

Datenschutz, Geheimhaltung und Sicherheitsstandards

Stand: 01.10.2026

A. Datenschutz

I. Einhaltung des Datenschutzes durch den (potentiellen) Auftragnehmer

1. Einhaltung der Datenschutzbestimmungen

Beide Parteien werden sicherstellen, dass in ihrem Verantwortungsbereich die für sie jeweils geltenden einschlägigen Regelungen zum Datenschutz, insbesondere die Datenschutz-Grundverordnung (DSGVO), das Bundesdatenschutzgesetz (BDSG), das Bayerische Datenschutzgesetz (BayDSG) und soweit anwendbar die Anforderungen an Patientendaten, z.B. nach dem Bayerischen Krankenhausgesetz (u.a. Art. 27 Abs.4 Bayerisches Krankenhausgesetz) eingehalten werden. Der Auftragnehmer ist sich bewusst, dass er im Rahmen des Auftrags mit besonderen und sensiblen personenbezogenen Daten in Berührung kommen kann (Art. 9 DSGVO).

Der Auftragnehmer sorgt dafür, dass alle Personen, die von ihm mit der Bearbeitung oder Erfüllung des Vertrages betraut sind, zuverlässig sind und die gesetzlichen Bestimmungen über den Datenschutz beachten: er verpflichtet seine Mitarbeiter (auch freie Mitarbeiter) sowie eventuell mit vorheriger Zustimmung des Auftraggebers eingesetzte Unterauftragnehmer oder/und Nachunternehmer zur nachgewiesenen Wahrung der Vertraulichkeit in gleichem Umfang.

Personenbezogene Daten, insbesondere Patientendaten, dürfen nur zum vertraglich vorgesehenen Zweck verwendet werden. Eine davon abweichende Verwendung zu eigenen Zwecken des Auftragnehmers oder Dritten ist nicht gestattet.

2. Freigabeverfahren

Vor Leistungsbeginn wird, sofern personenbezogene Daten durch den Auftragnehmer bzw. Unterauftragnehmer im Auftrag des Auftraggebers verarbeitet werden, ein datenschutzrechtliches Freigabeverfahren durchgeführt.

3. Auftragsverarbeitungsvereinbarung sowie technische und organisatorische Maßnahmen

Werden zumindest auch personenbezogene Daten durch den Auftragnehmer im Auftrag des Auftraggebers verarbeitet, so ist eine Auftragsverarbeitungsvereinbarung gem. Art. 28 DSGVO zu schließen. Die Auftragsverarbeitungsvereinbarung ist grundsätzlich vor Vertragsschluss, bei öffentlichen Ausschreibungen ist die Auftragsverarbeitungsvereinbarung innerhalb von 14 Tagen nach Zuschlagserteilung zu schließen.

Sofern der Auftragnehmer nicht selbst Daten verarbeitet, sondern durch Unterauftragnehmer personenbezogene Daten des Auftraggebers mit dessen Zustimmung verarbeiten lässt, hat er mit diesem Unterauftragnehmer eine entsprechende Auftragsverarbeitungsvereinbarung abzuschließen. Das Weisungsrecht des Auftraggebers bleibt in Bezug auf eine Datenverarbeitung gegenüber dem Auftragnehmer uneingeschränkt erhalten.

Auf die Meldeverpflichtung gemäß Art. 33 Absatz 2 DSGVO (Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten) wird hingewiesen.

Der Auftragnehmer, ergreift soweit erforderlich, dem Stand der Technik entsprechende technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit, insbesondere der IT-Sicherheit in Bezug auf die Leistungen und die vom Auftragnehmer für deren Leistungsdurchführung genutzten Systeme. Auf die Einhaltung der Sicherheit der Verarbeitung im Sinne des Art. 32 DSGVO wird hingewiesen. Der Auftragnehmer wird dem Auftraggeber auf Anforderung bereits vor Vertragsschluss bzw. Zuschlagserteilung angemessene technische und organisatorische Maßnahmen nach Art. 32 DSGVO vorlegen, weil diese für die Entscheidung, ob ein Vertrag geschlossen bzw. der Zuschlag erteilt wird relevant sind.

