dialogmanagement 4
2.2 Kundenservice 5

3. Einzelaufträge und Kampagnen **6**
4. Ansprechpartner und operative Steuerung **7**
5. Kontaktbearbeitung **7**
6. Kommunikationskanäle **8**
7. Telefonische Kommunikation **9**

7.1 Inbound 9
7.2 Outbound 9

8. E-Mail, SMS und sonstige Nachrichten **10**
9. Beratungsumfang und fachliche Verantwortung **10**
10. Informationsmaterialien **12**

10.1 Porto- und Briefabholungskosten 12

11. Personal **12**

11.1 Persönliche und kommunikative Anforderungen 13
11.2 Fachliche Kenntnisse 13
11.3 Sprachliche Anforderungen 14
11.4 Schulungen 14

12. Qualitätssicherung und Prozessmanagement **15**

12.1 Softwaregestützte Qualitätssicherung 16
12.2 Beschwerdemanagement 16
12.3 Kundenkontakt- und Wiedervorlagemanagement 17
12.4 Änderungs- und Weiterentwicklungsmanagement 17

13. Controlling, Berichtspflichten, Kennzahlenmeetings **18**
14. Technik / IT-Anforderungen / Datenaustausch **20**

14.1 Grundanforderungen an die Systemlandschaft 20
14.2 Dialer- und Zuweisungssysteme 21
14.3 Datenlieferung 22
14.4 Anforderungen an den Datenschutz und Informationssicherheit 22
14.5 Nachweispflichten des Auftragnehmers 32
14.6 AUDIT-Rechte 33
14.7 Rechtsgrundlagen 35

Hinweis zur Verwendung von Bezeichnungen

Aus Gründen der besseren Lesbarkeit wird in dieser Leistungsbeschreibung auf eine geschlechtsspezifische Differenzierung verzichtet. Personenbezeichnungen und sonstige verwendete Bezeichnungen gelten gleichermaßen für alle Geschlechter und sind ausdrücklich nicht diskriminierend zu verstehen.

1. Ziele der Ausschreibung

Die AOK Baden-Württemberg – nachfolgend „Auftraggeberin" – beabsichtigt, einen Rahmenvertrag über die Erbringung von Dienstleistungen im Bereich Dialogmanagement und Kundenservice abzuschließen.

Gegenstand des Rahmenvertrags ist die bedarfsabhängige Erbringung von Kundenkommunikations-, Beratungs-, Service- und unterstützenden Bearbeitungsleistungen über die von der Auftraggeberin vorgegebenen Kommunikationskanäle.

Ziel der Zusammenarbeit ist die Sicherstellung einer kundenorientierten, fachlich korrekten, effizienten und qualitativ hochwertigen Betreuung der Kundinnen und Kunden der Auftraggeberin. Der Auftragnehmer hat die Leistungen so zu erbringen, dass die von der Auftraggeberin vorgegebenen fachlichen, organisatorischen, technischen, datenschutzrechtlichen und qualitativen Anforderungen eingehalten werden.

Die Leistungen werden auf Grundlage einzelner Leistungsabrufe bzw. Kampagnenbeauftragungen innerhalb des Rahmenvertrags erbracht. Umfang, Leistungszeitraum, Zielgruppe, Kommunikationskanäle, Kontaktlogik, fachlicher Inhalt und erwartetes Leistungsvolumen werden im jeweiligen Einzelauftrag festgelegt.

Ein Anspruch des Auftragnehmers auf Abruf einer bestimmten Mindestmenge besteht nicht, soweit in den Vergabeunterlagen ausdrücklich nichts Abweichendes bestimmt ist.

Für den Rahmenvertrag wird ein **Budgetvolumen von 16,8 Mio. Euro für die gesamte Vertragslaufzeit einschließlich aller Verlängerungsoptionen** zugrunde gelegt.

Der vorgenannte Höchstwert bildet die Obergrenze der im Rahmen dieses Vertrags abrufbaren Leistungen.

2. Leistungsumfang

Die Leistungen gliedern sich insbesondere in folgende Bereiche:

1. Dialogmanagement (Outbound-Telefonie),

2. Kundenservice (inkl. Inbound-Telefonie),

4. Nachbearbeitung und Dokumentation,

5. Qualitätssicherung und Coaching,

6. Reporting und Controlling,

7. technische Unterstützung und Datenverarbeitung.

Zu den Kernleistungen des Auftragnehmers gehören insbesondere die Ziffern 1-4.

Unterstützende Tätigkeiten (z. B. Dokumentation, Recherche, Terminverwaltung) im Rahmen der zu erbringenden Dienstleistung dürfen unter Einsatz von Programmen mit künstlicher Intelligenz (KI) erfolgen, sofern insbesondere die Anforderungen des Kapitels 14.4.3 gewährleistet sind. Die unmittelbare Telefonie mit dem Kunden (insbesondere Gespräche, die einen direkten Austausch mit dem Kunden beinhalten) muss jedoch ausschließlich durch menschliche Mitarbeiter erfolgen; der Einsatz von KI-generierten Stimmen oder mechanischen Stimmen ist hierbei nicht zulässig. Die Telefonie darf nicht durch automatisierte Systeme, Sprachsynthese oder ähnliche Technologien erfolgen, die nicht auf einer natürlichen menschlichen Stimme basieren.

2.1 Dialogmanagement

Das Dialogmanagement umfasst die aktive und reaktive Kundenkommunikation im Rahmen von durch die Auftraggeberin beauftragten Maßnahmen und Kampagnen.

Der Auftragnehmer übernimmt insbesondere:

- Selektion von Daten und Aufbereitung von Daten;
- die aktive Kundenansprache (Outbound) über die von der Auftraggeberin vorgegebenen Kommunikationskanäle;
- die Annahme und Bearbeitung von Rückmeldungen der kontaktierten Personen;
- die fallabschließende Bearbeitung derjenigen Kundenanliegen, für die der Auftragnehmer nach den Vorgaben der Auftraggeberin zuständig ist;
- die strukturierte Erfassung des Kontaktergebnisses;
- die Durchführung definierter Folgemaßnahmen;
- die Weiterleitung solcher Vorgänge, die einer Bearbeitung durch die Auftraggeberin bedürfen;
- die ordnungsgemäße Dokumentation sämtlicher relevanter Kundenkontakte;

- die Einhaltung der jeweils vorgegebenen Gesprächsleitfäden, Arbeitsanweisungen und fachlichen Vorgaben.

Die Auftraggeberin bestimmt Ziel, Zielgruppe, fachlichen Inhalt, Kommunikationsstrategie und die zulässigen Kommunikationskanäle der jeweiligen Kampagne.
Der Auftragnehmer unterstützt die Auftraggeberin bei der operativen Umsetzung der Kampagne und bringt seine hierfür erforderliche technische und organisatorische Fachkompetenz ein.
Eine eigenständige Änderung der fachlichen Zielsetzung oder der rechtlichen bzw. leistungsrechtlichen Aussagen der Auftraggeberin durch den Auftragnehmer ist nicht zulässig.

2.2 Kundenservice

Der Kundenservice umfasst die Annahme, Bearbeitung und – soweit nach den Vorgaben der Auftraggeberin zulässig – fallabschließende Beantwortung von Kundenanliegen über die vereinbarten Kommunikationskanäle.

Hierzu gehören insbesondere:

- telefonische Inbound-Bearbeitung (Inbound-Hotlines);
- telefonische Outbound-Kommunikation (Rückrufe);
- Beratung auf Grundlage der von der Auftraggeberin bereitgestellten Informationen;
- Bearbeitung allgemeiner Fragen zu Leistungen, Services und Angeboten;
- allgemeine Informationen zu Verfahrens- und Bearbeitungsabläufen;
- Hinweise zu erforderlichen Unterlagen und Nachweisen;
- Erfassung und Dokumentation von Kundenanliegen;
- Durchführung definierter Nachbearbeitungen;
- Weiterleitung nicht abschließend bearbeitbarer Vorgänge.

Der Auftragnehmer ist nicht berechtigt, eigenständige rechtliche Bewertungen vorzunehmen, von den Vorgaben der Auftraggeberin abweichende fachliche Aussagen zu treffen oder verbindliche Entscheidungen für die Auftraggeberin zu treffen.
Die fachliche und rechtliche Letztentscheidung verbleibt bei der Auftraggeberin.

3. Einzelaufträge und Kampagnen

Der zuständige Geschäftsbereich der Auftraggeberin beauftragt einzelne Kampagnen bzw. Leistungsmaßnahmen innerhalb des Rahmenvertrags. Eine unmittelbare fachliche Abstimmung mit anderen Organisationseinheiten der Auftraggeberin erfolgt nur nach vorheriger Abstimmung oder Beauftragung durch den zuständigen Geschäftsbereich.

Der jeweilige Einzelauftrag enthält insbesondere:

- Bezeichnung und Ziel der Maßnahme oder Kampagne;
- Zielgruppe;
- Leistungszeitraum;
- Kommunikationskanal bzw. Kommunikationskanäle;
- voraussichtliches Kontaktvolumen;
- Kontaktlogik;
- zulässige Kontaktfrequenz;
- fachliche Inhalte;
- Gesprächsleitfäden bzw. sonstige Kommunikationsvorgaben;
- Anforderungen an die Dokumentation;
- erforderliche Folgemaßnahmen;
- einzuhaltende Service- und Qualitätskennzahlen;
- gegebenenfalls besondere Schulungsanforderungen.

Der Auftragnehmer prüft den Einzelauftrag unverzüglich auf technische, organisatorische und kapazitive Umsetzbarkeit. Der Auftragnehmer bringt seine fachliche Expertise sowie seine Kenntnisse aus dem relevanten Branchen- und Fachumfeld in die Zusammenarbeit mit der Auftraggeberin ein. Er informiert die Auftraggeberin über relevante fachliche Entwicklungen, aktuelle Erkenntnisse aus Wissenschaft und Praxis sowie branchenspezifische Trends und Erfahrungen, soweit diese für die Erbringung oder Weiterentwicklung der vertraglichen Leistungen von Bedeutung sind. Der Auftragnehmer weist die Auftraggeberin auf fachliche Weiterentwicklungsmöglichkeiten und Optimierungspotenziale hin und unterstützt durch geeignete Vorschläge die kontinuierliche Weiterentwicklung der Leistungen im Bereich Dialogmanagement und Kundenservice.

