TEAM 1
GESUND
L HEIT

Datenschutzvereinbarung zur Auftragsverarbeitung nach § 80 SGB X, Art 28 EU-Datenschutz-Grund-verordnung (DSGVO)

Version 2.1, Februar 2026

Vereinbarung nach § 80 SGB X, Art. 28 Datenschutz-Grundverordnung (DSGVO)

Zwischen

Kundenname
Straße Nr.
PLZ Ort

nachstehend auch „*Auftraggeber*“ genannt

und der

Team Gesundheit Gesellschaft für Gesundheitsmanagement mbH
Rellinghauser Str. 93
45128 Essen

– Auftragsverarbeiter –
nachstehend auch „*Auftragnehmer*“ genannt

Präambel

Diese Vereinbarung regelt die Maßnahmen zum Schutz des Sozialgeheimnisses und der Sozialdaten im Sinne des § 35 SGB I oder anderer personenbezogener Daten bei der Datenverarbeitung im Auftrag unter Berücksichtigung des § 80 SGB X, soweit Sozialdaten verarbeitet werden, sowie des Art. 28 DSGVO.

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus dem jeweiligen Leistungsvertrag, auf den hier verwiesen wird (im Folgenden auch Leistungsvereinbarung). Zur Konkretisierung werden die Angaben zudem in Anhang 1 zusammengefasst. (Anmerkung: Anhänge 1.1 bis 1.3 umfassen verschiedene Leistungsbereiche; ausschließlich maßgeblich für diesen AV-Vertrag ist die jeweils zum Leistungsvertrag korrespondierende Darstellung!)

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der jeweiligen Leistungsvereinbarung bis zur vollständigen Erfüllung und Abwicklung der vereinbarten Leistungen aus der Leistungsbeschreibung. Zur Konkretisierung werden die Angaben zudem in Anhang 1 zusammengefasst.

Die Geheimhaltungspflicht gilt darüber hinaus unbegrenzt.

Der Auftraggeber kann den Hauptvertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn

a) ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen des Vertrages vorliegt oder

b) der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder

c) der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert oder

d) die Grundlage der Vertragserfüllung wesentlich verändert wird oder ganz entfällt aufgrund einer Änderung der Rechts- oder Gesetzeslage oder wegen aufsichtsrechtlicher Maßnahmen oder

e) Daten vertragswidrig durch den Auftragnehmer an Staaten übermittelt werden, die kein Mitgliedsstaat der Europäischen Union, kein anderer Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder die Schweiz sind oder für die kein Angemessenheitsbeschluss nach Art. 45 DSGVO vorliegt.

Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

§ 2 Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten / Sozialdaten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der jeweiligen Leistungsvereinbarung. Zur Konkretisierung werden die Angaben zudem in Anhang 1.1 zusammengefasst.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des

Abkommens über den Europäischen Wirtschaftsraum statt. Sofern Sozialdaten verarbeitet werden, darf die Datenverarbeitung zusätzlich neben den vorgenannten Staaten auch in der Schweiz erfolgen. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn

a) die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, sofern personenbezogenen Daten verarbeitet werden, die keine Sozialdaten sind (es gilt ausschließlich Art. 28 DSGVO) oder
b) sofern Sozialdaten verarbeitet werden, ein Angemessenheitsbeschluss nach Art. 45 DSGVO vorliegt (Art. 28 DSGVO i.V.m. § 80 SGB X).

Ein Zugriff auf personenbezogene Daten durch Staaten, für die kein solcher Angemessenheitsbeschluss vorliegt, ist dem Auftraggeber unverzüglich mitzuteilen. In Anhang 2 sind die Standorte, bei denen Sozialdaten / personenbezogene Daten des Auftraggebers verarbeitet werden, einzutragen und ggf. Feststellungen zum angemessenen Schutzniveau in den betreffenden Drittländern zu treffen. Eine Veränderung der Standorte oder Räumlichkeiten, in denen Daten des Auftraggebers verarbeitet werden, oder ein Verlagern der Auftragsdurchführung an eine andere Örtlichkeit als die mit dem Auftraggeber vereinbarte, bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers. Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DSGVO verantwortlich.

