



Allgemeine Anforderungen Informationssicherheit und Datenschutz

Allgemeine Anforderungen

Als Betreiber einer kritischen Infrastruktur im Gesundheitswesen trägt der Auftraggeber besondere Verantwortung für die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von Informationen sowie den Schutz personenbezogener und insbesondere gesundheitsbezogener Daten. Die Sicherheit der Versorgung und das Vertrauen von Patientinnen und Patienten hängen maßgeblich von einem robusten Informationssicherheits- und Datenschutzniveau entlang der gesamten Liefer- und Wertschöpfungskette ab. Vor diesem Hintergrund definieren die nachfolgenden allgemeinen Anforderungen verbindliche Mindeststandards, die in Beschaffungen und Vergaben maßgeblich sind und als Vertragsbestandteil für alle Auftragnehmer gelten.

Der Anwendungsbereich erstreckt sich auf sämtliche Lieferanten, Dienstleister und Partner, die im Rahmen von Planung, Entwicklung, Lieferung, Integration, Betrieb, Wartung, Support oder Entsorgung mit Informationen, IT-Systemen, medizinischen Geräten oder Services des Auftraggebers in Berührung kommen – unabhängig davon, ob Leistungen vor Ort oder als Cloud-/Managed-Service erbracht werden. Die Pflichten gelten gleichermaßen für vom Auftragnehmer eingesetzte Unterauftragnehmer sowie die gesamte nachgelagerte Lieferkette und sind über geeignete vertragliche Regelungen sicherzustellen.

Die Anforderungen orientieren sich an geltenden gesetzlichen und regulatorischen Vorgaben, insbesondere der EU-Datenschutz-Grundverordnung (einschließlich Art. 28 und 32) und dem BDSG, dem BSI-Gesetz einschließlich KRITIS-bezogener Vorgaben (IT-Sicherheitsgesetz 2.0), sowie – soweit einschlägig – den Vorgaben aus NIS2. Zudem bilden anerkannte Standards wie der branchenspezifische Sicherheitsstandard (B3S) für die Medizinische Versorgung sowie ISO/IEC 27001/27002 und – je nach Datenverarbeitung – ISO/IEC 27701, 27017 und 27018 die fachliche Grundlage.

Auftragnehmer sind verpflichtet, angemessene technische und organisatorische Maßnahmen umzusetzen, deren Wirksamkeit nachzuweisen und Audit- sowie Einsichtsrechte des Auftraggebers zu ermöglichen. Hierzu zählen insbesondere ein wirksames Informationssicherheitsmanagement, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Zugriffs- und Berechtigungskonzepte, Verschlüsselung, Schwachstellen- und Patch-Management, sichere Softwareentwicklung, Notfall- und Wiederanlaufplanung sowie ein strukturiertes Management von Sicherheitsvorfällen einschließlich fristgerechter Meldungen von Informationssicherheits- und Datenschutzvorfällen. Datenübermittlungen an Dritte oder in Drittländer bedürfen einer rechtmäßigen Grundlage; Unterauftragnehmer sind vertraglich zu gleichwertigen Standards zu verpflichten.

Die Einhaltung ist Voraussetzung für die Teilnahme an Vergaben und den Vertragsabschluss; Verstöße können zum Ausschluss aus dem Vergabeverfahren sowie zu vertraglichen Sanktionen bis hin zur Kündigung führen. Mit Angebotsabgabe und Vertragsunterzeichnung erkennt der Auftragnehmer die vorliegenden Anforderungen als verbindlichen Bestandteil der Leistungsbeziehung an.