Erkennbare Widersprüche, Unklarheiten oder technische bzw. organisatorische Hindernisse sind der Auftraggeberin unverzüglich mitzuteilen.

Für jede Kampagne per Telefon (Outbound- und Inbound) hält der Auftragnehmer separate Kampagnenrufnummern vor. Der Auftragnehmer hat sicherzustellen, dass die telefonische Kommunikation im Rahmen der Leistungserbringung unter der der Auftraggeberin zugeordneten Ortsnetzrufnummer „0711" bzw. „+49711" erfolgen kann. Die Nutzung der Ortsnetzrufnummer hat unter Einhaltung der jeweils geltenden telekommunikationsrechtlichen Vorgaben, insbesondere der Anforderungen an den Ortsnetzbezug, zu erfolgen. Eine entsprechende technische und rechtmäßige Umsetzung ist durch den Auftragnehmer sicherzustellen.

Die operative Umsetzung beginnt erst nach Freigabe durch die Auftraggeberin.

4. Ansprechpartner und operative Steuerung

Der Auftragnehmer benennt für die gesamte Vertragslaufzeit:

- eine Projektleitung,
- eine stellvertretende Projektleitung
- eine technische Ansprechperson

als zentrale Ansprechpartner für die Auftraggeberin.

Eine Ansprechperson des Projektteams muss während der Geschäftszeiten der Auftraggeberin von Montag bis Freitag in der Zeit von 08:00 Uhr bis 18:00 Uhr erreichbar sein.

Anfragen, Störungen, Anforderungen, Beschwerden oder sonstige Anliegen der Auftraggeberin sind durch den Auftragnehmer unverzüglich zu bearbeiten. Bei als dringend gekennzeichneten oder aufgrund ihrer Auswirkungen als dringend einzustufenden Anliegen hat eine qualifizierte Rückmeldung innerhalb von sechs (6) Stunden während der Geschäftszeiten der Auftraggeberin zu erfolgen. Ist absehbar, dass eine abschließende Bearbeitung innerhalb dieses Zeitraums nicht möglich sein wird, hat der Auftragnehmer die Auftraggeberin hierüber unverzüglich durch eine qualifizierte Zwischennachricht zu informieren. Diese sollte mindestens den Bearbeitungsstand, die bereits eingeleiteten Maßnahmen sowie den voraussichtlichen Zeitpunkt der abschließenden Bearbeitung enthalten.

5. Kontaktbearbeitung

Ein Kundenkontakt gilt als vollständig bearbeitet, wenn sämtliche für die jeweilige Maßnahme vorgesehenen Prozessschritte ordnungsgemäß durchgeführt und dokumentiert wurden.

Hierzu gehören insbesondere:

1. Durchführung des vorgesehenen Kontaktversuchs;

2. Bearbeitung des Gesprächsanlasses nach den vorgegebenen fachlichen Anforderungen;

3. Erfassung des Kontaktergebnisses;

4. Erfassung der vorgegebenen Informationen;

5. Durchführung erforderlicher Folgeschritte;

6. Dokumentation des Vorgangs im vorgesehenen System.

Der Eintritt eines bestimmten Erfolgs, insbesondere das Erreichen einer Zielperson oder der Abschluss eines Vertrags, ist nur dann geschuldet, wenn dies im jeweiligen Einzelauftrag ausdrücklich als Leistungsziel vereinbart wurde.

Mehrere Kontaktversuche mit demselben Kunden- oder Vorgangsbezug sind einem einheitlichen Vorgang zuzuordnen und nachvollziehbar zu dokumentieren.

6. Kommunikationskanäle

Die Leistungserbringung kann insbesondere über folgende Kommunikationskanäle erfolgen:

- Telefonie;
- E-Mail;
- SMS bzw. vergleichbare Kurznachrichtendienste;
- Chat;
- sonstige digitale Kommunikationskanäle;
- postalische Kommunikation;
- Co-Browsing bzw. vergleichbare assistierte Online-Verfahren.

Die konkret einzusetzenden Kommunikationskanäle werden im jeweiligen Einzelauftrag festgelegt.

Weitere Kommunikationskanäle dürfen nur dann in den Leistungsumfang aufgenommen werden, wenn deren Art, technischer und organisatorischer Umfang sowie die hierfür geltenden Leistungsanforderungen vorab hinreichend bestimmt und durch eine nach § 132 GWB zulässige Änderungs- oder Optionsregelung gedeckt sind.

Eine Erweiterung des Leistungsumfangs allein aufgrund eines einseitigen Weisungsrechts der Auftraggeberin findet nicht statt, soweit dadurch der ursprüngliche Auftragsgegenstand wesentlich verändert oder erweitert würde.

7. Telefonische Kommunikation

7.1 Inbound

Der Auftragnehmer nimmt eingehende Kundenkontakte innerhalb der vereinbarten Servicezeiten entgegen und bearbeitet diese entsprechend den fachlichen und organisatorischen Vorgaben der Auftraggeberin.

Nicht abschließend bearbeitbare Anliegen sind entsprechend den vorgegebenen Eskalations- und Weiterleitungsprozessen zu behandeln.

Reguläre telefonische Inbound-Leistungen erfolgen in der Regel werktags von Montag bis Freitag in der Zeit von 07:00 Uhr bis 18:00 Uhr.

Sofern dies für die Durchführung einzelner Maßnahmen oder Kampagnen erforderlich ist, können abweichende Servicezeiten zwischen Auftraggeberin und Auftragnehmer vereinbart werden.

Ausgenommen sind gesetzliche Feiertage im Land Baden-Württemberg sowie der 24. Dezember und der 31. Dezember.

7.2 Outbound

Outbound-Kontakte erfolgen ausschließlich auf Grundlage von durch die Auftraggeberin freigegebenen Kampagnen.

Der Auftragnehmer hat insbesondere sicherzustellen, dass:

- ausschließlich von der Auftraggeberin freigegebene Zielgruppen kontaktiert werden;
- die vorgegebenen Kontaktzeiten eingehalten werden;
- die vorgegebenen Kontaktfrequenzen eingehalten werden;
- gesperrte bzw. ausgeschlossene Datensätze nicht kontaktiert werden;
- sämtliche Kontaktversuche nachvollziehbar dokumentiert werden;
- Rückrufe der jeweiligen Kampagne eindeutig zugeordnet werden können.

Die technische Umsetzung der Telefonie muss den jeweils geltenden telekommunikationsrechtlichen Anforderungen entsprechen.

Reguläre telefonische Outbound-Leistungen erfolgen in der Regel werktags von Montag bis Freitag in der Zeit von 08:00 Uhr bis 18:00 Uhr.

Sofern dies für die Durchführung einzelner Maßnahmen oder Kampagnen erforderlich ist, können abweichende Servicezeiten zwischen Auftraggeberin und Auftragnehmer vereinbart werden.

Ausgenommen sind gesetzliche Feiertage im Land Baden-Württemberg sowie der 24. Dezember und der 31. Dezember.

8. E-Mail, SMS und sonstige Nachrichten

Der Versand elektronischer Nachrichten erfolgt ausschließlich nach den Vorgaben der Auftraggeberin.

Die Auftraggeberin bestimmt insbesondere:

- Empfängerkreis;
- Inhalt;
- Versandzeitpunkt;
- Versandfrequenz;
- Anlass des Versands;
- zulässigen Kommunikationskanal.

Der Auftragnehmer hat die technischen und organisatorischen Voraussetzungen für die Umsetzung dieser Vorgaben sicherzustellen.

Der Auftragnehmer darf Inhalte, Versandzeitpunkte oder Empfängergruppen nicht eigenständig verändern.

9. Beratungsumfang und fachliche Verantwortung

Die Beratung erfolgt ausschließlich auf Grundlage der von der Auftraggeberin bereitgestellten und freigegebenen Informationen.

Hierzu gehören insbesondere:

- Unternehmenswebsite;
- Wissensdatenbanken;
- Mitarbeiter- und Prozessportale;

- FAQ;
- Gesprächsleitfäden;
- Arbeitsanweisungen;
- Schulungsunterlagen;
- freigegebene Textbausteine.

Die bereitgestellten Informationen bilden die verbindliche fachliche Grundlage der Leistungserbringung.

Der Auftragnehmer hat sicherzustellen, dass die eingesetzten Mitarbeitenden ausschließlich die jeweils aktuellen Informationen verwenden.

Der **Beratungsumfang** umfasst insbesondere:

- allgemeine Informationen zu den Services der Auftraggeberin;
- Informationen zu KundenCentern, Standorten und Öffnungszeiten;
- Informationen zu Online-Services;
- allgemeine Informationen zu versicherungsrechtlichen Sachverhalten;
- allgemeine Informationen zu Leistungen der gesetzlichen Krankenversicherung;
- allgemeine Informationen zu Bearbeitungs- und Verfahrensabläufen;
- allgemeine Informationen zu Bearbeitungsständen, soweit hierfür eine entsprechende Freigabe besteht;
- Hinweise auf notwendige oder erforderliche Unterlagen;
- allgemeine Informationen zu Angeboten und Produkten der Auftraggeberin.

Eine individuelle rechtliche oder leistungsrechtliche Anspruchsprüfung oder Entscheidung wird durch den Auftragnehmer nicht getroffen.

Insbesondere sind Mitarbeitende des Auftragnehmers nicht berechtigt,

- Leistungsansprüche verbindlich festzustellen;

- Leistungen verbindlich zu bewilligen oder abzulehnen;
- Verwaltungsakte zu erlassen;
- rechtsverbindliche Erklärungen für die Auftraggeberin abzugeben;
- von den Vorgaben der Auftraggeberin abweichende Rechtsauffassungen gegenüber Kunden zu vertreten.