(2) Art der Daten

Die Art der betroffenen Daten ergibt sich aus Anhang 1.1.

(3) Kategorien betroffener Personen

Die Kategorien der durch den Umgang mit ihren personenbezogenen (Sozial-) Daten im Rahmen dieses Auftrags Betroffenen sind in Anhang 1.1 dargestellt.

§ 3 Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung schriftlich oder in Textform zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen (Einzelheiten in Anhang 3).

(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 revisionssicher zu dokumentieren.

(4) Sämtliche Dokumentationen zu den technischen und organisatorischen Maßnahmen, Dokumentationen von Regelungen zum Datenschutz und zur Informationssicherheit und Audit- bzw. Prüfberichte müssen in deutscher Sprache verfasst bzw. in deutscher Übersetzung bereitgehalten werden.

§ 4 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Die schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme in Anhang 1 mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

b) Die Wahrung der Vertraulichkeit und des Daten- sowie Sozialgeheimnisses (sofern Sozialdaten verarbeitet werden) gemäß Art. 28 Abs. 3 Satz 2 lit. b, 29, 32 Abs. 4 DSGVO, § 35 SGB I. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit und zur Geheimhaltung unter Hinweis auf die rechtlichen Folgen einer Pflichtverletzung, insbesondere nach § 203 Abs. 4 StGB, nachweisbar verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Dies umfasst die Verpflichtung zur Geheimhaltung auch über das bestehende Dienst- oder Beschäftigungsverhältnis hinaus. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten bzw. Sozialdaten 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.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 Satz 2 lit. c, 32 DSGVO (Einzelheiten in Anhang 3).

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bzw. Sozialdaten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bzw. Sozialdaten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

g) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt

auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bzw. Sozialdaten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

h) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bzw. Sozialdaten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

i) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bzw. Sozialdaten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

j) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bzw. Sozialdaten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

k) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bzw. Sozialdaten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

l) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

m) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

n) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird. Die Kontrollen, die Ergebnisse und ggf. umgesetzte Maßnahmen sind zu protokollieren und für mindestens 6 Jahre aufzubewahren.

o) Die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 6 dieses Vertrages.

p) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln. Diese Verpflichtung besteht über das Ende des Vertragsverhältnisses hinaus.

q) Sozialdaten / personenbezogene Daten des Auftraggebers dürfen nicht im öffentlichen

Raum (z.B. Flughafen, Bahn etc.) verarbeitet werden. Die Verarbeitung der Sozialdaten des Auftraggebers außerhalb der Geschäftsräume des Auftragnehmers ist nur im nichtöffentlichen Raum zulässig und nur mit gesicherten firmeneigenen Geräten des Auftragnehmers. Es muss sich dabei um verschlüsselte Festplatten, geschützte Verbindungen und fortschrittliche Sicherheitsvorkehrungen (jeweils aktuell) wie z.B. Firewall handeln, sowie aktuelle Signaturen von Viren- und Malwarescannern. Die Bestimmungen zu den technisch-organisatorischen Maßnahmen nach § 3 sind zu beachten.

r) Die Verwendung privater IT-Geräte wie PCs, Tablets, Notebooks, Smartphones etc. bzw. die private Nutzung der firmeneigenen IT-Geräte ist grundsätzlich nicht gestattet. Ausnahmen bedürfen der vorherigen ausdrücklichen Zustimmung (schriftlich oder in Textform) des Auftraggebers und stehen unter dem Vorbehalt, dass sich der Auftraggeber von einer hinreichenden Endgerätesicherheit des Auftragnehmers überzeugen kann. Der Auftragnehmer hat dem Auftraggeber hierzu geeignet nachzuweisen, dass er bei der Verwendung privater IT-Geräte dem Schutzbedarf der Daten und dem jeweiligen Stand der Technik entsprechende Maßnahmen umgesetzt hat. Die Bestimmungen zu den technisch-organisatorischen Maßnahmen nach § 3 sind zu beachten.