Allgemeine Anforderungen der Informationssicherheit

1. Alle Informationen und Daten des Auftraggebers, auf die der Auftragnehmer Zugriff hat oder die durch den Auftragnehmer verarbeitet werden, müssen durch den Auftragnehmer stets mit geeigneten technischen und organisatorischen Maßnahmen nach dem jeweils aktuellen Stand der Technik gegen Kenntnisnahme durch unbefugte Personen, unbefugte Offenlegung, unerlaubte Übermittlung, Veränderung, Vervielfältigung, Vernichtung, Verlust sowie anderweitig unbefugte Verarbeitung oder unbefugten Zugriff und Zugang und sonstigen Gefährdungen der Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität wirksam gesichert sein.
2. Alle informationstechnischen Systeme, Komponenten, Anlagen oder Anwendungen, die der Auftragnehmer im Rahmen der Leistungserbringung für den Auftraggeber betreibt, wartet oder überwacht, müssen durch den Auftragnehmer stets mit geeigneten technischen und organisatorischen Maßnahmen nach dem jeweils aktuellen Stand der Technik gegen Störungen der Verfügbarkeit, Zerstörung oder Schädigung, unbefugten Zugang sowie Zugriff oder unerlaubte Veränderungen von Einstellungen oder Konfigurationen und sonstigen Gefährdungen der Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität wirksam gesichert sein.
3. Ist im Rahmen der Leistungserbringung durch den Auftragnehmer eine Verarbeitung von Informationen und Daten oder der Betrieb informationstechnischer Systeme, Komponenten, Anlagen oder Anwendungen auf dem Betriebsgelände des Auftraggebers erforderlich, so wird der Auftragnehmer geeignete technische und organisatorische Maßnahmen ergreifen, damit es zu keiner Beeinträchtigung der technischen Infrastruktur des Auftraggebers kommt. Sofern eine Beeinträchtigung, beispielsweise aufgrund von Wartungsarbeiten, nicht vermieden werden kann, erfolgt zwingend eine vorherige Abstimmung mit dem Auftraggeber.
4. Tätigkeiten zur Fehleranalyse, bei denen ein Datenabzug von informationstechnischen Systemen, Komponenten, Anlagen oder Anwendungen des Auftraggebers erforderlich ist, bedürfen der vorherigen schriftlichen Zustimmung des Auftraggebers. Die Verarbeitung dieser Daten erfolgt ausschließlich auf Equipment des Auftraggebers oder auf solchem des Auftragnehmers, sofern die vorherige Zustimmung des Auftraggebers vorliegt. Nach Bereinigung des Fehlers sind alle Kopien der Daten, unabhängig vom verwendeten Medium, datenschutzkonform durch den Auftragnehmer zu vernichten. Die Vernichtung ist dem Auftraggeber unverzüglich schriftlich zu bestätigen.
5. Ein Zugriff auf informationstechnische Systeme, Komponenten, Anlagen oder Anwendungen des Auftraggebers darf nur mit Erlaubnis des Auftraggebers im erlaubten und für die Leistungserbringung erforderlichen Umfang – auch in zeitlicher Hinsicht – durch die dazu autorisierten Personen erfolgen. Der Auftragnehmer verpflichtet sich, die ihm zugewiesenen Zugriffsdaten gesichert zu verwahren und keinen unbefugten Personen bekannt zu geben. Sofern im Rahmen der Leistungserbringung ein Zugriff durch Unterauftragnehmer oder freien Mitarbeitenden auf informationstechnische Systeme, Komponenten, Anlagen oder Anwendungen des Auftraggebers erforderlich ist, so ist zuvor die schriftliche Zustimmung des Auftraggebers einzuholen. Der Auftragnehmer muss Unterauftragnehmer unter besonderer Berücksichtigung der Eignung hinsichtlich der Erfüllung der zwischen Auftraggeber und Auftragnehmer vereinbarten technischen und organisatorischen Maßnahmen gewissenhaft auswählen. Diesem Unterauftragnehmer müssen im Wege eines Vertrags dieselben Pflichten auferlegt werden, die in der Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind. Der Auftragnehmer informiert den Auftraggeber unverzüglich über nicht mehr benötigte Zugriffsberechtigungen, sodass der Auftraggeber diese entziehen kann.
6. Fernzugriffe auf informationstechnische Systeme, Komponenten, Anlagen oder Anwendungen des Auftraggebers sowie sämtliche in diesem Zusammenhang erforderlichen Tätigkeiten erfolgen durch den Auftragnehmer ausschließlich über das vom Auftraggeber bereitgestellte

Fernzugangssystem mit Mehrfachfaktorauthentifizierung. Der Auftragnehmer hat das vom Auftraggeber festgelegte Betriebskonzept zur Nutzung des Fernzugangs in der jeweils gültigen Fassung und die dort definierten Anforderungen zur Informationssicherheit zu befolgen. Es ist dem Auftragnehmer in keinem Fall gestattet, eigene oder fremde Fernzugangssysteme für den Fernzugriff auf informationstechnische Systeme, Komponenten, Anlagen oder Anwendungen des Auftraggebers einzusetzen. Alle Fernzugriffe werden durch den Auftraggeber dokumentiert und protokolliert. Der Auftraggeber ist berechtigt, Fernzugriffe bei und nach Durchführung zu kontrollieren sowie diese jederzeit zu verfolgen, jegliche Aktivitäten aufzuzeichnen und jederzeit abubrechen.

