Vereinbarung zur Auftragsverarbeitung im Gesundheitswesen

Regelungen zu Datenschutz und Datensicherheit in Auftragsverhältnissen
Online-Variante, Stand Januar 2026

Zwischen

siehe Angaben zum Kunden

- Verantwortlicher –
(nachfolgend Auftraggeber genannt)

und

Deutsches Medizinrechenzentrum GmbH
Werftstraße 16
40549 Düsseldorf

- Auftragsverarbeiter –
(nachfolgend Auftragnehmer genannt)

– beide nachfolgend gemeinsam „Vertragsparteien“ genannt –

Präambel

Um die Rechte und Pflichten aus dem Auftragsdatenverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung aus Art. 28 DSGVO zu konkretisieren, die sich aus der im Vertrag über die Abrechnungs-/Zusatzleistungen nebst der diesen konkretisierenden allgemeinen Geschäftsbedingungen (im Folgenden „Hauptvertrag“) beschrieben Auftragsverarbeitung ergeben, schließen die Vertragsparteien die nachfolgende Vereinbarung.

Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

1 Gegenstand des Auftrags, Art und Zweck der Verarbeitung

(1) Abrechnung von Leistungen nach den §§ 302 SGB V, 295 sowie 105 SGB XI gegenüber Kostenträgern.

(2) Im Übrigen ergibt sich der Gegenstand des Auftrags aus dem Hauptvertrag der Parteien zur Nutzung des dmrz.de Abrechnungsservice und den vertraglich zur Verfügung gestellten Funktionen.

(3) Die Verarbeitung der personenbezogenen Daten findet grundsätzlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus

dem Gebiet der EU oder des EWR erbringen, ist nur unter den Voraussetzungen nach Art. 44ff. DSGVO möglich (z.B. Angemessenheitsbeschluss der Kommission, Standarddaten-schutzklauseln, genehmigte Verhaltensregeln).

2 Art der personenbezogenen Daten, Kategorien betroffener Personen, Leistungen des Auftragnehmers abhängig vom jeweiligen Hauptvertragsverhältnis

(1) Art der personenbezogenen Daten sind:

- Versichertendaten / Patientendaten / Kunden der Kunden: Name, Anschrift, Alter, Versichertenstatus, Versichertennummer, Krankenkasse, Verordnungen, verordnete Arzneimittel und Leistungen, erbrachte Leistungen, Indikationen, Diagnosen, Zuzahlungen

- Personenstammdaten

- Kommunikationsdaten (Fax- und Telefonnummer, E-Mail-Adresse, IP-Adressen)

- Vertragsstammdaten (z.B. Verträge und Vertragsänderungen)

- Kundenhistorie (Korrespondenz mit dem Auftraggeber)

- Planungs- und Steuerungsdaten, Krankenfahrten

- Abrechnungs- und Zahlungsdaten

(2) Bei den Betroffenen dieser Daten handelt es sich um:

- Auftraggeber / Mitarbeiter des Auftraggebers

- Versicherte

- Ärzte

- Leistungserbringer in den Bereichen:

  - Rehabilitation und Funktionstraining

  - Hilfsmittel

  - Stationäre Pflege

  - Haushaltshilfe

  - Hebammen

  - Spezielle ambulante Palliativversorgung

  - Sonstige

(3) Leistungen/Zugriff des Auftragnehmers:

Der Auftragnehmer erbringt für den Auftraggeber bezogen auf die in (1) genannten Datenarten die Leistung der Bereitstellung einer Abrechnungsplattform zur Abrechnung von Leistungen gegenüber den gesetzlichen Kostenträgern samt Zusatzfunktionen.

(4) Dem Auftragnehmer bleibt es vorbehalten, die Auftraggeber-Daten zu anonymisieren oder zu aggregieren, so dass eine Identifizierung einzelner betroffener Personen nicht mehr möglich ist, und in dieser Form zum Zweck der bedarfsgerechten Gestaltung, der Weiterentwicklung und der Optimierung sowie der Erbringung des nach Maßgabe des Hauptvertrags vereinbarten Dienstes zu verwenden. Die Parteien stimmen darin überein, dass anonymisierte bzw. nach obiger Maßgabe aggregierte Auftraggeber-Daten nicht mehr als Auftraggeber-Daten im Sinne dieses Vertrags gelten.

3 Dauer des Auftrages

(1) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung aus dem Hauptvertrag, sofern sich aus den Bestimmungen dieses Vertrages nicht etwas anderes ergibt.

(2) Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt. Kündigungen müssen schriftlich (Fax oder Mail ausreichend) erfolgen. Eine Kündigung dieses Vertrages erstreckt sich auf das Hauptvertragsverhältnis.

4 Verantwortlichkeit und Weisungsbefugnis

(1) Der Auftraggeber ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (Art. 4 Nr. 7 DSGVO). Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Etwas anderes gilt nur in dem in Absatz 2 genannten Umfang.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, es sei denn es besteht eine anderweitige Verpflichtung durch Unionsrecht oder dem Recht des Mitgliedsstaates, dem der Auftragnehmer unterliegt. Im Falle einer anderweitigen Verpflichtung teilt der Auftragnehmer dem Auftraggeber vor der Verarbeitung unverzüglich die entsprechenden rechtlichen Anforderungen mit. Die Weisungen des Auftraggebers werden vom Auftraggeber dokumentiert und dem Auftragnehmer unmittelbar nach erfolgter Dokumentation als unterschriebene Kopie zur Verfügung gestellt.

(3) Änderungen des Vertragsgegenstands und Verfahrensänderungen sind von der Weisungsbefugnis des Auftraggebers gedeckt und entsprechend zu dokumentieren. Bei einer vom Auftragnehmer als wesentlich angesehenen Änderung des Auftrags steht dem Auftragnehmer ein Widerspruchsrecht zu. Besteht der Auftraggeber trotz des Widerspruchs

des Auftragnehmers auf der Änderung, so ist diese Änderung als wichtiger Grund anzusehen und erlaubt eine fristlose Kündigung des von der Weisung betroffenen Auftragsverarbeitungsvertrages sowie der von der Auftrags-verarbeitungsvereinbarung betroffenen Bestandteile des entsprechenden Hauptvertrages.