s) Die Nutzung von Cloudcomputing durch den Auftragnehmer ist nur zulässig, wenn dieser mit dem jeweiligen Anbieter eine Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DS-GVO abschließt und – soweit Sozialdaten und / oder Gesundheitsdaten verarbeitet werden – die Vorgaben des § 393 Abs. 2 bis 4 SGB V und bei der Verarbeitung von Sozialdaten zusätzlich die Anforderungen des § 80 SGB X, insbesondere dessen Abs. 2, bezüglich der räumlichen Beschränkungen der Verarbeitung eingehalten werden.

t) Der Auftragnehmer darf ausschließlich solche Datenverarbeitungsvorgänge durchführen, die ihm innerhalb des Auftragsverhältnisses gemäß Art. 28 DSGVO und sofern Sozialdaten verarbeitet werden i.V.m. § 80 SGB X eingeräumt werden. Insbesondere ist die Anonymisierung zu eigenen Zwecken, z.B. für eigene (Daten-)Analysen ausgeschlossen.

u) Analysen des Nutzungsverhaltens und das Erfassen, Sammeln und Verarbeiten personenbezogener Telemetrie- und Diagnosedaten durch den Anbieter des eingesetzten Dienstes zu eigenen Zwecken (z. B. zur Optimierung der eigenen Produkte, Dienste und Geräte per Fernmessung) sind ausgeschlossen. Es dürfen nur die zur Bereitstellung des Dienstes zwingend erforderlichen technischen und sonstigen Informationen verarbeitet werden, sofern dies durch eine gesetzliche Befugnis gerechtfertigt ist.

v) Der Auftragnehmer verpflichtet sich, dass die Daten des Auftraggebers von Daten anderer Auftraggeber streng getrennt werden. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

w) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (z.B. durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren) oder durch sonstige Ereignisse gefährdet werden, hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer ist verpflichtet, alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber zu unterrichten, dass es sich um Daten des Auftraggebers handelt, über die er keinerlei Verfügungs- oder sonstige Bestimmungsgewalt oder Eigentumsrechte hat.

§ 5 Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen, und bei denen ein Zugriff auf Sozialdaten bzw. personenbezogene Daten nicht ausgeschlossen werden kann. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsdienstleister, dem Postgeheimnis unterliegende Post-/Transportdienstleistungen, Gebäudereinigung sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Sicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragnehmer) nur nach vorheriger ausdrücklicher Zustimmung (mindestens Textform) des Auftraggebers beauftragen und soweit der Auftragnehmer mit dem Unterauftragnehmer eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DSGVO und - sofern Sozialdaten verarbeitet werden - i.V.m. § 80 SGB X, die zudem die in diesem Vertrag vereinbarte Rechte und Pflichten berücksichtigt, geschlossen hat.

Der Auftraggeber stimmt der Beauftragung der in Anhang 1.3 aufgeführten und **für ihn nach Maßgabe des Auftragsgegenstandes relevanten** Unterauftragnehmer zu, soweit jeweils eine vertragliche Vereinbarung nach Maßgabe von Satz 1 geschlossen wurde.

(3) Sollen vom Auftragnehmer während der Vertragslaufzeit andere als in Anhang 1.3 benannte Unterauftragnehmer beauftragt oder Standorte von Unterauftragnehmern verlegt/erweitert werden, sind dem **nach Maßgabe des Auftragsgegenstandes betroffenen Auftraggeber** rechtzeitig vor der geplanten Veränderung geeignete Unterlagen mindestens in Textform zur Zustimmung vorzulegen, insbesondere:

a) Beschreibung der Arbeiten, die der Unterauftragnehmer ausführen soll,

b) Ort der Datenverarbeitung,

c) Bericht der letzten Prüfung (nicht älter als 12 Monate),

d) Kopie der geplanten vertraglichen datenschutzrelevanten Regelungen (einschließlich der technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit) mit dem Unterauftragnehmer.