Anliegen, die eine Entscheidung oder fachliche Prüfung durch die Auftraggeberin erfordern, sind nach dem jeweils geltenden Eskalations- bzw. Weiterleitungsprozess an die zuständige Stelle der Auftraggeberin weiterzuleiten.

10. Informationsmaterialien

Die Auftraggeberin kann dem Auftragnehmer Informations- und Kampagnenmaterialien zur Verfügung stellen. Der Auftragnehmer stellt hierfür geeignete und gesicherte Lagerflächen bereit. Der voraussichtliche Lagerbedarf beträgt derzeit etwa 5 m^2.

Der Auftragnehmer führt eine nachvollziehbare Bestandsübersicht. Für jedes Material werden – soweit erforderlich – Mindestbestände festgelegt. Bei Erreichen des jeweiligen Mindestbestands informiert der Auftragnehmer die Auftraggeberin unverzüglich.

10.1 Porto- und Briefabholungskosten

Anfallende Portokosten z. B. im Rahmen des Versands von Informationsmaterialien, werden direkt über den von der Auftraggeberin beauftragten Postversanddienstleister abgerechnet.

Der Auftragnehmer erfasst und übermittelt hierfür die erforderlichen Versanddaten und hält diese laufend aktuell. Die über den Postweg versendeten Sendungen sind nachvollziehbar zu dokumentieren.

Kosten für die Abholung von Briefen werden, sofern erforderlich, entweder gegen geeigneten Nachweis über die Auftraggeberin oder direkt über den von ihr beauftragten Postversanddienstleister abgerechnet. Die Abrechnungs- und Abwicklungsform legt die Auftraggeberin fest.

11. Personal

Der Auftragnehmer setzt ausschließlich Personal ein, das für die jeweilige Tätigkeit fachlich, persönlich, sprachlich und technisch geeignet ist.

Die erforderlichen fachlichen Kenntnisse müssen spätestens zum Zeitpunkt des erstmaligen Einsatzes im jeweiligen Aufgabenbereich vorhanden sein.

Es ist nicht erforderlich, dass sämtliche fachlichen Kenntnisse bereits zum Zeitpunkt der Angebotsabgabe bei sämtlichen vorgesehenen Mitarbeitenden vorhanden sind, sofern die Auftraggeberin die entsprechende Qualifizierung vor Einsatz zulässt.

Der Auftragnehmer hat jedoch sicherzustellen, dass die Mitarbeitenden vor Aufnahme der jeweiligen Tätigkeit über sämtliche für diese Tätigkeit erforderlichen Kenntnisse verfügen.

11.1 Persönliche und kommunikative Anforderungen

Die eingesetzten Mitarbeitenden müssen insbesondere über folgende Kompetenzen verfügen:

- ausgeprägte Kunden- und Serviceorientierung;
- höfliches und wertschätzendes Auftreten;
- Empathie;
- strukturierte Gesprächsführung;
- Konflikt- und Deeskalationskompetenz;
- lösungsorientiertes Arbeiten;
- Belastbarkeit;
- sichere Kommunikation auch in schwierigen Gesprächssituation.

11.2 Fachliche Kenntnisse

Die eingesetzten Mitarbeitenden müssen über die für den jeweiligen Aufgabenbereich erforderlichen Kenntnisse des Systems der gesetzlichen Krankenversicherung sowie der von der Auftraggeberin bereitgestellten fachlichen Inhalte verfügen.

Die erforderlichen Kenntnisse können insbesondere durch:

- Schulungen;
- E-Learning;
- praktische Einarbeitung;
- Coaching;
- Berufserfahrung;
- regelmäßige Qualifizierungsmaßnahmen

vermittelt bzw. sichergestellt werden.

11.3 Sprachliche Anforderungen

Die Projektsprache im Rahmen der Leistungserbringung ist Deutsch.

Der Auftragnehmer stellt sicher, dass alle im Projekt eingesetzten Mitarbeitenden über sehr gute Deutschkenntnisse in Wort und Schrift verfügen. Die eingesetzten Mitarbeitenden müssen über ein Sprachniveau verfügen, das mindestens dem Niveau C1 bis C2 des Gemeinsamen Europäischen Referenzrahmens für Sprachen (GER) entspricht oder vergleichbare Sprachkenntnisse aufweisen.

Diese Anforderung eines bestimmten GER-Niveaus ist nur dann Bestandteil der Leistungsanforderungen, wenn dieses Niveau für die konkrete Leistungserbringung sachlich erforderlich und verhältnismäßig ist.

11.4 Schulungen

Der Auftragnehmer ist für die ordnungsgemäße Einarbeitung und laufende Qualifizierung des eingesetzten Personals verantwortlich.

Vor dem erstmaligen Einsatz müssen die Mitarbeitenden mindestens:

- die erforderlichen fachlichen Inhalte;
- die relevanten Prozessvorgaben;
- die eingesetzten Systeme;
- die Datenschutz- und Informationssicherheitsanforderungen;
- die Anforderungen bei Einsatz von unterstützender KI (KI-Kompetenz);
- die Kommunikations- und Qualitätsstandards

kennen und anwenden können.

Ändern sich fachliche, rechtliche, organisatorische oder technische Vorgaben, hat der Auftragnehmer die erforderliche Nachschulung vor Umsetzung der Änderung sicherzustellen.

Die Auftraggeberin kann bei begründeten Qualitätsabweichungen zusätzliche Schulungsmaßnahmen verlangen.

12. Qualitätssicherung und Prozessmanagement

Der Auftragnehmer unterhält während der gesamten Vertragslaufzeit ein dokumentiertes Qualitätssicherungssystem.

Dieses umfasst insbesondere:

- regelmäßige Qualitätskontrollen;
- Stichprobenprüfungen;
- Auswertung von Kundenkontakten;
- Ermittlung und Dokumentation von Qualitätsabweichungen;
- Ursachenanalyse;
- Korrekturmaßnahmen;
- Wirksamkeitskontrolle;
- kontinuierliche Verbesserung.

Die Auftraggeberin ist berechtigt, die Qualität der Leistungserbringung durch Stichproben, Testkontakte, Audits, Silent Monitoring oder vergleichbare geeignete Prüfverfahren zu kontrollieren, soweit dies datenschutzrechtlich zulässig.

Es erfolgen mindestens zwei (2) Qualitätsprüfungen pro Kalenderjahr. Die Durchführung kann vor Ort beim Auftragnehmer oder mittels geeigneter digitaler Prüfungsformate erfolgen. Die Termine werden zwischen Auftraggeberin und Auftragnehmer rechtzeitig abgestimmt.

Der Auftragnehmer wirkt an den Qualitätssicherungsmaßnahmen der Auftraggeberin aktiv mit und stellt die hierfür erforderlichen Informationen, Nachweise und Ansprechpartner zur Verfügung.

Der Auftragnehmer hat sicherzustellen, dass neue oder geänderte Prozesse strukturiert eingeführt, dokumentiert und in die bestehende Leistungserbringung integriert werden. Darüber hinaus sind bestehende Prozesse regelmäßig zu überprüfen und bei Bedarf weiterzuentwickeln.

Der Auftragnehmer ist verpflichtet, prozessuale Schwachstellen sowie Optimierungspotenziale zu identifizieren und der Auftraggeberin geeignete Verbesserungsmaßnahmen vorzuschlagen. Die Umsetzung dieser Maßnahmen erfolgt in Abstimmung mit der Auftraggeberin. Die

Prozessgestaltung hat sich an den fachlichen Vorgaben der Auftraggeberin sowie an den Anforderungen einer service- und kundenorientierten Leistungserbringung auszurichten.

Die eingesetzten Prozessverantwortlichen müssen über die für die Aufgabenerfüllung erforderlichen Kenntnisse und Erfahrungen im Bereich Prozessmanagement verfügen. Dies umfasst insbesondere die Fähigkeit zur Analyse, Weiterentwicklung und Optimierung von Prozessen sowie zur Steuerung der damit verbundenen Maßnahmen.

12.1 Softwaregestützte Qualitätssicherung

Der Auftragnehmer hat während der gesamten Vertragslaufzeit ein geeignetes, softwaregestütztes System zur Qualitätssicherung und Analyse der Kundenkontakte einzusetzen.

Das System muss insbesondere die Analyse und Auswertung von Kundenkontakten (z. B. Gesprächsaufzeichnungen, Stichprobenbewertungen oder vergleichbare Verfahren) ermöglichen und die Ergebnisse der Qualitätssicherung nachvollziehbar dokumentieren.

Die Auftraggeberin ist berechtigt, Einblick in die Ergebnisse der Qualitätssicherung zu nehmen. Dies umfasst insbesondere Auswertungen, Qualitätskennzahlen sowie dokumentierte Bewertungen von Kundenkontakten.

Der Zugriff kann nach Wahl des Auftragnehmers beispielsweise über ein geeignetes Reporting, einen Systemzugang oder einen sicheren Remote-Zugriff erfolgen.

Die konkrete technische Ausgestaltung des eingesetzten Systems ist vom Auftragnehmer sicherzustellen und mit der Auftraggeberin abzustimmen.

12.2 Beschwerdemanagement

Beschwerden von Kundinnen und Kunden sind unverzüglich entsprechend den Vorgaben des Beschwerdemanagementprozesses zu erfassen und in geeigneter Form an die Auftraggeberin weiterzuleiten, sofern sie in deren Zuständigkeit fallen oder eine weitergehende Bearbeitung durch die Auftraggeberin erforderlich ist.

Beschwerden, die der Auftraggeberin im Zusammenhang mit der Leistungserbringung des Auftragnehmers bekannt werden und an diesen weitergeleitet werden, sind vom Auftragnehmer unverzüglich zu bearbeiten.

Der Auftragnehmer erstellt hierzu eine sachgerechte Stellungnahme zum jeweiligen Sachverhalt und stellt diese der Auftraggeberin innerhalb der vereinbarten Fristen und über die vorgesehenen Kommunikationswege zur Verfügung.

Die Auftraggeberin verfügt über einen standardisierten Prozess zur Bearbeitung von Beschwerden. Der Auftragnehmer hat diesen Prozess sowie die darin festgelegten Abläufe, Zuständigkeiten, Kommunikationswege und Dokumentationsanforderungen einzuhalten.