(4) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er gemäß Art. 28 Abs. 3 S. 3 DSGVO unverzüglich den Auftraggeber. Bis zur schriftlichen (Telefax oder Mail ausreichend) Bestätigung oder Änderung der entsprechenden Weisung ist der Auftragnehmer berechtigt, die Durchführung der Weisung auszusetzen.

5 Vertraulichkeit

Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die gemäß Art. 28 Abs. 3 S. 2 lit. b DSGVO auf die Vertraulichkeit und gemäß § 203 StGB auf die Verschwiegenheit verpflichtet worden sind und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz und zur Verschwiegenheit vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

6 Datensicherheit

(1) Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen zum angemessenen Schutz der personenbezogenen Daten gemäß Art. 28 Abs. 3 lit. DSGVO in Verbindung mit Art. 32 Abs. 1 DSGVO, um die Sicherheit der Verarbeitung im Auftrag zu gewährleisten. Dazu wird der Auftragnehmer

- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, sicherstellen sowie
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung unterhalten.

Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

(2) Die Vertragsparteien vereinbaren die in **der Anlage 1 „Technische und organisatorische Maßnahmen“** zu dieser Vereinbarung niedergelegten konkreten Datensicherheitsmaßnahmen. Der Auftraggeber hat im Hinblick auf den Schutzbedarf der Daten dafür gesorgt, dass diese ausreichend sind.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber schriftlich mitzuteilen.

7 Rechte und Pflichten beim Desktop Support / Information bei außerordentlichem Zugriff

Falls Problemlösungen oder der Supportwünsche des Auftraggebers nicht im Rahmen des erweiterten Zugriffs möglich sind, kann ein Desktop-Support notwendig sein, welcher mit Einverständnis des Auftraggebers gemäß den nachstehenden Regelungen erfolgt:

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung / -erhebung / -nutzung sowie für die Wahrung der Rechte der Betroffenen ist im Rahmen des Desktop-Supports allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Ablauf des Desktop-Supports zu erteilen.

(3) Im System des Auftraggebers können alle Zugriffe des Auftragnehmers im Rahmen des Desktop-Supports protokolliert werden. Die Protokollierung darf vom Auftragnehmer nicht abgeschaltet werden.

(4) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten feststellt, die beim Desktop-Support aufgetreten sind oder die einen Zugriff durch Unbefugte möglich machen.

(5) Der Auftragnehmer führt die Datenverarbeitung, insbesondere den Desktop-Support, ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers durch.

(6) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn eine vom Auftraggeber erteilte Weisung nach seiner Meinung zu einem Verstoß gegen gesetzliche Vorschriften führen kann. Die Weisung braucht in diesem Fall nicht befolgt zu werden, solange sie nicht durch den Auftraggeber ausdrücklich bestätigt wird.

(7) Der Beginn des Desktop-Supports ist grundsätzlich anzukündigen, um den Auftraggeber die Möglichkeit zu geben, die Maßnahmen des Desktop-Supports zu verfolgen. Soll von dieser Regelung im Einzelfall abgewichen werden, so ist dies gesondert zwischen Auftraggeber und Auftragnehmer zu regeln.

(8) Desktop-Support Maßnahmen dürfen nur von solchen Systemen des Auftragnehmers vorgenommen werden, welche den technischen und organisatorischen Anforderungen des Auftragnehmers entsprechen.

(9) Wurden Daten des Auftraggebers im Zuge des Desktop-Supports kopiert, so sind diese nach Abschluss des konkreten Desktop-Supports unverzüglich zu löschen. Die Verpflichtung zur Löschung gilt nicht, solange bestimmte Daten zur Dokumentationskontrolle, für Revisionsmaßnahmen des Desktop-Supports oder für den konkreten Auftrag benötigt werden.

(10) Der Auftragnehmer wird zudem informiert, wenn interne oder externe Mitarbeiter des Auftraggebers ohne vorherige Zustimmung lesend oder schreibend auf Daten des Auftragnehmers zugreifen werden oder zugegriffen haben. Die Information je Ereignis und umfasst Anlass, Zeitpunkt, Dauer, Art und Umfang des Zugriffs, soweit die Daten des Auftragnehmers nicht verschlüsselt sind oder waren, die Verschlüsselung für den Zugriff aufgehoben wird oder wurde oder die vertraglichen Vereinbarungen eine solche Information nicht explizit ausschließen. Die Information erfolgt dergestalt, dass sachverständige Personen des Auftragnehmers eine sachgerechte Risikobewertung vornehmen können. Die Mitteilung erfolgt spätestens 72 Stunden nach dem Zugriff, sofern andere vertragliche Vereinbarungen dies nicht abweichend regeln.

(11) Für die Sicherheit erhebliche Entscheidungen zur Organisation und Durchführung des Desktop-Supports sind mit dem Auftraggeber abzustimmen.

(12) Der Auftraggeber hat das Recht, den Desktop-Support zu unterbrechen, insbesondere wenn er den Eindruck gewinnt, dass unbefugt auf Dateien zugegriffen wird.

8 Einbeziehung weiterer Auftragsverarbeiter (Subunternehmer)

(1) Als Subunternehmer im Sinne dieser Regelung gelten vom Auftragnehmer beauftragte Auftragsverarbeiter, deren Dienstleistungen sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht dazu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen und Reinigung in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Die Auslagerung auf Subunternehmer oder der Wechsel des bestehenden Subunternehmers sind zulässig. Der Auftragnehmer wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter schriftlich oder in Textform informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potentiellen weiteren Auftragsverarbeiters zu erheben. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von 3 Monaten zu kündigen.

(3) Der Vertrag zwischen dem Auftragnehmer und dem weiteren Auftragsverarbeiter muss letzterem dieselben Pflichten auferlegen, wie sie dem Auftragnehmer kraft dieses Vertrages obliegen. Die Parteien stimmen überein, dass diese Anforderung erfüllt ist, wenn der Vertrag ein diesem Vertrag entsprechendes Schutzniveau aufweist bzw. dem weiteren Auftragsverarbeiter die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegt sind.