7. Es ist dem Auftragnehmer in keinem Fall gestattet, an informationstechnischen Systemen, Komponenten, Anlagen oder Anwendungen des Auftraggebers ohne vorherige schriftliche Genehmigung des Auftraggebers eine Internetverbindung herzustellen oder auf dem Betriebsgelände des Auftraggebers eine Internetverbindung zu schalten oder diese über einen Dritten schalten zu lassen. Dabei ist es unerheblich, mit welcher Technologie (z.B. DSL, Bluetooth, LTE oder offenes WLAN) die Internetverbindung hergestellt oder geschaltet wird.
8. Der Auftragnehmer verfügt über ein Informationssicherheitskonzept, das geeignet ist, alle vom Auftraggeber aufgeführten allgemeinen Anforderungen sowie in Lastenheften oder anderen schriftlichen Dokumenten spezifisch definierten Anforderungen an die Informationssicherheit wirksam zu erfüllen und verpflichtet sich diese einzuhalten. Das Informationssicherheitskonzept ist insbesondere hinsichtlich der spezifischen Anforderungen an die Informationssicherheit mit dem Auftraggeber abzustimmen. Der Auftraggeber ist jederzeit dazu berechtigt, einen schriftlichen Nachweis über die Umsetzung und Einhaltung des Informationssicherheitskonzepts zu verlangen.
9. Der Auftragnehmer hat den Auftraggeber über jegliche Änderungen des Informationssicherheitskonzepts sowie über wesentliche Änderung der technischen und organisatorischen Maßnahmen, die im Rahmen des Informationssicherheitskonzepts durch den Auftragnehmer umgesetzt sind, schriftlich zu informieren. Hierbei sind Umfang der Änderung und die Auswirkungen auf das Informationssicherheitskonzept für den Auftraggeber nachvollziehbar dazulegen. Bei einer absehbaren Minderung der Schutzwirkung des Informationssicherheitskonzepts ist vor Umsetzung der Änderung die vorherige schriftliche Zustimmung des Auftraggebers einzuholen.
10. Der Auftragnehmer verpflichtet sich, bei Kenntniserlangung von als auch bei begründetem Verdacht auf Verletzungen des Informationssicherheitskonzepts oder sonstigen Vorfällen, die geeignet sind, die Schutzwirkung des Informationssicherheitskonzepts in wesentlichem Ausmaß zu mindern, bereits zu einer wesentlichen Minderung der Schutzwirkung geführt haben oder die Verfügbarkeit, Vertraulichkeit, Integrität oder Authentizität von Informationen, Daten, Systemen, Komponenten, Anlagen oder Anwendungen des Auftraggebers in wesentlichem Ausmaß gefährden oder gefährdet haben (Informationssicherheitsvorfälle), unverzüglich dem Auftraggeber schriftlich mitzuteilen sowie sofort – in Abstimmung mit dem Auftraggeber – alle erforderlichen Schritte zur Aufklärung des Sachverhalts und zur Schadensbegrenzung einzuleiten.
11. Der Auftragnehmer verpflichtet sich, die gesetzlichen Vorgaben zu Datenschutz und Informationssicherheit bereits im Entwicklungsprozess und im Produktdesign umzusetzen. Im Rahmen der geteilten Verantwortlichkeit unterstützt der Auftragnehmer den Auftraggeber bei der Bewertung von Sicherheitsrisiken indem er die hierfür erforderlichen Informationen und Unterlagen aktuell und hinreichend detailliert zur Verfügung stellt, einschließlich Angaben zu Schnittstellen, Ports und Protokollen, Diensten, Kommunikationspartnern, Datenflüssen, implementierten Sicherheitsfunktionen, Update- sowie Patchprozessen sowie den bekannten Restrisiken.
12. Der Auftragnehmer benennt gegenüber dem Auftraggeber eine mit hinreichenden Befugnissen ausgestattete verantwortliche Person oder Organisationseinheit, die für sämtliche Themen der Informationssicherheit zur Verfügung steht, insbesondere im Rahmen der

Abstimmung des Informationssicherheitskonzepts sowie zur Aufklärung von Informationssicherheitsvorfällen. Hinsichtlich der festgelegten Genehmigungs- und Informationspflichten wendet sich der Auftragnehmer ausschließlich an die Stabsstelle Informationssicherheit des Auftraggebers.