Der Auftragnehmer hat dem Auftraggeber ein Verzeichnis seiner Verarbeitungstätigkeiten gemäß Art. 30 DSGVO auf Anforderung durch den Auftraggeber vorzulegen.

4. Datenschutzrechtliche Mitwirkungspflichten und Löschung von Daten

Macht ein Patient des Auftraggebers oder eine sonstige betroffene Person im Zusammenhang mit dem Vertragsverhältnis Rechte gemäß Art. 15 ff. DSGVO, insbesondere (aber nicht beschränkt) auf Auskunft (Art. 15 DSGVO), Berichtigung (Art. 16 DSGVO) oder Löschung (Art. 17 DSGVO) gegenüber einer Partei geltend, so informiert diese umgehend die jeweils andere Partei, damit diese die entsprechenden Begehren umsetzen kann. Beide Parteien verpflichten sich, diese Ansprüche im Rahmen ihres Verantwortungsbereichs zu erfüllen und sich, soweit es erforderlich sein sollte, dabei auch gegenseitig zu unterstützen.

Personenbezogene Daten sind unverzüglich zu löschen, wenn der Grund für ihre Verarbeitung weggefallen ist.

Sämtliche personenbezogenen Daten sind bei Beendigung des Vertragsverhältnisses an den Auftraggeber unaufgefordert zu übergeben oder auf dessen Verlangen unverzüglich und nachweisbar zu löschen. Vor jeder Rückgabe eines Datenträgers stellen beide Parteien die Löschung schutzwürdiger Inhalte sicher.

5. Datenübermittlung an Drittstaaten

Der Auftragnehmer wird eine Übermittlung von personenbezogenen Daten in Drittstaaten (Staaten außerhalb des Geltungsbereichs der DSGVO) grundsätzlich nicht vornehmen.

Der Auftragnehmer wird die Daten ausnahmsweise nur dann an Drittstaaten übermitteln soweit dies

- a. zur Anbahnung oder Ausführung von Verträgen erforderlich ist (z.B. im Zusammenhang mit Zahlungen an Unterauftragnehmer mit Bankverbindung / Sitz im außereuropäischen Ausland),

- b. es gesetzlich nach deutschen Recht vorgeschrieben ist (z. B. steuerrechtliche Meldepflichten) oder
- c. der Betroffene dem Auftragnehmer seine Einwilligung erteilt hat.

Unabhängig von dem vorgenannten darf eine Übermittlung in Drittstaaten auch dann nur stattfinden, wenn der Auftragnehmer vor einem Transfer die erforderlichen Maßnahmen ergriffen hat, damit die zusätzlichen Anforderungen des V. Kapitels der DSGVO eingehalten werden. Auf Aufforderung sind dem Auftraggeber die entsprechenden Nachweise dafür vorzulegen.

6. Nachweis der Datenschutzkonformität und Datenschutzbeauftragter

Der Auftragnehmer hat auf Anforderung zu den vorab genannten Punkten entsprechende Nachweise/Erklärungen/Akzeptanzbestätigungen beizufügen, die seine datenschutzrechtliche Befähigung untermauern.

Der Auftragnehmer verfügt, soweit gesetzlich erforderlich, über einen betrieblich bestellten Datenschutzbeauftragten mit der erforderlichen Fachkunde und teilt dem Auftraggeber auf Anfrage dessen Kontaktdaten mit.