(4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Subunternehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die durch den Auftraggeber zum Zeitpunkt des Vertragsschlusses genehmigten Subunternehmer sind in der **Anlage 2** zu diesem Vertrag aufgelistet.

(5) Erbringt der Subunternehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

9 Unterstützung bei der Wahrung von Betroffenenrechten

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftraggeber wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z.B. durch Einholung von Schweigepflichtentbindungserklärungen, Einwilligungserklärungen für die Verarbeitung der Daten) geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen rechtsverletzungsfrei erbringen kann.

(2) Der Auftragnehmer ist verpflichtet, den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Wahrung der in Art. 12 bis 22 DSGVO genannten Rechte der betroffenen Personen zu unterstützen (Art. 28 Abs. 3 S. 2 lit. e DSGVO). Insbesondere wird der

Auftragnehmer den Auftraggeber darin unterstützen, Ansprüche Betroffener auf Löschung ihrer personenbezogenen Daten gemäß Art. 17 DSGVO zu erfüllen.

(3) Der Auftragnehmer darf personenbezogene Daten nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken (Art. 28 Abs. 3 S. 2 lit. g DSGVO). Auskünfte an Dritte oder den betroffenen Personen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

(4) Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer wendet, um ihre Rechte gemäß Art. 12 bis 22 DSGVO geltend zu machen, wird der Auftragnehmer das Ersuchen unverzüglich an den Auftraggeber weiterleiten, sofern dieses eindeutig zuzuordnen ist.

10 Unterstützung bei Dokumentations- und Meldepflichten

(1) Der Auftragnehmer ist nach Art. 37 DSGVO, § 38 BDSG dazu verpflichtet, einen Datenschutzbeauftragten zu benennen. Ein/Eine Datenschutzbeauftragte/er ist beim Auftragnehmer bestellt und unter datenschutz@dmrz.de zu erreichen. Deren/Dessen jeweils aktuelle Kontaktdaten sind im Impressum oder der Datenschutzerklärung der Homepage des Auftragnehmers leicht zugänglich hinterlegt. Ein Wechsel der/des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen (z.B. per Mail oder Nachricht im Kundenkonto des Auftraggebers).

(2) Wenn dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Auftraggeber unverzüglich Art. 28 Abs. 3 lit. f, Art. 33 Abs. 2 DSGVO). Das Gleiche gilt, wenn beim Auftragnehmer beschäftigte Personen gegen diese Vereinbarung verstoßen.

(3) Nach Absprache mit dem Auftraggeber trifft der Auftragnehmer unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen.

(4) Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Erfüllung der Informationspflichten gegenüber der zuständigen Aufsichtsbehörde gemäß Art. 33 DSGVO und ggf. gegenüber den von der Verletzung des Schutzes personenbezogener Daten Betroffenen gemäß Art. 34 DSGVO.

(5) Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und ggf. bei einer vorherigen Konsultation der zuständigen Aufsichtsbehörde gemäß Art. 36 DSGVO.

(6) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen.

(7) Im Falle von Ermittlungsanfragen staatlicher Stellen informiert der Auftragnehmer den Auftraggeber nach Eingang einer Ermittlungsanfrage unverzüglich, soweit dies die Rechtsgrundlage, auf die sich die staatliche Stelle stützt, nicht untersagt oder eindeutige Hinweise auf rechtswidrige Handlungen im Zusammenhang mit der Nutzung des Dienstes vorliegen.

(8) Für Unterstützungsleistungen, die nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung in angemessenem Umfang verlangen.

11 Information und Einbindung des Auftraggebers bei Störungen (Incidents)

(1) Der Auftragnehmer informiert den Auftraggeber regelmäßig im Kundenkonto oder auf der Website des Auftragnehmers über den Status etwaiger den Auftraggeber betreffender sicherheitsrelevanter Störungen, die den Betrieb des Cloud-Dienstes beeinträchtigen oder beinträchtigen könnten (Incidents). Die Information erfolgt unverzüglich, spätestens innerhalb von 24 Stunden, und beinhaltet, soweit möglich und soweit einschlägig, Informationen über die Art des Vorfalls oder der Störung, betroffene Datenkategorien, Zeitpunkt und Dauer des Vorfalls und getroffene oder geplante Maßnahmen zur Eindämmung und Behebung.

(2) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung etwaiger Meldepflichten gemäß Art. 33, 34 DSGVO aufgrund einer solchen Störung (Incident).

(3) Der Auftragnehmer bindet den Auftraggeber, soweit dies angemessen und erforderlich ist, in die Behebung der Störung ein.

(4) Nach Behebung der Störung informiert der Auftragnehmer den Auftraggeber über die Behebung der Störung und die getroffenen Maßnahmen. Die Information erfolgt im Kundenkonto, auf der Website des Auftragnehmers oder im Falle einer individuellen Betroffenheit per Nachricht im Kundenkonto des Auftragnehmers.

12 Sicherheitsvorfälle

(1) Aufragnehmer und Auftraggeber sind gegenseitig dazu verpflichtet, Sicherheitsvorfälle, die ihnen bekannt werden und direkt mit dem vom Auftragnehmer bereitgestellten Cloud-Dienst in Verbindung stehen, zeitnah zu melden. Für Meldungen des Auftraggebers an den Auftragnehmer steht die Mailadresse dsk@dmrz sowie das Webformular www.dmrz.de/datenschutzvorfall zur Verfügung.

(2) Das Melden von Vorfällen, die sich im Nachhinein nicht als Sicherheitsvorfall („Falschmeldungen“) herausstellen, haben für den Melder keine negativen Folgen.

13 Beendigung des Auftrages

(1) Nach Abschluss der Erbringung der Verarbeitungsleistungen hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder zu löschen oder zurückzugeben,

sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

(2) Der Auftragnehmer weist dem Auftraggeber auf Anfordern in Textform mit Datumsangabe nach, dass er sämtliche Datenträger sowie sonstigen Unterlagen an den Auftraggeber herausgegeben oder datenschutzkonform vernichtet oder gelöscht und somit keine Daten des Auftraggebers zurückbehalten hat.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(4) Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

14 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, vor Beginn der Verarbeitungsleistung und währenddessen regelmäßig die technischen und organisatorischen Maßnahmen sowie die Einhaltung dieser Vereinbarung und datenschutzrechtlicher Vorgaben zu kontrollieren. Dazu kann der Auftraggeber oder ein beauftragter Prüfer die Datenverarbeitungsanlagen und die Datenverarbeitungsprogramme des Auftragnehmers inspizieren.