Die Änderung der vorlegten Unterlagen in dieser Hinsicht ist nur zulässig, wenn der Auftraggeber dem ausdrücklich zustimmt. Der Auftraggeber wird die Unterlagen binnen 4 Wochen ab Zugang der Änderungsmitteilung und aller vollständigen Unterlagen prüfen. Er wird zustimmen, wenn der Änderung kein sachlicher Grund entgegensteht. Ein sachlicher Grund im Sinne dieser Regelung liegt insbesondere vor, wenn der Unterauftragnehmer bei der Verarbeitung von Sozialdaten seinen Sitz nicht in einem Land hat, das Mitglied der EU/des EWR ist oder zu dem die Kommission einen Angemessenheitsbeschluss nach Art. 45 DSGVO erlassen hat oder der Unterauftragnehmereinsatz nicht den Vorgaben des § 393 SGB V entsprechen würde.

(4) Erfordert abweichend von Absatz 3 ein unvorhergesehenes Ereignis, wie z. B. ein IT-Sicherheitsvorfall, den Ersatz oder die Hinzuziehung neuer Unterauftragnehmer, damit die vertraglich geschuldete Leistung noch erbracht werden kann, wird der Auftraggeber

unverzüglich über die Maßnahme in Textform informiert. Der Auftragnehmer darf den Unterauftragnehmer erst beauftragen, wenn der Auftragnehmer mit dem Unterauftragnehmer eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DSGVO und - sofern Sozialdaten verarbeitet werden - i.V.m. § 80 SGB X, die zudem die in diesem Vertrag vereinbarten Rechte und Pflichten berücksichtigt, geschlossen hat. Die Unterlagen nach § 5 Abs. 3 von a) bis d) dieser Vereinbarung werden vom Auftragnehmer unverzüglich zur Genehmigung durch den Auftraggeber nachgereicht. Der Auftraggeber wird die Unterlagen binnen 4 Wochen ab Zugang der Änderungsmitteilung und aller vollständigen Unterlagen prüfen. Er wird den Ersatz bzw. die Hinzuziehung des Unterauftragnehmers genehmigen, wenn kein sachlicher Grund entsprechend Abs. 3 entgegensteht. Der Auftragnehmer hat sicherzustellen, dass der neue bzw. hinzugezogene Unterauftragnehmer noch von der Leistungserbringung ausgeschlossen werden kann, wenn ein sachlicher Grund zur Versagung der Genehmigung besteht. In diesem Fall werden die Parteien unter Beachtung der Aufrechterhaltung der Leistungserbringung gemeinsam eine einvernehmliche Lösung finden.

(5) Die Weitergabe von personenbezogenen Daten und Sozialdaten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller gesetzlichen und vertraglich vereinbarten Voraussetzungen insbesondere der vorliegenden schriftlichen (mindestens Textform) Zustimmung des Auftraggebers für eine Unterbeauftragung gestattet.

(6) Erbringt der Unterauftragnehmer die vereinbarte Leistung im Sinne von Abs. 1 Satz 2, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

(7) Eine weitere Auslagerung durch einen Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des (Haupt-)Auftraggebers mindestens in Textform. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

(8) Die vertraglichen Vereinbarungen zwischen Auftragnehmer und Unterauftragnehmer sind so zu gestalten, dass sie den Bestimmungen des Vertragsverhältnisses zwischen Auftraggeber und Auftragnehmer entsprechen. Dies gilt insbesondere im Hinblick auf die Zweckbindung und die Vertraulichkeit der Datenvereinbarung im Sinne des § 4 dieses Vertrages. Die entsprechenden vertraglichen Vereinbarungen sind durch den Auftragnehmer nachzuweisen und rechtzeitig vor Abschluss des Vertrages vorzulegen.

(9) Der Auftragnehmer hat den Unterauftragnehmer bezüglich der Einhaltung der vertraglichen Pflichten regelmäßig zu prüfen. Das Ergebnis ist zu dokumentieren, mindestens 6 Jahre aufzubewahren und auf Verlangen dem Auftraggeber vorzulegen.

(10) Der Auftragnehmer stellt die datenschutzrechtliche Zulässigkeit bei der Erbringung von Leistungen durch Unterauftragnehmer durch entsprechende Maßnahmen sicher. Das Verhalten eines Unterauftragsnehmers ist dem Auftragnehmer wie eigenes Verhalten zuzurechnen.