II. Einhaltung des Datenschutzes durch das LMU Klinikum

1. Datenabfrage im Vergabeverfahren: Gesetzliche Grundlagen

Der Auftraggeber ist öffentlicher Auftraggeber im Sinne des § 99 GWB und als solcher gesetzlich verpflichtet, öffentliche Aufträge im Wege eines Vergabeverfahrens zu vergeben. In diesem Zusammenhang kann es insbesondere zur Prüfung der Eignung der Bieter und der späteren Angebote erforderlich sein, personenbezogene Daten, z.B. der Namen und Kontaktdaten der Mitarbeiter der Bieter, abzufragen. Die abgefragten Informationen können personenbezogene Daten nach Art. 4 Nr.1 DSGVO beinhalten. Im Rahmen ihrer Verfahrensbeteiligung obliegt es den Bietern, die abgefragten Informationen bereitzustellen. Sofern sie diese Informationen nicht bereitstellen, muss der Auftraggeber sie gegebenenfalls vom Vergabeverfahren ausschließen.

Zur Verarbeitung personenbezogener Daten ist der Auftraggeber gemäß Art. 6 Abs. 1 lit. b), c) und lit. e) DSGVO berechtigt.

2. Verantwortungsvoller Umgang mit Daten der Bieter

Mit der Einreichung von Unterlagen im Vergabeverfahren erklärt der Bieter gegenüber dem Auftraggeber, dass er bei der Weitergabe der Daten, die Regelungen der DSGVO und der weiteren einschlägigen Datenschutzvorschriften einhält und seinen Informationspflichten nach §§ 13, 14 DSGVO nachkommt, insbesondere die betroffenen Mitarbeiter über die Verarbeitung der Daten vorab informiert und deren Einwilligung zur Datenverarbeitung eingeholt hat. Dazu weist der Auftraggeber auf Folgendes hin:

Der Auftraggeber wird die übermittelten Daten nur für die Zwecke des Vergabeverfahrens verwenden, insbesondere die Prüfung und Wertung der Teilnahmeanträge und der Angebote, der Kommunikation mit den Bietern, der Dokumentation, zu Statistikzwecken nach der Vergabestatistikverordnung, sowie bei dem bezuschlagten Bieter für die Zwecke der Vertragsdurchführung und Vertragsabwicklung. Dabei unterliegt er den Geheimhaltungsvorschriften des GWB und der VgV.

Die Daten werden ausschließlich an Mitarbeiter des Auftraggebers sowie an vertraglich gebundene Berater des Auftraggebers, die mit dem Vergabeverfahren betraut und zur Geheimhaltung verpflichtet sind, weitergegeben.

Der Auftraggeber wird die Daten unter Beachtung der Anforderungen des V. Kapitels der DSVO an Drittstaaten übermitteln soweit dies

- a. zur Anbahnung oder Ausführung von Verträgen erforderlich ist (z.B. im Zusammenhang mit Zahlungen an Auftragnehmer mit Bankverbindung / Sitz im außereuropäischen Ausland),
- b. es gesetzlich vorgeschrieben ist (z. B. steuerrechtliche Meldepflichten) oder
- c. der Betroffene dem Auftraggeber seine Einwilligung erteilt hat.

Darüber hinaus übermittelt der Auftraggeber keine personenbezogenen Daten an Stellen in Drittstaaten oder internationale Organisationen.

3. Zeitlich befristete Datennutzung

Der Auftraggeber verarbeitet und speichert die Daten nur soweit und solange es für die Erfüllung vertraglicher, gesetzlicher und behördlicher Pflichten erforderlich ist.

- a. Vergaberechtlich sind gemäß § 8 Abs.4 Satz 1 VgV die Dokumentation, der Vergabevermerk, die Angebote, die Teilnahmeanträge und ihre Anlagen bis zum Ende der Laufzeit des Vertrags aufzubewahren, mindestens jedoch drei Jahre ab dem Tag des Zuschlags. Gleiches gilt nach § 8 Abs.4 Satz 2 VgV für Kopien aller abgeschlossenen Verträge, die bei Dienstleistungsaufträgen mindestens einen Auftragswert von € 1 Mio. haben.
- b. Förderrechtlich können die Aufbewahrungspflichten variieren. In Fällen der Beschaffung im Zusammenhang mit EU-geförderten Programmen beträgt die Aufbewahrungsfrist in der Regel zehn Jahre nach Ablauf des Förderprogramms;
- c. Handels- und steuerrechtlicher Aufbewahrungspflichten: Insbesondere nach dem Handelsgesetzbuch (HGB) und der Abgabenordnung (AO) betragen zwei bis zehn Jahre;
- d. Zur Erhaltung von Beweismitteln im Rahmen der gesetzlichen Verjährungsvorschriften. Nach den §§ 195 ff. des Bürgerlichen Gesetzbuches (BGB) können diese Verjährungsfristen bis zu 30 Jahre betragen. Die regelmäßige Verjährungsfrist beträgt drei Jahre;
- e. zu Zwecken der Rechnungsprüfung.