(2) Zu diesem Zweck ist der Auftragnehmer verpflichtet, dem Auftraggeber auf dessen Kosten, soweit nicht unerhebliche Verstöße die Kontrollen veranlasst haben. In diesem Fall übernimmt der Auftraggeber die Kosten. Kontrollen sind zu den üblichen Geschäftszeiten nach rechtzeitiger Vorankündigung ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers Zutritt zu den Räumlichkeiten zu gewähren, in denen die Daten des Auftraggebers physisch oder elektronisch verarbeitet werden. Der Auftraggeber stimmt die Durchführung der Kontrollen mit dem Auftragnehmer so ab, dass der Betriebsablauf beim Auftragnehmer so wenig wie möglich beeinträchtigt wird.

(3) Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Überprüfung, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von dieser Ziffer 12 dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber ihm die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Wettbewerber des Auftragnehmers mit der Kontrolle beauftragen.

(4) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der technischen und organisatorischen Maßnahmen sowie der Einhaltung dieser Vereinbarung und datenschutzrechtlicher Vorgaben zur Verfügung. Zu diesen Informationen gehören insbesondere aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, externe Sachverständige, IT-Sicherheits- oder Datenschutzauditoren) und geeignete Zertifizierung (z.B. nach BSI-Grundschutz). Der Auftragnehmer erteilt dem Auftraggeber unverzüglich konkrete Auskunft im Einzelfall.

(5) Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die

Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten.

(6) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch in angemessenen Umfang geltend machen.

15 Haftung

(1) Auftraggeber und Auftragnehmer haften im Außenverhältnis nach Art. 82 Abs. 1 DSGVO für materielle und immaterielle Schäden, die eine Person wegen eines Verstoßes gegen die DSGVO erleidet.

(2) Der Auftragnehmer haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der er

a. den aus der DSGVO resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder

b. unter Nichtbeachtung der oder gegen die rechtmäßig erteilten Anweisungen des Auftraggebers gehandelt hat.

(3) Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragnehmer vorbehalten.

(4) Im Innenverhältnis zwischen Auftraggeber und Auftragnehmer haftet der Auftragnehmer für den durch eine Verarbeitung verursachten Schaden jedoch nur aus den in (2) genannten Gründen.

(5) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

16 Änderungsvorbehalt, Widerspruchsregelung

(1) Der Auftragnehmer ist dazu berechtigt, die Regelungen dieser Vereinbarung zu ändern, soweit hierdurch wesentliche Regelungen dieser Vereinbarung nicht berührt werden und dies zur Anpassung an den aktuellen Stand der Technik, an geänderte Betriebsabläufe oder zur Umsetzung von Vorgaben seiner Aufsichtsbehörden erforderlich ist, welche bei Vertragsschluss nicht vorhersehbar waren. Wesentliche Regelungen sind insbesondere solche über Art und Umfang der vertragsgegenständlichen Leistungen sowie die Laufzeit einschließlich der Regelungen zur Kündigung. Ferner können Anpassungen oder Ergänzungen dieser Vereinbarung vom Auftragnehmer vorgenommen werden, soweit dies zur Beseitigung von Schwierigkeiten bei der Durchführung dieser Vereinbarung aufgrund von nach Vertragsschluss entstandenen Regelungslücken erforderlich ist. Dies kann insbesondere der Fall sein, wenn sich die Rechtsprechung ändert und eine oder mehrere Klauseln dieser Vereinbarung hiervon betroffen sind.

(2) Über die Änderungen informiert der Auftragnehmer den Auftraggeber mindestens einen Monat vor ihrem Wirksamwerden in elektronischer Form per E-Mail oder in seinem Kundenkonto. Widerspricht der Auftraggeber innerhalb von einem Monat nach Zugang der Änderungsmitteilung nicht in Textform (Fax oder E-Mail ausreichend), werden die Änderungen zum Zeitpunkt des Wirksamwerdens

Vertragsbestandteil. Der Auftraggeber wird auf die Folgen eines fehlenden Widerspruchs in der Änderungsmitteilung besonders hinweisen.

17 Schlussbestimmungen

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.

(2) Es gilt deutsches Recht.

(3) Gerichtsstand für alle Streitigkeiten aus diesem Vertrag ist der Sitz des Auftragnehmers.

(4) Sollten einzelne oder mehrere Regelungen dieser Vereinbarung unwirksam sein, so wird die Wirksamkeit der übrigen Vereinbarung hiervon nicht berührt. Für den Fall der Unwirksamkeit einzelner oder mehrere Regelungen werden die Vertragsparteien die unwirksame Regelung unverzüglich durch eine solche Regelung ersetzen, die der unwirksamen Regelung wirtschaftlich und datenschutzrechtlich am ehesten entspricht.

(5) Im Falle eines Widerspruchs zwischen dem Hauptvertrag und dieser Vereinbarung geht diese Vereinbarung vor, soweit der Widerspruch die Verarbeitung personenbezogener Daten betrifft.

(6) Die folgenden Anhänge sind Bestandteil dieser Vereinbarung:

- Anlage 1 „Technische und organisatorische Maßnahmen“
- Anlage 2 „Genehmigte Subunternehmer“

Anlage 1

Technische und organisatorische Maßnahmen

Stand: Januar 2026

1. Maßnahmen zur Gewährleistung der Vertraulichkeit

1.1 Zutrittskontrolle

Soll verhindern, dass Unbefugte räumlich Zugang zu Datenverarbeitungsanlagen erhalten. Maßnahmen zur Gebäude- und Raumsicherung.

Sicherung durch Wachdienst

Kontrolle des Unternehmensgebäudes außerhalb der Bürozeiten von außen durch einen Wachdienst.

Zutrittsbegrenzung

Der Zutritt zu den Unternehmensräumlichkeiten ist auf notwendiges Personal beschränkt. Es gibt spezielle Schutzvorkehrungen für Server- und Materialschränke.