12.3 Kundenkontakt- und Wiedervorlagemanagement

Der Auftragnehmer stellt ein System bereit, mit dem nicht abgeschlossene Kontaktvorgänge strukturiert weiterbearbeitet werden können.

Das System muss insbesondere ermöglichen:

- Wiedervorlagezeitpunkte festzulegen;
- Kontaktintervalle zu steuern;
- Kontaktfrequenzen zu begrenzen;
- Kontaktversuche zu dokumentieren;
- Ausschlussgründe zu berücksichtigen;
- Kampagnen eindeutig zuzuordnen;
- Rückrufe einer Kampagne zuzuordnen.

Die von der Auftraggeberin vorgegebenen Kontaktfrequenzen und Ausschlussregeln sind technisch umzusetzen.

12.4 Änderungs- und Weiterentwicklungsmanagement

Die Auftraggeberin kann innerhalb des in den Vergabeunterlagen festgelegten Leistungsumfangs fachliche, organisatorische und technische Anpassungen verlangen.

Solche Anpassungen können insbesondere erforderlich werden aufgrund:

- gesetzlicher Änderungen;
- Änderungen von Leistungen oder Prozessen;
- Änderungen der Kommunikationsstrategie;
- technischer Weiterentwicklungen;
- Änderungen von Informations- und Wissensinhalten.

Soweit eine Anpassung eine wesentliche Erweiterung oder Veränderung des Auftragsgegenstands darstellen würde, ist sie nicht allein aufgrund dieser Leistungsbeschreibung geschuldet. Die Parteien prüfen in diesem Fall, ob und auf welcher vergaberechtlichen Grundlage eine Vertragsänderung zulässig ist.

13. Controlling, Berichtspflichten, Kennzahlenmeetings

Zur Steuerung, Überwachung und kontinuierlichen Weiterentwicklung der Leistungserbringung führt der Auftragnehmer ein regelmäßiges Reporting der Kampagnen durch. Die für das Reporting relevanten Kennzahlen werden von der Auftraggeberin vorher festgelegt. Hierzu können insbesondere gehören:

- Anzahl der Kontaktversuche und Anwahlversuche;
- Anzahl erreichter Kunden;
- Kontaktquote;
- Bearbeitungsvolumen;
- Erreichbarkeit;
- Servicelevel;
- Wartezeiten;
- Bearbeitungszeiten;
- Abbruchquoten;
- Weiterleitungsquoten;
- Qualitätswerte;
- Beschwerdequote;
- Rückrufquote;
- Ergebnisse der Qualitätssicherung.

Die Definition, Berechnung und Ermittlungsmethode jeder KPI wird vor Beginn der Leistungserbringung verbindlich festgelegt. Die Kennzahlen richten sich nach Art, Umfang und Zielsetzung der beauftragten Leistungen sowie den eingesetzten Kommunikationskanälen; dies gilt gleichermaßen für während der Vertragslaufzeit neu hinzukommende Leistungen oder Kommunikationskanäle.

Die Bereitstellung der Reportings erfolgt grundsätzlich in von der Auftraggeberin vorgegebenen Formaten (z. B. XLSX, CSV oder PDF) sowie bei Bedarf über vereinbarte technische Schnittstellen oder Reportinglösungen.

Die Berichte sind innerhalb folgender Fristen bereitzustellen:

- Tagesberichte: spätestens am folgenden Arbeitstag,
- Wochenberichte: spätestens am ersten Arbeitstag der Folgewoche,
- Monatsberichte: spätestens bis zum fünften (5.) Arbeitstag des Folgemonats,
- Jahresberichte: spätestens bis zum 15. Januar des Folgejahres.

Der Auftragnehmer stellt sicher, dass die vereinbarten Kennzahlen vollständig, korrekt, nachvollziehbar und auf einer belastbaren Datengrundlage erhoben, dokumentiert, ausgewertet und der Auftraggeberin in geeigneter Form zur Verfügung gestellt werden. Die Herleitung und Berechnung der Kennzahlen müssen jederzeit nachvollziehbar und transparent sein.

Der Auftragnehmer analysiert eigenständig Auffälligkeiten, wesentliche Abweichungen von vereinbarten Kennzahlen sowie erkennbare Trends und Entwicklungen und stellt diese im Reporting nachvollziehbar dar. Dazu gehören die Analyse möglicher Ursachen, Bewertung der Auswirkungen auf die Leistungserbringung sowie die Entwicklung geeigneter Maßnahmen zur Stabilisierung und kontinuierlichen Verbesserung der Leistungen. Ergänzend zum regelmäßigen Reporting führen die Auftraggeberin und der Auftragnehmer einmal wöchentlich ein gemeinsames Kennzahlenmeeting durch. Das Kennzahlenmeeting ist Bestandteil der operativen Leistungssteuerung und dient der gemeinsamen Bewertung, Steuerung und kontinuierlichen Weiterentwicklung der Leistungserbringung. Gegenstand des Kennzahlenmeetings sind insbesondere:

- Vorstellung und Erläuterung der aktuellen Tages-, Wochen-, Monats- und gegebenenfalls Jahresberichte,
- Analyse der Entwicklung der vereinbarten Kennzahlen,
- Bewertung von Auffälligkeiten, Trends und wesentlichen Abweichungen,
- Analyse der Ursachen von Zielabweichungen,
- Abstimmung und Priorisierung geeigneter Maßnahmen zur Stabilisierung und Verbesserung der Leistungserbringung,
- Nachverfolgung vereinbarter Maßnahmen einschließlich Verantwortlichkeiten, Umsetzungsfristen und Wirksamkeit,
- Identifikation von Optimierungs- und Weiterentwicklungspotenzialen,

- Bewertung geänderter fachlicher, organisatorischer oder technischer Anforderungen sowie deren Auswirkungen auf die Leistungserbringung und die Kennzahlen.

Soweit erforderlich, können anlassbezogen weitere Kennzahlenmeetings durchgeführt werden. Der Auftragnehmer bereitet die Kennzahlenmeetings fachlich vor und stellt der Auftraggeberin die hierfür erforderlichen Berichte, Auswertungen, Analysen sowie Entscheidungsgrundlagen rechtzeitig zur Verfügung. Auf Verlangen der Auftraggeberin sind Kennzahlen, Auswertungen und Auffälligkeiten zu erläutern sowie die zugrunde liegenden Berechnungs- und Ermittlungsmethoden nachvollziehbar darzustellen.

Da sich die Anforderungen an die Leistungserbringung während der Vertragslaufzeit ändern können (z. B. durch neue Leistungen, Kommunikationskanäle, gesetzliche oder organisatorische Anforderungen sowie geänderter Steuerungsbedarfe), ist die Auftraggeberin berechtigt, Kennzahlen sowie deren Definition, Ausgestaltung, Berechnungsmethoden und Berichtsformate unter Berücksichtigung der berechtigten Interessen des Auftragnehmers anzupassen, zu ergänzen oder durch andere geeignete Kennzahlen zu ersetzen, soweit dies für eine sachgerechte Steuerung und Bewertung der Leistungserbringung erforderlich ist.

14. Technik / IT-Anforderungen / Datenaustausch

14.1 Grundanforderungen an die Systemlandschaft

Der Auftragnehmer hat während der gesamten Vertragslaufzeit eine leistungsfähige, sichere und dem Stand der Technik entsprechende IT- und Kommunikationsinfrastruktur vorzuhalten, die eine ordnungsgemäße Erbringung der vertraglich geschuldeten Leistungen gewährleistet.

Die eingesetzten Systeme müssen insbesondere geeignet sein, Kundenkontakte zu steuern, Kommunikationsvorgänge zu dokumentieren, Kampagnen durchzuführen, Kontaktergebnisse zu erfassen sowie Auswertungen und Reportings bereitzustellen. Hierfür sind die erforderlichen technischen Systeme und Anwendungen (z. B. Telefonieplattform, Dialer-Systeme, CRM-Systeme, Datenbanken und Reportinglösungen usw.) bereitzustellen und der Auftraggeberin auf Anforderung zu beschreiben.

Für Datenlieferungen sind ausschließlich sichere und dem Stand der Technik entsprechende Übertragungsverfahren einzusetzen. Hierzu zählen insbesondere verschlüsselte Dateiübertragungsverfahren (z. B. SFTP), gesicherte Web-Protokolle (HTTPS/TLS) oder vergleichbare Verfahren.

Die Kommunikation zwischen Auftraggeberin und Auftragnehmer hat bei der Übermittlung schutzbedürftiger oder personenbezogener Daten ausschließlich über verschlüsselte Kommunikationswege zu erfolgen. Der Auftragnehmer hat spätestens zum Beginn der Vertragslaufzeit ein

Verfahren zur E-Mail-Verschlüsselung bereitzustellen. Hierfür sind mindestens die Verfahren S/MIME oder PGP zu unterstützen.

Die Gewährleistung der technischen Voraussetzungen zur Anbindung an die Systeme der Auftraggeberin sowie zur Nutzung der von ihr bereitgestellten Anwendungen obliegt dem Auftragnehmer. Sofern die Auftraggeberin künftig vorsieht, dass Mitarbeitende des Auftragnehmers unmittelbar auf Anwendungen, Fachverfahren, CRM-Systeme oder sonstige Systeme der Auftraggeberin zugreifen, hat der Auftragnehmer die hierfür erforderlichen technischen, organisatorischen und sicherheitsrelevanten Voraussetzungen zu schaffen und aufrechtzuerhalten.

Der Auftragnehmer beobachtet die für die Leistungserbringung relevanten technischen Entwicklungen auf dem Markt sowie innerhalb seines Unternehmens, insbesondere im Hinblick auf neue Technologien, Verfahren oder erprobte Lösungen. Er informiert die Auftraggeberin proaktiv über wesentliche Veränderungen des Stands der Technik sowie über relevante interne Entwicklungen, soweit diese Auswirkungen auf die vertragsgegenständlichen Leistungen oder deren wirtschaftliche, qualitative oder technische Umsetzung haben können.