Sind die Daten für die Erfüllung vertraglicher oder gesetzlicher Pflichten nicht mehr erforderlich, werden sie regelmäßig gelöscht.

4. Rechte der betroffenen Personen

Den betroffenen Personen stehen gegenüber dem Auftraggeber alle Ansprüche und Rechte nach den Art. 15 ff. DSGVO zu. Ebenso haben die betroffenen Personen ein Beschwerderecht bei der zuständigen Aufsichtsbehörde, wenn sie der Ansicht sind, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt, Art. 77 DSGVO. Zuständige Aufsichtsbehörde ist:

Prof. Dr. Thomas Petri

Der Landesbeauftragte für den Datenschutz des Freistaats Bayern

Hausanschrift: Wagnmüllerstraße 18, 80538 München

Postanschrift: Postfach 22 12 19, 80502 München

Telefon +49 89 212672-0

Telefax +49 89 212672-50
poststelle(at)datenschutz-bayern.de

Der Verantwortliche im Sinne der Datenschutz-Grundverordnung und anderer nationaler Datenschutzgesetze der Mitgliedsstaaten der EU sowie sonstiger datenschutzrechtlicher Bestimmungen ist:

Klinikum der Ludwig-Maximilians-Universität München (LMU Klinikum)
Anstalt des öffentlichen Rechts (AöR)
vertreten durch den Ärztlichen Direktor und den Kaufmännischen Direktor
Marchioninistraße 15
81377 München
Info(at)klinikum.uni-muenchen.de
Tel.: 089 4400 0

Behördlicher Datenschutzbeauftragter des LMU Klinikums

Thomas Petschenka
Pettenkoferstraße 8a,
80336 München
E-Mail: datenschutz(at)med.uni-muenchen.de
Tel.: +49 89 4400 -5 2783

B. Geheimhaltung und Vertraulichkeit

Der Auftragnehmer verpflichtet sich, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und von als vertraulich bezeichneten Informationen nur zur Durchführung dieses Auftrags zu verwenden und zeitlich unbegrenzt vertraulich zu behandeln.