Verschlossene Serverräume

Serversysteme im Unternehmensgebäude befinden sich in separaten verschlossenen Räumlichkeiten.

Schlüsselverwaltung

Es wird eine Schlüsselausgabeliste zur Nachvollziehbarkeit der Zutrittsmöglichkeiten zu den Unternehmensräumlichkeiten geführt.

Begleitung von Besucherzutritten

Ein unberechtigter Zutritt wird durch die Begleitung von Besuchern in den Räumlichkeiten des Unternehmens verhindert.

Rechenzentren
Die eingesetzten Rechenzentren verfügen über eine Videoüberwachung, Wach-/Sicherheitsdienst/Werksschutz/Empfang, Alarmanlage, Besucherregelungen und Berechtigungskonzepte/Zugangsregelungen durch Nutzung von personifizierte Magnet-, Chipkarten oder Ausweise, elektronische Zugangssicherungen.

1.2 Zugangskontrolle

Soll den Zugang Unbefugter zu Datenverarbeitungssystemen und deren unbefugte Nutzung verhindern. Systemabsicherung.

Diebstahlsicherung
Testgeräte werden über eine Ausleihliste ausgegeben und befinden sich ansonsten in einem Safe. Grundsätzlich verlassen diese aber nicht das Unternehmensgebäude.

Konzeptionelle Sicherheit
Schon während der Konzeption wird die Sicherheit der Schnittstellenkommunikation, des Berechtigungskonzepts und der Bereitstellung von Zugängen für externe Kräfte einbezogen und danach konzipiert.

Beschränkung Anmeldeversuche
Zur Verhinderung von unberechtigten Zugriffen ist die Anzahl der Anmeldeversuche beschränkt.

Zwei-Faktor Authentifizierung

Zur Nutzung der Systeme wird eine Zwei-Faktor-Authentifizierung eingesetzt.

Authentifizierung
Eine Herausgabe von Daten oder ein Zurücksetzen von Passwörtern findet nur nach vorheriger Authentifizierung mittels festgelegter Faktoren statt.

Berechtigungskonzept
Einsatz eines Berechtigungskonzepts, das regelmäßig überprüft und angepasst wird. Dieses ist darauf ausgelegt, dass Mitarbeiter nur diejenigen Daten bearbeiten oder einsehen, die für ihren Tätigkeitsbereich erforderlich sind.

Benutzerkonten
Es ist in einer Richtlinie festgelegt, wie Benutzerkonten eingerichtet, geändert, gesperrt und gelöscht werden. Für privilegierte Konten gelten besondere Vergabe-, Nutzungs- und Protokollierungsvorgaben.

Rechtevergabe neuer Mitarbeiter
Neue Mitarbeiter erhalten nur diejenigen Berechtigungen, die für die konkrete Tätigkeit benötigt werden.

Rechteanpassung Abteilungswechsel
Bei Wechsel des Arbeitsplatzes werden die Berechtigungen dem neuen Tätigkeitsbereich angepasst.

Rechteentzug Offboarding
Beim Austritt eines Mitarbeiters aus dem Unternehmen werden sämtliche Zugriffsmöglichkeiten gesperrt.

Zugriffsbeschränkung Datenbank
Ein direkter Zugriff auf die Systemdatenbanken ist nur durch ausgewählte Personen möglich.

Betrieb Firewall
Zur Absicherung der Systeme werden redundante Firewalls betrieben, welche mittels kontinuierlicher Updates das System gegen Bedrohungen schützen.

Betrieb End-Point-Protection
Eingesetzte Geräte sind mit einer End-Point-Protection ausgestattet.

IT-Inventarliste
Verwendete Soft- und Firmware, sowie die eingesetzte Hardware sind in einer Inventarliste aufgeführt.

Systemmonitoring

Die eingesetzten IT-Systeme werden zur Erkennung von Unregelmäßigkeiten und Einleitung von Entstörungsmaßnahmen einem Monitoring unterzogen.

Dokumentenverschlüsselung
Es werden Verschlüsselungstechniken für Daten, Datentransfer und die Kundenkommunikation eingesetzt.

Servergespeicherte Profile
Nutzerprofile der Mitarbeiter werden auf einem lokalen Server gespeichert.

Passwortvorgaben
Einsatz von Passwortvorgaben mit Mindestvorgaben hinsichtlich der Komplexität der Passwörter, sowie der Wechselhäufigkeit.

Automatische Bildschirmsperre
Zur Verhinderung von unberechtigten Zugriffen sind die elektronischen Arbeitsplätze mit einer automatischen Bildschirmsperre bei Inaktivität nach einem definierten Zeitraum ausgestattet.

Softwarefreigaberichtlinie
Es wird auf den Systemen nur freigegebene Software aus spezifizierten Quellen installiert, die zuvor eine Prüfung nach festgelegten Vorgaben einer Prüfung zur Softwarefreigabe durchlaufen hat.

Mitarbeiterauswahl
Mitarbeiter werden anhand ihrer Qualifikation sorgfältig ausgewählt.

Mobiles Arbeiten
Die Mitarbeiter werden bei Einsatz im Rahmen eines mobilen Arbeitens zuvor insbesondere hinsichtlich datenschutzrechtlicher als auch IT-sicherheitsrelevanter Aspekte unterrichtet und geschult.

1.3 Zugriffskontrolle
Soll unerlaubte Tätigkeiten in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen verhindern.

Clean Desk Policy
Im Unternehmen existiert eine Clean Desk Policy.

Regelung zur Anfertigung von Kopien
Es existiert eine Regelung bezüglich der Anfertigung von Kopien, Ausdrucken und Papierkopien, welche auf das erforderliche Maß beschränkt sind.

Löschkonzept
Im Unternehmen ist ein Löschkonzept für sämtliche Daten aufgestellt, welches die gesetzlichen Aufbewahrungspflichten und den Grundsatz der Datenminimierung der DSGVO beachtet.

Verwaltung Datenträger
Datenträger werden in einer Inventarliste erfasst.

Lokalisierung Datenträger
Datenträger dürfen sich nur in einem definierten Bereich befinden und diesen nicht verlassen.

Datenträgervernichtung
Datenträger werden ordnungsgemäß unter Aufsicht durch einen externen Dienstleister gemäß DIN66399 Sicherheitsstufe 2 oder höher vernichtet.