14.2 Dialer- und Zuweisungssysteme

Der Auftragnehmer hat ein Dialer- und/oder automatisiertes Zuweisungssystem bereitzustellen, das eine effiziente und gleichmäßige Verteilung der zu bearbeitenden Kontakte sicherstellt.

Das System muss so konfigurierbar sein, dass fachliche und organisatorische Vorgaben der Auftraggeberin systemseitig umgesetzt werden können. Hierzu gehören insbesondere Vorgaben zu Kontaktlogiken, Priorisierungen, Kontaktfrequenzen, Kontaktintervallen sowie Verteil- und Steuerungsmechanismen. Eine Konzentration von Kontakten auf einzelne Regionen, Mitarbeitende, bestimmte Bearbeitungseinheiten oder sonstige vergleichbare Einheiten bzw. Strukturen ist systemseitig zu verhindern, sofern dies nicht ausdrücklich durch die Auftraggeberin vorgegeben wird. Der Auftragnehmer hat sicherzustellen, dass entsprechende Anpassungen durch Konfiguration oder geeignete technische Anpassungen während der Vertragslaufzeit umgesetzt werden können.

Darüber hinaus ist sicherzustellen, dass durch Outbound-Kampagnen ausgelöste Rückrufe von Kundinnen und Kunden den jeweiligen Kampagnen zugeordnet werden können und eine konsistente Bearbeitung der Kundenanliegen gewährleistet ist.

Der Auftragnehmer stellt sicher, dass die eingesetzten Dialer- und Zuweisungssysteme dem aktuellen Stand der Technik entsprechen. Er beobachtet relevante technologische Entwicklungen und informiert die Auftraggeberin über neue Funktionen, Erweiterungen oder Optimierungsmöglichkeiten.

14.3 Datenlieferung

Die Auftraggeberin stellt die für die jeweilige Maßnahme erforderlichen Daten über die vereinbarten sicheren Übertragungswege zur Verfügung. Die fachlichen, technischen und organisatorischen Anforderungen an die Schnittstelle werden in der Ausschreibungsphase näher erläutert. Der Auftragnehmer hat die technischen Voraussetzungen für die Anbindung und Nutzung der Schnittstelle zu schaffen und während der gesamten Vertragslaufzeit aufrechtzuerhalten. Erforderliche Anpassungen, die sich aus fachlichen, technischen oder gesetzlichen Anforderungen ergeben, sind innerhalb angemessener Fristen umzusetzen.

Der Auftragnehmer ist verpflichtet, die Daten nach Eingang auf Vollständigkeit und technische Verarbeitbarkeit zu prüfen.

Festgestellte Fehler oder Unstimmigkeiten sind unverzüglich zu melden.

Der Auftragnehmer dokumentiert insbesondere:

- Zeitpunkt des Datenimports;
- verwendeten Datenbestand;
- Kontaktversuche;
- Kontaktergebnisse;
- Weiterleitungen;
- Löschungen bzw. Sperrungen.

Datensätze, die von der Auftraggeberin als zu löschen, gesperrt oder von der weiteren Bearbeitung ausgeschlossen gekennzeichnet wurden, sind unverzüglich aus den aktiven Bearbeitungsprozessen zu entfernen. Eine weitere Kontaktaufnahme mit diesen Datensätzen ist technisch und organisatorisch auszuschließen.

14.4 Anforderungen an den Datenschutz und Informationssicherheit

Der Auftragnehmer erbringt alle Leistungen stets im Einklang mit den spezifischen gesetzlichen und regulatorischen Vorgaben dieses Kapitels. Der Auftragnehmer stellt die vollständige, nachweisbare und auditfähige Umsetzung dieser Vorgaben über die gesamte Vertragslaufzeit sicher und kaskadiert die Anforderungen vertraglich auf Unterauftragnehmer.

14.4.1 Anforderungen an den Datenschutz:

Der Auftragnehmer unterstützt die Auftraggeberin vollumfänglich und berücksichtigt alle Anforderungen bei der rechtssicheren Verarbeitung von Sozial- und Gesundheitsdaten insbesondere nach den bereichsspezifischen Vorgaben des SGB. Maßgeblich sind der Sozialdatenschutz des SGB X (u. a. Begriffsbestimmungen/Sozialgeheimnis und Auftragsverarbeitung), die Regeln des SGB V für Krankenkassen und die Vorgaben des SGB XI für Pflegekassen und Pflegeleistungen.

Der Auftragnehmer verarbeitet Sozialdaten ausschließlich im Rahmen einer Auftragsverarbeitung nach Art. 28 DSGVO i. V. m. § 80 SGB X mit schriftlich fixierten technisch-organisatorische Maßnahmen (TOMs), Weisungs- und Kontrollrechten der Auftraggeberin.

Die Verarbeitung der im Rahmen dieses Auftrags anfallenden Sozialdaten erfolgt ausschließlich

- im Inland,
- in einem Mitgliedstaat der Europäischen Union,
- in einem nach § 35 Abs. 7 SGB I gleichgestellten Staat (insbesondere EWR-Staaten und Schweiz)
- oder in einem Drittstaat, für den ein Angemessenheitsbeschluss gemäß Art. 45 DSGVO besteht.

Die Verarbeitung in anderen Staaten ist ausgeschlossen. Erfolgt die Verarbeitung von Sozialdaten im Wege des Cloud-Computing-Dienstes muss die datenverarbeitende Stelle über eine Niederlassung im Inland verfügen. Der Auftragnehmer hat sicherzustellen, dass sämtliche gesetzlichen Anforderungen an die Verarbeitung von Sozialdaten nach § 80 SGB X und § 393 SGB V eingehalten werden.

Hinweis:
Sollte für einen Drittstaat kein Angemessenheitsbeschluss mehr bestehen, ist die Verarbeitung dort unverzüglich einzustellen und auf die oben genannten Staaten zu beschränken

Der Auftragnehmer stellt Datenminimierung, Zweckbindung, Protokollierung, Rollen-/Rechte-Konzepte, Incident-Prozesse sowie Lösch-/Sperrkonzepte sicher und liefert dafür prüffähige Evidenzen. Unterauftragnehmer werden nur nach vorheriger Zustimmung der Auftraggeberin und unter Sicherstellung gleichwertiger Schutzmaßnahmen eingebunden.

Sofern Vertrauensdienste eingesetzt werden, berücksichtigt der Auftragnehmer die eIDAS-Verordnung (u. a. elektronische Signaturen, Siegel, Zeitstempel, elektronische Zustelldienste, Website-Zertifikate).

Anforderungen an die Örtlichkeit:

Der Leistungsort muss sich im Inland, in einem Mitgliedstaat der Europäischen Union, in einem nach § 35 Abs. 7 SGB I gleichgestellten Staat (insbesondere EWR-Staaten und Schweiz) oder in einem Drittstaat, für den ein Angemessenheitsbeschluss gemäß Art. 45 DSGVO besteht, befinden. Die für die Auftraggeberin eingesetzten Mitarbeitenden sind in räumlich abgegrenzten, abschließbaren und gegen unbefugten Zutritt gesicherten Bereichen einzusetzen. Der Auftragnehmer hat durch geeignete organisatorische und technische Maßnahmen sicherzustellen, dass unbefugte Personen keinen Zugriff auf die im Rahmen der Leistungserbringung verarbeiteten Daten und Informationen erhalten. Der Auftragnehmer hat die geltenden arbeitsschutzrechtlichen Vorschriften einzuhalten und geeignete Arbeitsbedingungen für die eingesetzten Mitarbeitenden sicherzustellen.

Governance, DSB, Vertraulichkeit:

Der Auftragnehmer bestellt einen Datenschutzbeauftragten gem. Art. 37 ff. DSGVO i. V. m. §§ 38, 39 BDSG und verpflichtet alle eingesetzten Personen vor Erstzugriff schriftlich zur Vertraulichkeit, einschließlich der Verpflichtung auf das Sozialgeheimnis. Ein aktuelles, revisionssicheres Register dieser Verpflichtungen ist zu führen und auf Anforderung vorzulegen.

Privacy & Security by Design/Default:

Der Auftragnehmer verankert Art. 25 und 32 DSGVO durchgängig in Architektur, Parametrierung, Änderungen und Betrieb. Dazu gehören mindestens: wirksame Rollen-/Berechtigungskonzepte (Need-to-know/Least-Privilege, Trennung privilegierter von fachlichen Rechten), Pseudonymisierung/Verschlüsselung, Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit, Wiederherstellungsfähigkeit bei Störungen sowie ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der TOM-Wirksamkeit. Bei der Auswahl konkreter Maßnahmen berücksichtigt der Auftragnehmer anerkannte Empfehlungen wie die Technischen Richtlinien/IT-Grundschutz des BSI.

Auftragsverarbeitung & Unterauftragsverhältnisse:

Der Auftragnehmer stellt prüffähige Auftragsverarbeitungsunterlagen nach Art. 28 DSGVO bereit (u. a. Gegenstand/Zweck, Kategorien von Daten/Beschäftigten, TOM, Lösch-/Rückgabekonzepte, Audit-/Informationsrechte). Unterauftragnehmer werden nur nach vorheriger Zustimmung der Auftraggeberin eingebunden; Pflichten sind inhaltlich gleichwertig per B2B-Verträge weiterzugeben. Beabsichtigte Änderungen bei Unterauftragnehmern sind der Auftraggeberin rechtzeitig mitzuteilen (Art. 28 Abs. 2, 4) und bedürfen der Genehmigung der Auftraggeberin

Betroffenenrechte & Unterstützungspflichten:

Der Auftragnehmer betreibt Ende-zu-Ende-Prozesse zur rechtssicheren Wahrnehmung der Rechte nach Art. 12–22 DSGVO (Information, Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch, Datenübertragbarkeit). Diese umfassen Identitätsprüfung, fristgerechte fachlich/technische Umsetzung, Dokumentation und revisionssichere Nachweisführung; hierfür stellt der Auftragnehmer der Auftraggeberin unverzüglich erforderliche Informationen und Systemfunktionen bereit (Art. 28 Abs. 3 lit. e).