(11) Wird beim Auftragnehmer die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen und kann dabei der Zugriff auf Sozialdaten / personenbezogene Daten oder deren Kenntnisnahme durch diese Stellen nicht ausgeschlossen werden, sind dem Auftraggeber rechtzeitig vor der Auftragserteilung die Verträge über Wartungsarbeiten einschließlich der damit Beauftragten mitzuteilen. Sind Störungen im Betriebsablauf zu erwarten oder bereits eingetreten, ist der Vorgang dem Auftraggeber unverzüglich mitzuteilen.

(12) Umfasst der Leistungsgegenstand Transportdienstleistungen und wird durch den Auftragnehmer für den Datentransport ein Transportunternehmen beauftragt, so hat er

vertraglich sicherzustellen und dem Auftraggeber auf Verlangen nachzuweisen, dass der Transportunternehmer den Datenschutzbestimmungen Genüge tut. Werden Unterlagen des Auftraggebers abgeholt, stattet der Auftragnehmer den Transportunternehmer mit einem schriftlichen Berechtigungsausweis für die Entgegennahme der Unterlagen aus.

§ 6 Kontrollrechte des Auftraggebers und dessen Aufsichtsbehörden

(1) Der Auftraggeber, dessen zuständige Aufsichtsbehörden bzw. ein von ihm beauftragter Sachverständiger und neutraler Dienstleister, der in keinem Wettbewerbsverhältnis zum Auftragnehmer stehen darf und zuvor schriftlich vom Auftraggeber auf die Vertraulichkeit und Wahrung der Geschäftsgeheimnisse zu verpflichten ist, haben das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Sie haben das Recht, sich durch Stichprobenkontrollen von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Das Prüfrecht umfasst insbesondere die Besichtigung von Grundstücken und Geschäftsräumen, Auskünfte zur Vertragsausführung, Einsicht in Papierunterlagen und auch die Einsichtnahme in die beim Auftragnehmer gespeicherten personenbezogenen Daten / Sozialdaten des Auftraggebers, soweit dies im Rahmen des Auftrags zur Überwachung von Datenschutz und Datensicherheit erforderlich ist. Dies gilt insbesondere für den Nachweis der Umsetzung der technischen und organisatorischen Maßnahmen.

(4) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

a) die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO oder

b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;

c) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

d) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach ISO 27001 oder BSI-Standards).

(5) Der Auftragnehmer sichert zu, dass er die notwendige personelle und sachliche Unterstützung bei den Prüfungen zur Verfügung stellt.

(6) Aufwände und Kosten, die beim Auftragnehmer im Zuge der Prüfung durch den Auftraggeber entstehen, trägt allein der Auftragnehmer. Kosten, die dem Auftraggeber im Zuge der Prüfung entstehen, trägt dieser selbst. Eine Kostenverrechnung und -weitergabe an den Auftraggeber oder an vom Auftraggeber zur Durchführung der Prüfung beauftragte Dritte ist ausgeschlossen.

§ 7 Mitwirkungspflichten des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den § 83a bis 84 SGB X (soweit Sozialdaten verarbeitet werden) und den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherige Konsultationen der Aufsichtsbehörde. Hierzu gehören u.a.:

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,

b) die Verpflichtung, Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber zu melden. In diesem Falle hat der Auftragnehmer sofort alle erforderlichen Maßnahmen zur Sicherung der Sozialdaten zu treffen und weitere Anweisungen durch den Auftraggeber abzuwarten.

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,

d) nach Möglichkeit die Unterstützung des Auftraggebers bei der Beantwortung und Umsetzung von Betroffenenrechten mit geeigneten technischen und organisatorischen Maßnahmen (§ 3 und 9 bleiben hiervon unberührt),

e) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung,

f) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

§ 8 Weisungsbefugnis des Auftraggebers

(1) Der Auftraggeber hat das Recht, erforderlichenfalls Weisungen (mindestens Textform) im Rahmen der Art. 28, 32 DSGVO zur Ergänzung der beim Auftragnehmer vorhandenen technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit zu erteilen.

(2) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. in Textform).

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Ein Verfahren zur Gewährleistung des Datenschutzes/Vertraulichkeit in der telefonischen Kundenberatung des Systems wird von den Vertragsparteien in einem separaten Dokument geregelt.