Schutz gespeicherter Nutzer-Passwörter
Die gespeicherten Nutzerpasswörter sind verschlüsselt oder gehasht hinterlegt.

Anwenderschulung
Anwender werden im Umgang mit der jeweiligen Software geschult.

Verpflichtung zur Vertraulichkeit
Mitarbeiter werden durch eine Verpflichtungserklärung zur Vertraulichkeit unterrichtet und verpflichtet. Die Verpflichtungserklärung ist fester Bestandteil des Onboardingprozesses.

Berechtigungskonzept
Es besteht ein Konzept, das die Aufteilung und Vergabe von Berechtigungen sowie Rechten und Rollen regelt.

Rechte- und Rollenkonzept
Das Berechtigungskonzept wird ergänzt durch das Rechte- und Rollenkonzept. Darin sind Zugriffsberechtigungen genau festgelegt. Die Berechtigungen werden dadurch auf die notwendigen Personen beschränkt und bedarfsgerechte Zugriffsrechte geschaffen.

Eingabeprotokollierung/Login
Die Eingabe von persönlichen Daten in das Datensystem (z.B. Eingabe zur Anmeldung) wird technisch protokolliert.

Zugriffe auf Kundendaten
Zugriffe des Anbieters auf Kundendaten erfolgen nur bei dokumentiertem Bedarf und werden protokolliert.

1.4 Trennungskontrolle
Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden getrennt voneinander verarbeitet.

Mandantenfähigkeit
Das System verfügt über eine Mandantenfähigkeit, sodass die Kundendaten getrennt voneinander verarbeitet werden. Kundendaten werden mandantenbezogen logisch getrennt; die eingesetzten Mechanismen sind beschrieben.

Zonenarchitektur
Produktiv-, Test- und Entwicklungsumgebungen sind technisch und organisatorisch getrennt und diese Trennung ist dokumentiert.

Zweckbindung
Daten werden nur zu einem bestimmten Zweck gemäß den Vorschriften der DSGVO verarbeitet und gespeichert.

2. Maßnahmen zur Gewährleistung der Integrität

2.1 Weitergabekontrolle

Soll die Sicherheit der Daten bei elektronischer Übertragung und Datentransport und die Nachvollziehbarkeit der Weitergabe gewährleisten.

Verpackungs- und Versandvorschriften
Datenträger werden entsprechend der Kategorie der enthaltenen Daten besonders versendet.

Verschlüsselter Emailversand/Verschlüsselte Emailanhänge
E-Mails werden ab einer bestimmten Schutzstufe verschlüsselt versandt. E-Mailanhänge werden ab einer Einstufung in die Schutzklasse "vertraulich" verschlüsselt versandt, dies gilt insbesondere für die Anhänge beim DTA-Versand.

Transportverschlüsselter Datenaustausch
Ein Datenaustausch findet grundsätzlich verschlüsselt nach dem TLS-Standard statt.

Verbindungen
Für alle externen Verbindungen ist ein Kommunikations- und Verschlüsselungskonzept dokumentiert, das zulässige Protokolle und Gegenstellen definiert. Verbindungen werden protokolliert und auf unzulässige oder ungewöhnliche Zugriffe überprüft.

Überwachung und Protokollierung
Ein zentrales Protokollierungs- und Überwachungskonzept legt Ereignisarten, Protokollquellen und Aufbewahrungsfristen fest. Protokolle werden zentral gesammelt, vor unbefugter Änderung geschützt und nur berechtigten Personen zugänglich gemacht. Die für Protokollierung und Überwachung eingesetzten Systeme werden auf Verfügbarkeit und Aktualität überwacht. Anwendungen protokollieren sicherheitsrelevante Ereignisse (z.B. Anmeldeversuche, Rechteänderungen) in ausreichender Detailtiefe.

2.2 Eingabekontrolle

Soll gewährleisten, dass nachvollzogen werden kann, ob, wer, wann personenbezogene Daten in Datenverarbeitungssysteme eingeben, geändert oder gelöscht hat.

Versionsverwaltung
Dokumente werden auf Grundlage zuvor festgelegter Versionierungsvorgaben angelegt und verwaltet.

Protokollauswertung
Systemprotokolle werden regelmäßig ausgewertet, um Fehler und Sicherheitsprobleme zu identifizieren und zu beheben.

Rechte- und Rollenkonzept
Ein umfassendes Rechte- und Rollenkonzept regelt die Zugriffe und die Rechte zur Datenverarbeitung zur Beschränkung der Eingabe, der Veränderung und der Löschung von Daten.

3. Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Soll Daten gegen zufällige Zerstörung oder Verlust schützen.

Brandmeldeanlage Serverraum
Die Serverräume sind mit einer Brandmeldeanlage ausgestattet.

Klimatisierte Serverräume
Die Serverräume sind zum Schutz vor Überhitzung klimatisiert.

Brandschutz
Produktiv- und Backupserver befinden sich in verschiedenen Brandzonen. Es werden redundante Backups an verschiedenen Standorten vorgehalten.

Überspannungsschutz
Es ist ein Überspannungsschutz vorhanden.

USV-Anlage
Die Server sind mit einer Unterbrechungsfreien Stromversorgung ausgestattet.

Stromgenerator
Eingesetzte Rechenzentren verfügen über redundante Notstromaggregate.

Wartungszeiträume
Wartungen am System werden in definierten Zeiträumen durchgeführt, die eine geringe Auslastung haben.

RAID Datenspeicherung
Die Systeme sind mit einer RAID-Datensicherung ausgestattet.

Backup
Zur Absicherung der Daten werden inkrementelle sowie volle Backups nach einem Backupkonzept erstellt.

Backupwiederherstellung
Regelung bezüglich der Wiederherstellung von Backups, die entsprechend die Befugnisse und die Zeitpunkte eines Zugriffs festlegt.

Vertretungsregeln
Aufgrund von Vertretungsregelungen werden Lücken in Prozessen oder Wissen bei Abwesenheit oder Austritt von Personal reduziert oder verhindert.

Speicher- und Verarbeitungsorte
Speicher- und Verarbeitungsorte der Kundendaten werden dokumentiert und auf Anfrage bereitgestellt.