Verarbeitungsverzeichnisse:

Der Auftragnehmer führt ein eigenes Verzeichnis der Kategorien von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO für alle im Auftrag durchgeführten Verarbeitungen und liefert der Auftraggeberin die für dessen Verzeichnis nach Art. 30 Abs. 1 erforderlichen Informationen zu den durch den Auftragnehmer erbrachten Verarbeitungsvorgängen. (Primärpflichten für das Verzeichnis des Verantwortlichen verbleiben bei der Auftraggeberin; der Auftragnehmer liefert die zu seiner Verarbeitung gehörigen Angaben.)

Datenschutz-Folgenabschätzung (DSFA) & Risikomanagement:

Für neue oder wesentlich geänderte Verarbeitungen mit voraussichtlich hohem Risiko führt der Auftragnehmer eine DSFA nach Art. 35 DSGVO durch, dokumentiert Auslöser, Risikobewertungen, Maßnahmen und Wirksamkeitsnachweise und verzahnt dies mit seinem ISMS/Risikomanagement; außerdem unterstützt der Auftragnehmer die Auftraggeberin bei dessen DSFA-Pflichten (Art. 28 Abs. 3 lit. f).

Technische und organisatorische Maßnahmen (TOM):

Der Auftragnehmer implementiert und betreibt TOM gem. Art. 32 DSGVO unter Berücksichtigung des Risikos (z. B. Vernichtung, Verlust, Veränderung, unbefugte Offenlegung/Zugang). Hierzu zählen insbesondere Pseudonymisierung/Verschlüsselung, Sicherstellung von C-I-A-B (Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit), rasche Wiederherstellung nach physischen/technischen Zwischenfällen sowie ein Verfahren zur regelmäßigen Evaluierung der TOM-Wirksamkeit; die Vorgaben des BDSG werden – soweit anwendbar – einbezogen.

Daten Portabilität (Art. 20 DSGVO):

Der Auftragnehmer stellt – soweit für ihn als Auftragsverarbeiter technisch erforderlich – Funktionen bereit, um personenbezogene Daten in offenen, strukturierten, gängigen und maschinenlesbaren Formaten mit samt relevanter Metadaten/Protokollinformationen ausleiten zu können (z. B. HL7-FHIR/IHE-Profile, XML, JSON, CSV, soweit einschlägig).

EU-Data-Act-Konformität:

Für Datenverarbeitungsdienste beachtet der Auftragnehmer die Switching-/Portierungsanforderungen des EU Data Act, insbesondere Transparenz- und Informationspflichten zu Verfahren, Methoden und Formaten sowie technischen Beschränkungen (Art. 26), mit Blick auf Anbieterwechsel und Interoperabilität von Datenverarbeitungsdiensten; der Auftragnehmer richtet Prozesse und Vertragsunterlagen entsprechend aus.

Überwachung und Nachweise:

Der Auftragnehmer betreibt ein ISMS-kompatibles, revisionssicheres Datenschutzmanagementsystem der relevanten Prozesse (u. a. DSAR-Fristen, AV-/NDA-Gültigkeiten, Unterauftragnehmer-Änderungen, Umsetzung der Privacy-Kontrollen, Abarbeitung von Audit/DSFA-Findings) mit definierten Schwellwerten und Eskalationen. In abgestimmten Intervallen berichtet der Auftragnehmer in verständlicher Form (Management-Summary/Dashboard/Tabellen) mindestens zum Status von AV-Verträgen und NDAs (Gültigkeiten/Abdeckung), zum Unterauftragnehmer (Einsatz je Leistung/Projekt, Konformität, Historie), zu DSFA/PIA (Status, Risiken, Maßnahmen), zu Audit-/Kontrollergebnissen (Abweichungen, Kritikalität, Korrektur-/Wirksamkeitsnachweise) sowie zu relevanten regulatorischen Änderungen mit Auswirkungen auf die Auftragsverarbeitung oder TOM. Abweichungen behebt der Auftragnehmer fristgebunden und dokumentiert den Nachweis der Wirksamkeit.

Datenschutzvorfälle:

Handelt der Auftragnehmer als Auftragsverarbeiter, meldet er ohne unangemessene Verzögerung jeden ihm bekannt gewordenen personenbezogenen Datenvorfall an den Verantwortlichen der Auftraggeberin und liefert unverzüglich alle Informationen, die der Auftraggeberin für seine Behördenmeldung nach Art. 33 DSGVO benötigt (u. a. Art und Umfang des Vorfalls, betroffene Kategorien/Umfang von Daten/Personen, wahrscheinliche Folgen, ergriffene/empfohlene Maßnahmen). Die Behördenmeldung binnen 72 Stunden trifft den Verantwortlichen; der Auftragnehmer unterstützt diese sowie – sofern erforderlich – die Benachrichtigung betroffener Personen nach Art. 34 DSGVO (z. B. durch Textbausteine, FAQ, Hotline-Prozesse). Alle Bewertungen (Risiko, Ursache, Folge) sowie Abhilfemaßnahmen und „Lessons Learned“ müssen nachvollziehbar dokumentiert werden.

14.4.2 Anforderungen der Informationssicherheit

Die Auftraggeberin ist Betreiberin einer kritischen Anlage im Sinne des BSI-Gesetzes (BSIG) und betreibt ein Informationssicherheitsmanagementsystem (ISMS) auf Grundlage der ISO/IEC 27001:2022.

Der Auftragnehmer ist verpflichtet, bei der Erbringung der vereinbarten Dienstleistungen ein angemessenes Informationssicherheitsniveau nach dem Stand der Technik sicherzustellen.

Die Anforderungen gelten für sämtliche vom Auftragnehmer eingesetzten Personen, Prozesse, IT-Systeme, Endgeräte, Kommunikationsverbindungen und Unterauftragnehmer, soweit diese für die Leistungserbringung genutzt werden oder Informationen beziehungsweise Systeme der Auftraggeberin betreffen.

Der Auftragnehmer muss über dokumentierte organisatorische Regelungen zur Informationssicherheit verfügen. Diese müssen insbesondere Verantwortlichkeiten, Risikomanagement, Berechtigungsmanagement, Sicherheitsvorfälle, Schwachstellenmanagement und Notfallmanagement abdecken.

Ein bestehendes ISMS nach ISO/IEC 27001 oder ein vergleichbarer strukturierter Ansatz kann als Nachweis herangezogen werden.

Der Auftragnehmer muss vor der Aufnahme des produktiven Betriebs das Sicherheitskonzept auf Basis der beigefügten Anlage 11 erstellen, der Auftraggeberin vorlegen und dieses mit ihr abzustimmen. Das Sicherheitskonzept ist bei wesentlichen Änderungen zu aktualisieren, mindestens aber jährlich.

Der Auftragnehmer muss die mit seiner Leistungserbringung verbundenen Informationssicherheitsrisiken bewerten, dokumentieren und geeignete Maßnahmen zur Risikobehandlung umsetzen. Sicherheitsrisiken, die Systeme, Informationen oder Geschäftsprozesse der Auftraggeberin betreffen, sind der Auftraggeberin mitzuteilen. Wesentliche Restrisiken bedürfen vor Aufnahme des produktiven Betriebs einer dokumentierten Entscheidung der Auftraggeberin.

Der Zugriff auf Bestandssysteme der Auftraggeberin darf ausschließlich über die von der Auftraggeberin freigegebenen Zugangsverfahren erfolgen.

Der Auftragnehmer darf keine eigenständigen Netzwerkverbindungen, Fernzugriffslösungen oder technischen Schnittstellen zu Systemen der Auftraggeberin ohne deren vorherige Freigabe einrichten.

Für sämtliche zugriffsberechtigten Beschäftigten sind persönliche Benutzerkennungen zu verwenden. Die gemeinsame Nutzung von Benutzerkonten ist unzulässig. Die von der Auftraggeberin festgelegten Authentifizierungsverfahren, insbesondere eine gegebenenfalls vorgeschriebene Mehrfaktor-Authentifizierung, sind verbindlich einzuhalten.

Zugriffsrechte dürfen ausschließlich entsprechend den übertragenen Aufgaben und nach dem Prinzip der minimal erforderlichen Berechtigungen vergeben werden.

Der Auftragnehmer muss sicherstellen, dass:

- ausschließlich autorisierte Beschäftigte Zugriff erhalten,
- Berechtigungen regelmäßig überprüft werden,
- Rollen- und Personalwechsel unverzüglich berücksichtigt werden,
- Zugriffe ausgeschiedener Beschäftigter unverzüglich gesperrt werden,
- administrative Berechtigungen gesondert geschützt werden.

Für die Verarbeitung von Informationen der Auftraggeberin dürfen ausschließlich freigegebene und angemessen geschützte Endgeräte eingesetzt werden.

Diese müssen insbesondere über aktuelle Sicherheitsupdates, Schutz vor Schadsoftware, angemessene Zugriffssicherung und eine kontrollierte Softwareinstallation verfügen.

Die private Nutzung von Endgeräten zur Verarbeitung von Informationen der Auftraggeberin ist ohne ausdrückliche Freigabe untersagt.

Der Auftragnehmer muss sicherstellen, dass Informationen der Auftraggeberin nicht unberechtigt gespeichert, kopiert, ausgedruckt, übertragen oder an Dritte weitergegeben werden.

Insbesondere sind lokale Datenexporte, externe Speichermedien, private Kommunikationsdienste und nicht freigegebene Anwendungen zu unterbinden beziehungsweise durch die Auftraggeberin ausdrücklich freizugeben.

Der Auftragnehmer muss für die von ihm verantworteten Systeme ein geregeltes Schwachstellen- und Patchmanagement betreiben. Sicherheitsrelevante Schwachstellen sind risikoorientiert zu bewerten und innerhalb angemessener Fristen zu beheben. Kritische Schwachstellen, die Auswirkungen auf die Auftraggeberin haben können, sind unverzüglich mitzuteilen. Sicherheitsrelevante Ereignisse in den vom Auftragnehmer verantworteten Systemen müssen angemessen protokolliert und überwacht werden.