- a. Vertrauliche Informationen sind solche Informationen, die als vertraulich gekennzeichnet sind oder deren Vertraulichkeit sich aus den Umständen ergibt, unabhängig davon, ob sie in schriftlicher, elektronischer, verkörperter oder mündlicher Form mitgeteilt worden sind.
- b. Keine vertraulichen Informationen sind solche Informationen, die
 - der Öffentlichkeit auf andere Weise als durch eine Verletzung dieser Ziffer bekannt geworden sind,
 - eine Partei von einem Dritten erhalten hat, soweit dieser Dritte in Bezug auf die Informationen nicht seinerseits einer Verschwiegenheitsverpflichtung unterlag, oder
 - von einer Partei unabhängig von dem Zugang zu vertraulichen Informationen der anderen Partei entwickelt wurden oder dieser Partei bereits vorher bekannt waren.
- c. Den Parteien ist es untersagt, vertrauliche Informationen im Wege des Reverse Engineering zu erlangen. "Reverse Engineering" sind dabei sämtliche Handlungen, einschließlich des Beobachtens, Testens, Untersuchens und des Rück- sowie ggf. erneuten Zusammenbaus, mit dem Ziel, an vertrauliche Informationen zu gelangen.
- d. Die Geheimhaltungsverpflichtung nach dieser Ziffer (erster Absatz) gilt außer in den Fällen des § 5 Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) auch dann nicht, soweit die Parteien gesetzlich oder aufgrund bestands- bzw. rechtskräftiger Behörden- oder Gerichtsentscheidung zur Offenlegung der vertraulichen Information verpflichtet sind. In diesem Fall wird die jeweilige Partei die jeweils andere Partei unverzüglich über die Verpflichtung zur Offenlegung informieren.
- e. Darüber hinaus werden die Parteien im Zuge der Offenlegung kenntlich machen, dass es sich, sofern dies der Fall ist, um Geschäftsgeheimnisse handelt, und darauf hinwirken, dass von den Maßgaben des § 16 GeschGehG Gebrauch gemacht wird.
- f. Eine Weitergabe von vertraulichen Informationen an Dritte ist nur mit schriftlicher Zustimmung der jeweils anderen Partei zulässig.
- g. Als Dritter für den Auftragnehmer gelten alle natürlichen oder juristischen Personen außer
 - professionelle Berater des Auftragnehmers, soweit diese unter einer gesetzlichen oder vertraglichen Schweigeverpflichtung stehen
 - sowie alle Unternehmen, die als rechtmäßige Subunternehmer gelten.
- h. Dritte sind also auch verbundene Unternehmen des Auftragnehmers im Sinne des §§ 14 AktG. Für diese müssen schriftliche Zustimmungen eingeholt werden.

- i. Als Dritter für den Auftraggeber gelten alle natürlichen oder juristischen Personen außer,
 - die mit dem Auftraggeber verbundenen Unternehmen im Sinne des §§ 14 AktG
 - die Anbieter von Umsystemen des Auftraggebers und Dienstleister, die der Auftraggeber für diese einsetzt
 - Dritte, deren sich der Auftraggeber im Zusammenhang mit diesem Vertrag bedient, z.B. zur Erfüllung von Mitwirkungen
- j. Bei vollständiger oder teilweiser Beendigung dieses Rahmenvertrages werden die Parteien sämtliche davon betroffenen vertraulichen Informationen übergeben, oder unter vorheriger schriftlicher Zustimmung vollständig und unwiederbringlich löschen.
- k. Die Bestimmungen dieser Ziffer beschränken nicht das Recht der Parteien, Ideen, Konzepte oder Verfahrensweisen, welche die Leistungen betreffen und im Laufe der Zusammenarbeit zu allgemeinem Know-how der jeweiligen Mitarbeiter werden, weiter zu verwenden, soweit hierdurch keine Schutzrechte oder die Verpflichtung zur Geheimhaltung vertraulicher Informationen der anderen Partei oder eines Dritten verletzt werden.
- l. In einer etwaigen Übergabe vertraulicher Informationen ist keine Übertragung von Eigentums- oder Nutzungsrechten zu sehen. Alle vom Auftragnehmer gefertigten, beschafften oder ihm vom LMU Klinikum überlassenen Unterlagen verbleiben im Eigentum des Auftraggebers und sind dem LMU Klinikum jederzeit auf Verlangen, spätestens jedoch unaufgefordert mit Ablauf des Vertragsverhältnisses auszuhändigen. Ein Zurückbehaltungsrecht des Auftragnehmers ist ausgeschlossen.
- m. Die Vorschriften zur Geheimhaltung gelten für weitere fünf (5) Jahre nach Beendigung des Vertrags fort.