Allgemeine Anforderungen des Datenschutzes

13. Sowohl der Auftragnehmer als auch dessen Mitarbeitende kommen bei der Ausübung ihrer Tätigkeit im, für und im Auftrag des Auftraggebers möglicherweise mit personenbezogenen Daten und gesetzlich geschützten Geheimnissen von Berufsgeheimnisträgern (i. S. v. § 203 StGB) in Berührung und können daher Kenntnis von solchen geschützten Daten und Geheimnissen erlangen. Der Auftragnehmer stellt sicher, dass sich die zur Verarbeitung der personenbezogenen und dem Berufsgeheimnis unterliegenden Daten des Auftraggebers befugten Mitarbeitenden sowie etwaige Unterauftragnehmer in Textform zur Wahrung der Vertraulichkeit und Einhaltung der datenschutzrechtlichen Anforderungen verpflichtet haben sowie über die ihnen bei Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Geheimnisse Stillschweigen zu bewahren und diese keinesfalls unbefugt Dritten zugänglich zu machen. Der Auftragnehmer ist dazu verpflichtet, seine Mitarbeitenden und etwaige Unterauftragnehmer über ihre Datenschutzpflichten und die mögliche Strafbarkeit nach § 203 Abs. 4 S. 1 StGB zu belehren. Die Pflicht zur Verschwiegenheit erstreckt sich nicht nur auf fremde Geheimnisse, sondern auf alle Tatsachen, Daten, Betriebs- und Geschäftsgeheimnisse sowie vertrauliche Angelegenheiten, die dem Auftragnehmer bzw. dessen Mitarbeitenden in Ausübung oder aus Anlass ihrer Tätigkeit anvertraut oder bekannt werden. Die Pflicht zur Verschwiegenheit besteht gegenüber jedermann und auch nach Beendigung der Beauftragung uneingeschränkt und zeitlich unbefristet fort.
14. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen hat der Auftragnehmer sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen getroffen, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der Datenschutz-Grundverordnung (DSGVO) zu genügen, die Rechte der betroffenen Personen zu schützen und ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
15. Der Auftragnehmer hat geeignete technische und organisatorische Maßnahmen getroffen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.
16. Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten. Sind die Voraussetzungen der Artikel 4 Nr. 8 und Artikel 28 DSGVO erfüllt, stimmen sich Auftraggeber und Auftragnehmer einvernehmlich auf einen Vertrag zur Auftragsverarbeitung ab.
17. Der Auftragnehmer stellt dem Auftraggeber die für die Übersicht nach Art. 30 DSGVO (Verzeichnis von Verarbeitungstätigkeiten) notwendigen Angaben zur Verfügung. Der Auftragnehmer unterstützt den Auftraggeber bei der Datenschutzfolgenabschätzung mit allen ihm zur Verfügung stehenden Informationen. Im Falle der Notwendigkeit einer vorherigen Konsultation der zuständigen Aufsichtsbehörde unterstützt der Auftragnehmer den Auftraggeber auch hierbei.

18. Der Auftragnehmer verfügt über ein Datenschutzkonzept, das geeignet ist, alle vom Auftraggeber aufgeführten allgemeinen Anforderungen sowie in Lastenheften oder anderen schriftlichen Dokumenten spezifisch definierten Anforderungen an den Datenschutz wirksam zu erfüllen und verpflichtet sich diese einzuhalten. Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten 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 sich aus der Prüfung/dem Audit des Auftraggebers ein Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Diese Maßnahmen muss der Auftragnehmer auf Anfrage dem Auftraggeber und ggfs. Aufsichtsbehörden gegenüber nachweisen. Dieser Nachweis beinhaltet insbesondere die Umsetzung der aus Art. 32 DSGVO resultierenden Maßnahmen. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative, nachweislich adäquate Maßnahmen umzusetzen. Dabei muss sichergestellt sein, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

19. Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftraggeber im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags wird vom Auftragnehmer unterstützt. Insbesondere verpflichtet sich der Auftragnehmer, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.

20. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten gegenüber der jeweils zuständigen Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen nach Art. 33, 34 DS-GVO.

21. Der Auftragnehmer teilt dem Auftraggeber Name und Kontaktdaten des Datenschutzbeauftragten mit. Der Auftragnehmer gewährleistet, dass die Anforderungen an den Datenschutzbeauftragten und seine Tätigkeit gemäß Art. 38 DS-GVO erfüllt werden. Sofern kein Datenschutzbeauftragter beim Auftragnehmer benannt ist, benennt der Auftragnehmer dem Auftraggeber einen Ansprechpartner. Ist der Auftragnehmer mangels Vorliegen der gesetzlichen Voraussetzungen zum gegenwärtigen Zeitpunkt nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet, ist die Bestellung eines solchen zu einem späteren Zeitpunkt bzw. ein Wechsel des Datenschutzbeauftragten dem Auftraggeber unverzüglich schriftlich mitzuteilen.