§ 9 Berichtigung, Einschränkung, Löschung und Rückgabe der vertragsgegenständlichen Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, ist das Löschkonzept, das Recht auf Vergessenwerden, die Berichtigung von personenbezogenen Daten / Sozialdaten, die Datenportabilität (soweit einschlägig) und Auskünfte nach Weisung (mindestens Textform) des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen und revisionssicher zu dokumentieren.

(3) Sämtliche Daten und Unterlagen sowie Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit den im Hauptvertrag genannten Leistungen dieser Datenschutzbestimmungen in die Verfügungsgewalt des Auftragnehmers gelangt sind, hat dieser entsprechend der jeweiligen Vereinbarungen im Einzelfall bzw. nach Abschluss der vertraglichen Arbeiten dem Auftraggeber auszuhändigen bzw. zu übermitteln.

(4) Auf Verlangen des Auftraggebers hat der Auftragnehmer in seinem Besitz befindliche Daten bzw. Datenbestände (z.B. physische Datenträger, elektronische Dateien oder Datenbanken in seinen Datenverarbeitungs-Systemen) nichtreproduzierbar zu löschen bzw. physisch zu vernichten. Die Vernichtung hat in Abhängigkeit von den verarbeiteten personenbezogenen Daten / Sozialdaten nach DIN 66399 Teile 1 bis 3 mindestens mit der Schutzklasse 3 mindestens mit Sicherheitsstufe 4 in der jeweils einschlägigen Materialklasse zu erfolgen. Die Datenlöschung hat nach anerkanntem Standard des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder anderweitiger adäquater Regelungen für vertrauliche Daten in der jeweils aktuellen Fassung zu erfolgen. Dies gilt auch für Test- und Zwischenergebnisse. Ist eine Löschung auf Sicherungskopien wegen der besonderen Art der Speicherung nur mit einem unverhältnismäßig hohen Aufwand möglich, sind die Daten nach Abstimmung mit dem Auftraggeber für jede weitere Verarbeitung einzuschränken.

(5) Die Löschung und Vernichtung hat der Auftragnehmer in geeigneter Weise zu protokollieren. Im Zweifelsfall sind geeignete Maßnahmen mit dem Auftraggeber abzustimmen. Hinsichtlich sämtlicher Löschvorgänge hat der Auftragnehmer dem Auftraggeber Löschprotokolle auf Verlangen zu übergeben.

Es sind folgende Mindestinhalte für ein Löschprotokoll zu berücksichtigen:

- Datum und Uhrzeit der Löschung,
- das gültige Löschkonzept (Version, Datum),
- die Methode der Datenlöschung (Verfahren),
- das betroffene Verfahren (Beschreibung der zu löschenden Daten),
- die angewandte Löschregel,
- die für die Löschung verantwortliche Person,
- die ausführenden Personen,
- bei automatisierter Löschung die Anzahl der zu löschenden Daten (Summenprotokolle, Zählreport) und
- bei automatisierter Löschung die Anzahl der gelöschten Daten (Summenprotokolle, Zählreport, Löschlaufreport).

Im Zusammenhang mit Aktenvernichtung ist entsprechend ein Vernichtungsprotokoll zu vereinbaren.

Das Löschprotokoll darf darüber hinaus keine personenbezogenen Daten und keine Sozialdaten enthalten. Sind von der Vernichtung auch nicht elektronische Unterlagen betroffen, ist ein Vernichtungsprotokoll zu erstellen.

(6) Endet das Vertragsverhältnis, hat der Auftragnehmer gegenüber dem Auftraggeber schriftlich zu erklären, dass die nicht mehr erforderlichen Daten und Datenträger ordnungsgemäß im Sinne dieses Vertrages gelöscht bzw. vernichtet wurden und welche Daten aus gesetzlichen Gründen über das Ende des Auftragsverhältnisses hinaus aufbewahrt werden müssen.