C. Informationssicherheit, Sicherheitsstandards (KRITIS) und Risikomanagement

1. Informationssicherheit

Auf die Leitlinie Informationssicherheit¹ und die IT-Sicherheitsrichtlinie² des Auftraggebers wird hingewiesen. Sie finden verbindliche Anwendung und sind verpflichtend durch alle Betreiber und Nutzer der IT-Systeme des Auftraggebers einzuhalten. Insbesondere gelten folgende Vorgaben:

- a. Die IT-Systeme des Auftragnehmers müssen insbesondere die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen und soweit zutreffend auch unter anderem die Anforderungen zum Umgang mit Patientendaten, womit sowohl die Sicherheit der Patientendaten als auch die Behandlungseffektivität gewährleistet wird.
- b. Der Auftragnehmer gewährleistet insbesondere die Einhaltung branchenspezifischer Sicherheitsstandards im Gesundheitswesen, insbesondere nach § 30 BSIG (vormals § 8a BSIG) sowie den jeweils aktuellen B3S-Branchenstandard und wird auf Wunsch des Auftraggebers entsprechende Maßnahmen darlegen und/oder Zertifikate zur Verfügung stellen.
- c. Der Auftragnehmer ist verpflichtet, für die IT-Sicherheit der ihm anvertrauten Daten eigenständig und selbstverantwortlich zu sorgen. Er sorgt dafür, dass sämtliche Leistungen frei von Schadprogrammen sind sowie auf Schadprogramme getestet wurden.
- d. Entdeckt der Auftragnehmer Umstände, die die IT-Sicherheit beim Auftraggeber beeinträchtigen könnten, teilt er dies dem Auftraggeber unverzüglich mit.

2. Einhaltung von Sicherheitsstandards (KRITIS), weiteren rechtlichen Regelungen sowie branchenspezifischen Anforderungen

- a. Der Auftragnehmer ist sich bewusst, dass der Auftraggeber zu den Kritischen Infrastrukturen (KRITIS) zählt: der Auftraggeber unterliegt als Betreiber einer kritischen Anlage im Gesundheitswesen den Anforderungen des BSI-Gesetzes in der Fassung des NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (BSIG n. F., in Kraft seit 6.12.2025) sowie – soweit einschlägig – des Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz, in Kraft seit 17.3.2026). Unabhängig von der KRITIS-Einordnung im Einzelfall gilt für den Auftraggeber als Krankenhaus zudem § 391 SGB V (IT-Sicherheit in Krankenhäusern). Somit muss er, falls einschlägig, den jeweils aktuellen und gültigen B3S Standard (Branchen-Standard-Sicherheits-Systeme³ nachweisen.
- b. Der Auftragnehmer ist sich bewusst, dass der Auftraggeber daneben weiteren gesetzlichen, regulatorischen und branchenspezifischen Anforderungen unterliegt, wozu insbesondere die jeweils geltenden Fassungen der nachfolgenden Regelungen zählen können: DSGVO, Bundesdatenschutzgesetz (BDSG), Bayerisches Datenschutzgesetz

¹https://cdn0.scrvt.com/4d3e519fe5939342b95c7312343779ef/6cd4d7dd6effabec/dd8ec2c2b682/Leitlinie_Informationssicherheit.pdf.

²https://cdn0.scrvt.com/4d3e519fe5939342b95c7312343779ef/cd39b39ebfe63238/398b3836da97/Richtlinie_IT_Sicherheit.pdf.

³[https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/kritis_node.html#:~:text=Kritische%20Infrastrukturen%20\(%20KRITIS%20\)%20sind%20Organisationen, andere%20dramatische%20Folgen%20eintreten%20w%C3%BCrden.](https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/kritis_node.html#:~:text=Kritische%20Infrastrukturen%20(%20KRITIS%20)%20sind%20Organisationen, andere%20dramatische%20Folgen%20eintreten%20w%C3%BCrden.)

(BayDSG), Krankenhaushygienevorschriften, Unfallverhütungsvorschriften, anwendbare Arbeitsschutzvorschriften, die allgemein anerkannten technischen, sicherheitstechnischen und arbeitsmedizinischen Regeln, Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) und sonstige IT-Sicherheitsgesetze oder das Bayerische Krankenhausgesetz (BayKrG).