Der Auftragnehmer muss sicherstellen, dass sicherheitsrelevante Ereignisse erkannt, bewertet und bei möglicher Betroffenheit der Auftraggeberin gemeldet werden.

Soweit seine Systeme in die Angriffserkennung der Auftraggeberin eingebunden werden müssen, hat der Auftragnehmer die hierfür erforderlichen technischen und organisatorischen Voraussetzungen bereitzustellen.

Der Auftragnehmer muss ein dokumentiertes Verfahren zur Erkennung, Behandlung und Meldung von Informationssicherheitsvorfällen betreiben. Sicherheitsvorfälle mit tatsächlichen oder möglichen Auswirkungen auf Informationen, Systeme oder Dienstleistungen der Auftraggeberin sind unverzüglich, spätestens innerhalb von 60 Minuten nach Erkennung, über die vereinbarten Meldewege mitzuteilen.

Der Auftragnehmer muss die Auftraggeberin bei der Bewertung, Eindämmung, Aufklärung und Dokumentation des Sicherheitsvorfalls unterstützen.

Hierfür sind geeignete Kontakt- und Eskalationswege einschließlich einer 24/7-Erreichbarkeit für kritische Sicherheitsvorfälle einzurichten.

Der Auftragnehmer muss über dokumentierte Verfahren zur Aufrechterhaltung beziehungsweise Wiederherstellung der beauftragten Dienstleistungen bei schwerwiegenden Störungen verfügen. Die Verfahren müssen insbesondere Ausfälle von IT-Systemen, Telekommunikationsdiensten, Standorten und wesentlichen Unterauftragnehmern berücksichtigen. Notfallverfahren sind regelmäßig zu überprüfen und zu testen. Die Ergebnisse sind auf Anforderung vorzulegen.

Der Einsatz von Cloud-Diensten, über die Informationen der Auftraggeberin verarbeitet werden, ist vorab offenzulegen und bedarf der schriftlichen Freigabe durch die Auftraggeberin.

Für Cloud-Dienste, die Sozial- oder Gesundheitsdaten verarbeiten, müssen die einschlägigen Anforderungen des § 393 SGB V erfüllt werden. Insbesondere sind die gesetzlich erforderlichen Sicherheitsnachweise, grundsätzlich ein aktuelles C5-Typ-2-Testat oder ein gesetzlich zulässiger gleichwertiger Nachweis, vorzulegen. Der Auftragnehmer muss den Geltungsbereich der Nachweise, die Verarbeitungsstandorte und die Umsetzung der für Cloud-Kunden vorgesehenen Sicherheitsmaßnahmen dokumentieren.

Der Einsatz von Unterauftragnehmern, die Informationen der Auftraggeberin verarbeiten oder Zugriff auf deren Systeme erhalten, bedarf der vertraglich vorgesehenen vorherigen Genehmigung. Der Auftragnehmer muss sicherstellen, dass die für die jeweilige Tätigkeit einschlägigen Informationssicherheitsanforderungen auch von seinen Unterauftragnehmern eingehalten werden. Die Auftraggeberin ist über wesentliche Änderungen der Unterauftragsnehmerstruktur zu informieren.

Die Auftraggeberin ist berechtigt, die Einhaltung der vertraglich vereinbarten Informationssicherheitsanforderungen in angemessenem Umfang selbst oder durch beauftragte Dritte zu überprüfen. Der Auftragnehmer muss die hierfür erforderlichen Informationen bereitstellen und bei der Durchführung von Prüfungen mitwirken. Festgestellte Sicherheitsmängel sind innerhalb vereinbarter, risikoorientierter Fristen zu beheben.

Der Auftragnehmer muss wesentliche technische oder organisatorische Änderungen, die Auswirkungen auf die Informationssicherheit der Auftraggeberin haben können, vor ihrer Umsetzung anzeigen. Änderungen der gesetzlichen und regulatorischen Anforderungen sind im Rahmen der vertraglich vereinbarten Zuständigkeiten zu bewerten und erforderliche Anpassungen abzustimmen.

Bei Beendigung des Vertrags muss der Auftragnehmer sämtliche Zugriffsberechtigungen auf Systeme der Auftraggeberin beenden und die in seinem Verantwortungsbereich gespeicherten Informationen nach Weisung der Auftraggeberin zurückgeben oder nachweisbar löschen, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Die sichere Übergabe und Beendigung der Dienstleistungen sind durch ein abgestimmtes Exit-Verfahren sicherzustellen.

Der Auftragnehmer muss die Auftraggeberin bei der Erfüllung der auf die beauftragte Leistung bezogenen Pflichten aus dem BSIG, insbesondere den §§ 30 bis 32 und 39 BSIG, unterstützen.

Dies umfasst die Bereitstellung relevanter Sicherheitsinformationen, die Mitwirkung bei Sicherheitsprüfungen sowie die Unterstützung bei der Bewertung und Meldung erheblicher Sicherheitsvorfälle. Eine eigenständige KRITIS-Einstufung des Auftragnehmers ergibt sich nicht allein aus dieser vertraglichen Verpflichtung.

Der Auftragnehmer muss die für seine Leistung relevanten und von der Auftraggeberin benannten Sicherheitsanforderungen des einschlägigen branchenspezifischen Sicherheitsstandards für gesetzliche Kranken- und Pflegeversicherungen (B3S-GKV/PV) berücksichtigen.

Die konkret anzuwendenden Anforderungen werden durch die Auftraggeberin auf Grundlage der Leistung, der eingesetzten Systeme und der jeweiligen Verantwortlichkeiten festgelegt.

Abweichungen von vereinbarten Anforderungen sind vor ihrer Umsetzung mit der Auftraggeberin abzustimmen.

Sämtliche Rechte und Pflichten gelten auch für etwaige Unterauftragnehmer in der Lieferkette.

14.4.3 Anforderungen bei KI-Einsatz

Der Auftragnehmer ist verpflichtet, die Auftraggeberin rechtzeitig und umfassend über den geplanten oder tatsächlichen Einsatz von KI-Systemen zu informieren, insbesondere wenn diese Systeme Auswirkungen auf die Art und Weise der Leistungserbringung, die Qualität oder die Ergebnisse der erbrachten Leistungen haben können. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch KI-Systeme darf nur mit ausdrücklicher Zustimmung der Auftraggeberin erfolgen.

Auf Verlangen der Auftraggeberin stellt der Auftragnehmer detaillierte, prüffähige Informationen zu den eingesetzten KI-Technologien, deren Funktionsweise, Leistungsgrenzen, Risiken und Vorteilen zur Verfügung. Dies umfasst insbesondere Angaben zur Systemarchitektur, zu den eingesetzten Algorithmen, zu Trainings- und Testdaten, zu Maßnahmen der menschlichen Aufsicht sowie zu etwaigen Änderungen während des Lebenszyklus des KI-Systems.

Der Auftragnehmer übernimmt die vollständige Verantwortung für den sachgerechten, sicheren und rechtskonformen Einsatz sämtlicher im Rahmen der Leistungserbringung eingesetzten KI-Systeme. Er gewährleistet, dass die eingesetzten KI-Systeme den vertraglichen Anforderungen sowie allen einschlägigen gesetzlichen und technischen Standards, insbesondere den Vorgaben der KI-VO und der DSGVO, entsprechen. Der Auftragnehmer verpflichtet sich, sämtliche erforderlichen technischen und organisatorischen Maßnahmen zur Sicherstellung von Datenschutz, IT-Sicherheit und Nachvollziehbarkeit zu ergreifen. Dies umfasst insbesondere:

- die Implementierung eines wirksamen Risikomanagementsystems für KI-Systeme, einschließlich einer fortlaufenden Bewertung und Dokumentation der Risiken für Gesundheit, Sicherheit und Grundrechte gemäß Anhang IV der KI-VO,
- die Durchführung und Dokumentation von Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO und Grundrechtefolgenabschätzung nach Art. 27 KI-VO, soweit erforderlich,
- die Sicherstellung, dass alle KI-Systeme vor unbefugtem Zugriff, Datenverlust oder Missbrauch geschützt sind, durch geeignete technische und organisatorische Maßnahmen nach Art. 32 DSGVO und Anhang IV der KI-VO,
- die lückenlose Dokumentation des Entwicklungs-, Trainings- und Einsatzprozesses der KI-Systeme, einschließlich der eingesetzten Daten, Algorithmen, Systemarchitektur und Cybersicherheitsmaßnahmen,

- die regelmäßige Kontrolle und Auditierung der eingesetzten KI-Systeme sowie die Nachweisführung über die Einhaltung aller relevanten Datenschutz- und Sicherheitsanforderungen,

- die Auswahl und Schulung von Mitarbeitern oder Dienstleistern, die mit dem Betrieb und der Nutzung der KI-Systeme befasst sind, um ein ausreichendes Maß an KI-Kompetenz sicherzustellen.

Der Auftragnehmer haftet für sämtliche Verstöße gegen die vertraglichen, gesetzlichen und technischen Vorgaben im Zusammenhang mit dem Einsatz von KI-Systemen und stellt die Auftraggeberin von allen daraus resultierenden Schäden und Ansprüchen Dritter frei.

Die Auftraggeberin ist berechtigt, den Einsatz von KI-Technologien, insbesondere im Hinblick auf die Qualität und Verlässlichkeit der erbrachten Leistungen, zu überprüfen. Stellt die Auftraggeberin fest, dass KI-gestützte Prozesse zu ungenauen, fehlerhaften oder unzulänglichen Ergebnissen führen, ist der Auftragnehmer verpflichtet, unverzüglich geeignete Maßnahmen zur Fehlerbehebung und Wiederherstellung der Leistungsqualität zu ergreifen.

Ergeben sich während der Vertragslaufzeit Änderungen im Bereich der KI-Technologien oder der rechtlichen Rahmenbedingungen (z. B. neue gesetzliche Anforderungen oder technische Standards), werden die Parteien die Vereinbarung im Rahmen des vergaberechtlich Zulässigen anpassen, um den neuen Gegebenheiten Rechnung zu tragen.