Sicherungs- und Wiederherstellungskonzept
Es ist ein Sicherungs- und Wiederherstellungskonzept dokumentiert, dass Sicherungshäufigkeiten, Aufbewahrungsorte und Verantwortlichkeiten enthält. Sicherungsläufe werden automatisiert überwacht; fehlerhafte Läufe werden ausgewertet und behoben. Wiederherstellungstests werden in festgelegten Abständen durchgeführt und protokolliert. Sicherungsdaten werden nach definierten Fristen und – sofern erforderlich – geographisch getrennt aufbewahrt.

Kritische Infrastruktur
Kritische Infrastruktur (Energie, Klima, Brandmeldung) wird überwacht; Störungen werden zeitnah bearbeitet.

Kapazitätsüberwachung
Kapazitäten der Produktivumgebungen werden geplant, überwacht und bei Bedarf erweitert.

3.2 Belastbarkeit

Soll Systeme befähigen, mit risikobedingten Veränderungen umgehen zu können und Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufzuweisen. Dadurch soll die Belastbarkeit der Systeme sichergestellt werden, so dass eine Sicherung der Daten ermöglicht wird.

Verfügbarkeit
Die Systeme werden redundant bereitgestellt.

Ausweichmaßnahmen
Ausfälle können durch gleichwertige Alternativen ausgeglichen oder abgemildert werden.

Standard-Hard- und -Software
Es wird, soweit möglich, auf Standard-Hard- und -Software zurückgegriffen, sodass Komponenten schnellstmöglich ersetzt werden können.

Soft- und Firmwareupdates
Soft- und Firmwareupdates werden regelmäßig aktualisiert.

Informationskanäle zu Herstellern
Es werden Informationskanäle zu den Herstellern genutzt, wie Emailregistrierungen und Informations-Abonnements.

Cyber-Versicherung
Das Unternehmen ist gegen IT bezogene Fälle versichert.

Redundante Speicherung
Datenbanktransaktionen werden redundant gespeichert.

Geo-Redundante Architektur
Zur Minimierung von Umwelteinflüssen ist die IT-Architektur geo-redundant, also örtlich verteilt, aufgebaut.

Ersatzstromversorgung
Die Server verfügen über eine Ersatzstromversorgung sowie USV-Anlagen.

Umgang mit technischen Schwachstellen, Störungen und Patches
Für den Umgang mit technischen Schwachstellen, Störungen und Patches besteht ein dokumentierter Prozess; Ergebnisse werden nachverfolgt.

Notfallmanagement
Notfall- und Wiederanlaufpläne werden erstellt, aktuell gehalten und auf Wirksamkeit geprüft.

4. Löschung und Verschlüsselung personenbezogener Daten

4.1 Löschung

Nach dem Prinzip der Datensparsamkeit sollen nur solche Daten gespeichert werden, die auch tatsächlich erforderlich sind. Nicht mehr benötigte Daten sollen gelöscht werden.

Löschkonzept
Im Unternehmen ist ein Löschkonzept für sämtliche Daten aufgestellt, welches die gesetzlichen Aufbewahrungspflichten und den Grundsatz der Datenminimierung der DSGVO beachtet. Es erfolgt somit eine regelmäßige Löschung nicht mehr benötigter Daten nach dem Prinzip der Datensparsamkeit. Löschvorgänge an personenbezogenen bzw. kundenspezifischen Daten werden protokolliert.

4.2 Verschlüsselung

Um die Sicherheit von personenbezogenen Daten umfassend zu gewährleisten sollen die Daten so verschlüsselt werden, dass diese ohne den entsprechenden Schlüssel keiner spezifischen Person zugeordnet werden können und kein Zugriff auf die Daten erfolgt.

Dokumentenverschlüsselung
Dokumente, die vom Kunden hochgeladen werden, werden zum Schutz verschlüsselt gespeichert.

Verschlüsselter Emailversand/Verschlüsselte Emailanhänge
E-Mails werden ab einer bestimmten Schutzstufe verschlüsselt versandt. E-Mailanhänge werden ab einer Einstufung in die Schutzklasse "vertraulich" verschlüsselt versandt, dies gilt insbesondere für die Anhänge beim DTA-Versand.

Transportverschlüsselter Datenaustausch
Ein Datenaustausch findet grundsätzlich verschlüsselt nach dem TLS-Standard statt. Daten werden bei Übertragung über öffentliche oder unsichere Netze verschlüsselt.

Richtlinie Kryptografie und Schlüsselverwaltung
Es ist eine Richtlinie zur Nutzung von Kryptografie und zur Schlüsselverwaltung vorhanden, die Rollen, Verfahren und Aufbewahrung regelt. Kryptografische Schlüssel werden sicher erzeugt, verteilt, rotiert, gesichert und bei Widerruf gesperrt.

5. Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung

5.1 Kontrollverfahren

Soll die Wirksamkeit der Datensicherheitsmaßnahmen gewährleisten.

Funktionstrennung
Zur Vermeidung von Interessenskonflikten sind operative und kontrollierende Aufgabe getrennt.

Automatisches Deployment
Der Deploymentprozess ist weitestgehend automatisiert und dadurch optimiert.

Vier-Augen-Prinzip
Zur Reduzierung von Benutzerfehlern, Missbrauch und Ähnlichem wird bei Systemänderungen zur Minimierung von Risiken im Vier-Augen-Prinzip gearbeitet.

Verarbeitungsverzeichnis
Ein Verarbeitungsverzeichnis nach den Vorgaben der DSGVO wird geführt und regelmäßig aktualisiert.

Regelmäßige Überprüfung
Prozesse, Daten, Verträge, Zugänge sowie Richtlinien und Verfahren werden regelmäßig auf Aktualität, Korrektheit und Einhaltung nach Vorgaben eines festgelegten PDCA-Zyklus überprüft. Durchführung interner Datenschutz-Audits.

Qualitätssicherung
Software, die erstellt oder eingesetzt wird, wird einem Freigabeprozess nach festgelegten Vorgaben unterzogen.

Lizenzmanagement
Produktlizenzen werden zentral verwaltet.