- c. Soweit der Auftragnehmer als unmittelbarer Anbieter im Sinne des § 30 Abs. 2 Nr. 5 BSIG (Sicherheit der Lieferkette) anzusehen ist oder Systeme, Komponenten oder Dienstleistungen liefert, die für die Funktionsfähigkeit der IT-Systeme des Auftraggebers wesentlich sind, wirkt er im angemessenen Umfang an der Lieferkettenrisikobewertung des Auftraggebers mit und stellt hierfür auf Anforderung geeignete Nachweise, Zertifizierungen, Sicherheitskonzepte, Software-Stücklisten/SBOM zur Verfügung.
- d. Der Auftragnehmer meldet dem Auftraggeber jeden Sicherheitsvorfall, der die vom Auftragnehmer gelieferten oder betreuten Systeme, Komponenten oder Daten betrifft oder betreffen kann, unverzüglich, in der Regel innerhalb von 24 Stunden nach Bekanntwerden, damit der Auftraggeber seine eigenen gesetzlichen Meldefristen (u. a. nach § 32 BSIG) einhalten kann. Erste Informationen können vorläufig sein und sind unverzüglich zu vervollständigen.
- e. Soweit für den Auftraggeber im Anwendungsbereich des KRITIS-Dachgesetzes eine physische Risikoanalyse und Resilienzplanung erforderlich ist, unterstützt der Auftragnehmer den Auftraggeber im zumutbaren Rahmen bei der Erhebung der hierfür erforderlichen produkt- und leistungsbezogenen Informationen (z. B. Ausfallwahrscheinlichkeiten, Redundanzkonzepte, Wiederanlaufzeiten).
- f. Der Auftragnehmer wird seine diesbezüglichen Leistungen jederzeit im Einklang mit den vorgenannten Regelungen, sowie jeglichen sonstigen gesetzlichen, regulatorischen und branchenspezifischen Anforderungen die für den Auftraggeber gelten und soweit sie auf die zu erbringenden Leistungen anwendbar sind, erbringen und hieran ausrichten und, soweit angemessen und erforderlich, auf eigene Kosten selbständig und rechtzeitig anpassen.

3. Internes Risikomanagement

- a. Der Auftraggeber ist bestrebt ein dem Stand der Technik sowie den gesetzlichen, individuellen und branchenspezifischen Anforderungen gerecht werdendes Risikomanagement vorzuhalten.
- b. Der Auftraggeber richtet dementsprechend sein Risikomanagement insbesondere an den jeweils geltenden Vorgaben für kritische Anlagen (KRITIS-Dachgesetz), sonstigen Vorgaben des BSIG oder anderer IT-Sicherheitsbehörden (insb. an Krankenhäuser), dem BSI-Leitfaden „Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus“⁴ aus. Gegebenenfalls sind zusätzlich die Vorgaben des IT „KUM“-Betriebshandbuchs zu beachten, das dem Auftragnehmer, wenn einschlägig, zur Verfügung gestellt wird.

⁴https://www.kritis.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Praxis_Bevoelkerungsschutz/PiB_2_Risikoman_Krankh_Leitfaden_Auszug_CD-ROM.pdf?__blob=publicationFile.

- c. Der Auftragnehmer ist sich den hohen Anforderungen an das Risikomanagement des Auftraggebers bewusst und wird seine diesbezüglichen Leistungen dementsprechend daran ausrichten und jederzeit, soweit angemessen und erforderlich, anpassen und dem Auftraggeber bei der Erfüllung seiner gesetzlichen sowie sonstigen branchenspezifischen und individuellen Vorgaben angemessen unterstützen.

D. Sonderkündigungsrecht

Kommt der Auftragnehmer den in Punkt A, B oder C aufgeführten Pflichten schuldhaft nicht nach oder verletzt er eine dieser Pflichten vorsätzlich oder grob fahrlässig, berechtigt dies den Auftraggeber zur fristlosen Kündigung des Vertrages. Eine solche Pflichtverletzung wird auch dann angenommen, wenn dem Auftragnehmer die datenschutzrechtliche Freigabe nicht erteilt wird.