14.5 Nachweispflichten des Auftragnehmers

Der Auftragnehmer hat die nachfolgend aufgeführten Zertifikate/Testate durch unabhängige Dritte (z. B. akkreditierte Stellen oder Prüfgesellschaften) nachzuweisen und diese während der gesamten Vertragslaufzeit aufrechtzuerhalten. Der Nachweis erstreckt sich auf sämtlichen vertragsgegenständlichen Leistungen, Standorte und IT-Services einschließlich aller relevanten Unterauftragnehmer und ggfs. genutzten Cloud-Dienste. Die entsprechenden Nachweise sind dem Auftraggeber in prüffähiger Form vorzulegen.

- ISO/IEC 27001:2022 (Informationssicherheits-Managementsystem), zertifiziert durch eine nach ISO/IEC 17021 akkreditierte Zertifizierungsstelle oder auch gleichwertige Nachweise, sofern der Bieter nachweist, dass die angebotene Leistung die Anforderungen der ISO/IEC 27001:2022 gleichermaßen erfüllt und die Gleichwertigkeit durch geeignete Unterlagen, wie z. B. eine technische Beschreibung oder einen Prüfbericht einer akkreditierten Konformitätsbewertungsstelle, belegt wird;

ggfs. für vertragsgegenständliche Cloud-Leistungen: aktuelles BSI C5-Testat (derzeit C5:2020, Typ 2) durch eine unabhängige, akkreditierte Prüfgesellschaft nach und hält dieses während der gesamten Vertragslaufzeit aufrecht. Nach finaler Veröffentlichung des BSI C5:2025 (Typ 2) stellt der Auftragnehmer sicher, dass der Umstieg auf C5:2025 (Typ 2) spätestens innerhalb von 6 Monaten erfolgt, sofern keine strengeren gesetzlichen Fristen gelten. Sofern für neu erbrachte Leistungen noch kein C5-Testat besteht und diese im Zuge der Leistungserbringung neu aufgebaut werden, ist das C5 Typ 1 Testat spätestens 6 Monate nach der ersten Leistungserbringung nachzuweisen; das C5 Typ 2 Testat spätestens weitere 6 Monate später. Handelt es sich um eine Erweiterung eines bestehenden C5 Typ 2 Testats auf neu erbrachte Leistungen, ist das erweiterte Testat spätestens 3 Monate nach der ersten Leistungserbringung nachzuweisen.

14.6 AUDIT-Rechte

Zur Sicherstellung der vertraglich vereinbarten Qualität, Sicherheit, Verfügbarkeit, Compliance und der rechtskonformen Verarbeitung von Daten erhält die Auftraggeberin und seine Gesellschafterorgane und die von ihm beauftragten Dritte ein umfassendes Auditrecht gegenüber dem Auftragnehmer. Dieses Auditrecht umfasst sämtliche gesetzlichen und vertraglichen Anforderungen, einschließlich, aber nicht beschränkt auf, die Vorgaben aus der Datenschutz-Grundverordnung (DSGVO), dem Bundesdatenschutzgesetz (BDSG), dem Handelsgesetzbuch (HGB), dem Gesetz gegen Wettbewerbsbeschränkungen (GWB), dem Energieeffizienzgesetz (EnEfG), den einschlägigen KRITIS-Regelungen sowie die Umsetzungspflichten aus der NIS2-Richtlinie (Umsetzungsgesetz 2025) und dem Cyber Resilience Act (CRA) der EU. Insbesondere ist sicherzustellen, dass Nachweise über Software-Stücklisten (SBOM) vorgelegt werden können und die Board-Accountability gemäß NIS2 gewährleistet wird. Das Auditrecht ist so auszugestalten, dass es auch künftige gesetzliche Änderungen und regulatorische Entwicklungen berücksichtigt.

Die Auftraggeberin sowie seine Gesellschafterorgane und von ihm beauftragte Dritte (z. B. interne Revision, Wirtschaftsprüfer, externe Auditoren) müssen berechtigt sein, Audits in angemessenem Umfang durchzuführen. Diese Audits müssen mindestens folgende Bereiche umfassen:

- Einhaltung vertraglicher Verpflichtungen,
- Betrieb, Wartung und Pflege der Systeme und Prozesse,
- Informationssicherheit und Datenschutz, einschließlich physischer Zutrittskontrollen,
- Business Continuity Management (BCM) und Risikomanagement,
- Nachweis der Einhaltung aller relevanten Gesetze und Verordnungen, einschließlich NIS2, CRA und KRITIS-spezifischer Vorgaben, C5, KI-Compliance,
- Vorlage prüffähiger und nachvollziehbarer Dokumentation von Abläufen und Prozessen,

- Prüfung der Unterauftragnehmer, einschließlich vertraglicher Durchsetzbarkeit der Auditrechte (B2B-Verträge).

Die Durchführung der Audits erfolgt nach einer vorherigen Ankündigungsfrist von mindestens fünf Arbeitstagen. Bei begründetem Verdacht auf Verstöße sind unangekündigte Audits zulässig. Der Auftragnehmer muss der Auftraggeberin Zugang zu allen erforderlichen Unterlagen, Systemen, Berichten und Räumlichkeiten gewähren und eine fachkundige Begleitperson zur Verfügung stellen. Darüber hinaus ist die Auftragnehmerin verpflichtet, umfassend zu kooperieren, Fragen zu beantworten und technische Einsicht zu ermöglichen. Die Audits müssen in einem für die Auftraggeberin zumutbaren Rahmen erfolgen, ohne den laufenden Betrieb unangemessen zu beeinträchtigen. Für die Auftraggeberin dürfen hierbei keine Kosten entstehen, ausgenommen ihre eigenen Aufwendungen.

Der Auftragnehmer ist verpflichtet, alle relevanten Prozesse, technischen Maßnahmen und Abläufe revisionssicher zu dokumentieren und diese Nachweise/Dokumente auf Anforderung bereitzustellen. Auditoren sind umfassende Nachweise wie Prüfprotokolle, Sicherheitsberichte, Zertifikate und Systemdokumentationen unmittelbar zur Verfügung zu stellen. Zudem muss der Auftragnehmer sicherstellen, dass die Auditrechte auch entlang der gesamten Lieferkette uneingeschränkt und durchgängig vertraglich durchsetzbar sind (B2B-Verträge).

Alle im Rahmen von Audits erhaltenen Informationen unterliegen der Vertraulichkeit. Geschäfts- und Betriebsgeheimnisse des Auftragnehmers sind angemessen zu schützen. Veröffentlichungen von Auditergebnissen erfolgen ausschließlich in Abstimmung mit dem Auftragnehmer. Festgestellte Verstöße oder Mängel sind vom Auftragnehmer fristgerecht zu beheben. Bei schwerwiegenden oder wiederholten Verstößen ist die Auftraggeberin berechtigt, vertraglich definierte Maßnahmen zu ergreifen, einschließlich Eskalationsverfahren, Vertragsstrafen oder Sonderkündigungsrecht.

Audits sollen mindestens einmal jährlich sowie risikobasiert durchgeführt werden. Der Auftragnehmer soll aktuelle Prüf- und Zertifizierungsnachweise (z. B. ISO/IEC 27001, EN ISO 22301, BSI C5 > C5-Testat (Typ 2) oder ISAE 3000, Type 2 ISAE 3402 Report oder IDW PS 951 Type 2) proaktiv bereitstellen. Ferner muss der Auftragnehmer ein internes Compliance- und Auditprogramm betreiben, das auch künftige gesetzliche Änderungen und KRITIS-spezifische Entwicklungen berücksichtigt. Unterauftragnehmer sollen regelmäßig einer eigenen Auditierung durch den Auftragnehmer unterzogen werden.

Die Auftraggeberin kann für spezielle Prüfgebiete externe Fachleute hinzuziehen. Audits können auch virtuell oder mithilfe automatisierter Monitoring-Lösungen erfolgen. Die Ergebnisse können durch die Auftraggeberin für Governance- und Berichtspflichten gegenüber Aufsichtsbehörden oder Gremien verwendet werden. Der Auftragnehmer kann Nachweise in Form international anerkannter Standards oder Zertifizierungen erbringen, sofern diese den gesetzlichen Anforderungen genügen.

14.7 Rechtsgrundlagen

Die Auftraggeberin ist eine gesetzliche Krankenkasse und unterliegt den nicht abschließend aufgeführten Vorschriften.

Die nicht abschließenden aufgeführten Rechtsgrundlagen müssen vom Auftragnehmer angewendet werden. Von EU-Recht abgeleitete nationale Gesetze müssen angewendet werden.

EU-Recht:

- Datenschutz-Grundverordnung (DSGVO) (u. a. Art. 6, 9, 12–22, 25, 28, 30, 32–35).
- Richtlinie (EU) 2022/2555 (NIS 2-Richtlinie).
- Verordnung (EU) 2024/1689 (Artificial Intelligence Act).
- Verordnung (EU) 2023/2854 (Data Act).
- Verordnung (EU) 910/2014 (eIDAS).

Bundesrecht (Deutschland)

- BSI-Gesetz (BSIG), insbesondere § 8a (Stand der Technik, Nachweis) und § 8b (Meldepflichten).
- Bundesdatenschutzgesetz (BDSG) (u. a. § 38).
- Landesdatenschutzgesetz Baden-Württemberg (LDSG BW)
- Sozialgesetzbuch (SGB): SGB I § 35 (Sozialgeheimnis), SGB X §§ 67 ff., § 80 (Auftragsverarbeitung Sozialdaten), SGB V §§ 392, 393, 103a, 217f Abs. 4c (branchen-spezifische Anforderungen, u. a. Cloud/C5-Bezug).

- NIS2UmsuCG
- eIDAS-Durchführungsgesetz bzw. Vertrauensdienstegesetz
- Energieeffizienzgesetz (EnEfG)

Standards/Rahmen

- B3S GKV/PV

Soweit in diesem Hauptvertrag Normen, Gesetze oder BSI-Kriterien genannt sind, gelten sie in der jeweils aktuellen, auf die Leistung anwendbaren Fassung.