Sicherheitsüberprüfungen
Sicherheitsüberprüfungen (z.B. Penetrationstests, Messungen) werden risikoorientiert durchgeführt und die Ergebnisse werden in Maßnahmen überführt.

Sicherheitsvorfälle
Sicherheitsvorfälle werden nach einem festgelegten Verfahren erfasst, klassifiziert, behandelt und nachverfolgt.

Eigenes geistiges Eigentum
Soweit möglich und sinnvoll wird eigenes geistiges Eigentum verwendet oder erzeugt, um Lizenzvereinbarungen zu vermeiden.

Datenschutzfreundliche Voreinstellung
Es werden so wenig Daten wie möglich erhoben und nach Möglichkeit nicht geteilt (privacy by default).

Datenschutzmanagementsystem
Es wird ein zentrales Datenschutzmanagementsystem geführt.

5.2 Auftragskontrolle

Soll sicherstellen, dass Daten, die im Auftrag durch Dienstleister (Subauftragnehmer) verarbeitet werden, nur gemäß der Weisung des Auftraggebers verarbeitet werden. Zudem soll sichergestellt werden, dass auch bei den Auftragnehmern eine ordnungsgemäße Datenverarbeitung erfolgt.

Auftragskontrolle Sub-Unternehmer

Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben des jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag abgeschlossen. Auftragnehmer werden auch während des Vertragsverhältnisses regelmäßig nach Vorgaben eines festgelegten PDCA-Zyklus kontrolliert.

Auswahl

Dienstleister werden ausgewählt, risikobewertet, vertraglich verpflichtet und regelmäßig überwacht; eine Ausstiegsstrategie ist, abhängig von der Risikoklassifizierung, definiert.

ISO/TÜV Zertifizierung

Es werden bevorzugt ISO/TÜV zertifizierte Dienstleister ausgewählt.

Service-Level-Agreements

Mit Dienstleistern sind Service-Level-Agreements vereinbart, welche den Betrieb und die Verfügbarkeit sicherstellen.

Vertragsstrafen

Soweit gesetzlich möglich werden Vertragsstrafen zur Verhinderung von Vertragsbrüchen vereinbart.

6. Sonstiges Datenschutzmanagement

Datenschutzbeauftragter

Das Unternehmen hat einen Datenschutzbeauftragten benannt und wird von diesem in datenschutzrechtlichen Angelegenheiten beraten.

Informationssicherheitsbeauftragte

Zur Beratung in Fragen der Informationssicherheit wird auf die Expertise eines Informationssicherheitsbeauftragen zurückgegriffen.

Sensibilisierung

Mitarbeiter werden regelmäßig in datenschutzrechtlichen und informationssicherheitstechnischen Themen geschult. Im Bereich des Datenschutzes wird ein Schwerpunkt auf den Schutz von Sozial- und Gesundheitsdaten gelegt.

PDCA-Zyklus
Regelmäßige Überprüfungen auf Grundlage eines festgelegten PDCA-Zyklus.

Vertraulichkeitsverpflichtung
Alle Mitarbeiter werden auf die Einhaltung des Datenschutzes, Sozialgeheimnis und zur Verschwiegenheit verpflichtet.

7. Allgemeine Maßnahmen

Informationssicherheits-Managementsystem (ISMS)

Es wird ein zentrales Informationssicherheits-Managementsystem (ISMS) betrieben.

Informationssicherheits-, IT-Nutzungs- und Datenschutzrichtlinien
Die Informationssicherheits-, IT-Nutzungs- und Datenschutzrichtlinien sind für alle Mitarbeiter im Zugriff und werden regelmäßig oder bei Bedarf aktualisiert. Sicherheits- und Datenschutzrichtlinien werden dokumentiert, regelmäßig geprüft, freigegeben und Ausnahmen werden nachvollziehbar genehmigt.

Anfragen von staatlichen Stellen
Anfragen von staatlichen Stellen oder sonstigen Dritten werden nach einem dokumentierten Verfahren geprüft, rechtlich bewertet, dokumentiert und – soweit zulässig – dem Kunden angezeigt.

Export- und Bereitstellungswege
Vereinbarte Export- bzw. Bereitstellungswege für Kundendaten sind beschrieben und werden auf Anforderung bereitgestellt.

IT-Sicherheit
Ein Risikomanagement ist etabliert und berichtet an die Geschäftsführung. Eine Notfallplanung und ein Wiederanlaufplan ist etabliert. Ein Incidentmanagement-System ist etabliert.

Audits
Regelmäßige interne Informationssicherheits- und Datenschutz Audits. Interne Audits, Managementbewertungen und die Ermittlung anwendbarer Anforderungen werden geplant, durchgeführt und dokumentiert.

Anlage 2
Genehmigte Subunternehmer

Firma (Subunternehmer), Adresse	Verarbeitungsstandort	Art der Dienstleistung
AnyDesk Software GmbH Friedrichstraße 9 70174 Stuttgart	Deutschland	Fernwartungssoftware
Blista Brailletec gGmbH Tom-Mutters-Str. 11 35041 Marburg	Deutschland	Druck und Blinden-Tan-Liste
centron GmbH Heganger 29 96103 Hallstadt	Deutschland	Bereitstellung Server (OCR-Software)
RHENUS Data Office GmbH Kölner Str. 24 40885 Ratingen	Deutschland	Papierentsorgung und Datenträgervernichtung
FAX.de GmbH & Co.KG Bei den Kämpen 10 21220 Seevetal-Ramelsloh	Deutschland	Fax-Service
Microsoft Corporation One Microsoft Way Redmond, USA	EU	Bereitstellung Server, Kommunikationstool Microsoft Teams, Videokonferenzen, Schulungen, Webinare
Netclusive GmbH Robert-Bosch-Str. 10 56410 Montabauer	Deutschland	Bereitstellung Produktiv- / System-Server, IT Support
Telekom Deutschland GmbH	Deutschland	Bereitstellung Server- und Clouddienste

Landgrabenweg 151 53227 Bonn		
PoKaMax GmbH Mergentheimer Str. 9c 97082 Würzburg	Deutschland	Grußkartenversand
WIVA Briefdruckzentrum Vacher Str. 197c 90766 Führt	Deutschland	Briefdruck und Versand