§ 10 Ansprechpartner

Ansprechpartner des Auftragnehmers ergeben sich aus Anhang 1.2

§ 11 Haftung

(1) Der Auftragnehmer haftet gegenüber dem Auftraggeber im Rahmen der gesetzlichen Bestimmungen für Schäden, die infolge schuldhaften Verhaltens gegen Datenschutzbestimmungen und gegen diese Datenschutzvereinbarung entstehen. Ebenso haftet er für schuldhaftes Verhalten seiner Unterauftragnehmer sowie deren Unterauftragnehmer.

(2) Der Auftragnehmer bestätigt, sich gegen die Inanspruchnahme wegen Verletzung von Datenschutzvorschriften hinreichend versichert zu haben und diesen Versicherungsschutz für die gesamte Laufzeit des Hauptvertrages in vollem Umfang aufrechtzuerhalten. Auf Nachfrage des Auftraggebers ist dies durch Vorlage geeigneter Dokumente nachzuweisen.

(3) Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

§ 12 Sonstiges

(1) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein oder nach Vereinbarungsschluss unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit der Vereinbarung im Übrigen unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkungen der wirtschaftlichen Zielsetzung am nächsten kommen, die die Vertragsparteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

(2) Sollten sich datenschutzrechtliche Änderungen während der Vertragslaufzeit ergeben, die zu einer Vertragsanpassung führen müssen, verpflichten sich die Vertragspartner Vertragsverhandlungen mit dem Ziel der Einigung aufzunehmen.

(3) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform.

(4) Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der personenbezogenen Daten/Sozialdaten und der zugehörigen Datenträger ausgeschlossen.

(5) Sämtliche Kommunikation zwischen dem Auftragnehmer und dem Auftraggeber sowie zwischen dem Auftragnehmer und den Aufsichten/Prüfdiensten haben in deutscher Sprache zu erfolgen.

§ 13 Inkrafttreten

(1) Diese Datenschutzbestimmungen treten mit Abschluss des Leistungsvertrages in Kraft, ohne dass es eines gesonderten Vertragsabschlusses dieser Datenschutzvereinbarung zur Auftragsverarbeitung bedarf.

(2) Es gilt die Gerichtsstandvereinbarung des Hauptvertrages.

Verzeichnis der Anhänge:

Anhang 1.1
Konkretisierung der Auftragsverarbeitung (Gegenstand, Dauer, Art und Zweck, Art der Daten, Kategorien betroffener Personen) je Leistungsgegenstand

Anhang 1.2
Übersicht der Ansprechpartner

Anhang 1.3
Übersicht eingesetzter Unterauftragsverarbeiter

Anhang 2
Übersicht der Standorte des Auftragnehmers

Anhang 3
Übersicht der technischen und organisatorischen Maßnahmen (TOM)

Anhang 1.1 - Konkretisierung der Auftragsverarbeitung

1.1 Mental Health Week

Gegenstand der Auftragsverarbeitung	Interessierten Personen soll die Möglichkeit zur Registrierung und zum Abrufen von digitalen Inhalten im Rahmen der Mental Health Week gewährt werden.
Dauer der Auftragsverarbeitung	Die Dauer der Leistung ergibt sich aus dem Leistungsvertrag.
Art und Zweck der Auftragsverarbeitung	Die personenbezogenen Daten werden erhoben, erfasst, gespeichert, ausgelesen und verwendet. Diese Datenverarbeitung dient der Erfüllung des Leistungsvertrages.
Art der betroffenen Daten	☒ Personenstammdaten (z.B. Anrede, Name, Vorname, Geburtsdatum, Adresse, Titel, Funktion) ☒ Kommunikationsdaten (Telefonnummer, E-Mail-Adressen) ☐ Vertragsstammdaten (z.B. Vertragsbeziehungen, Produkt- und Vertragsinteresse, Bewerbungsunterlagen) ☐ Kundenhistorie (z.B. Käufe, Angebote, Anfragen, Kaufverhalten) ☐ Vertragsstamm-, Vertragsabrechnungs- und Zahlungsdaten (letztere – außer bei Zahlungsart „Vorkasse“ beschränkt darauf, ob Zahlung beim Zahlungsanbieter erhalten wurde oder nicht) ☐ Planungs- und Steuerungsdaten ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen) ☒ Technische Protokolldaten (z.B. Login, IP, Zeitstempel) ☒ Daten, die Nutzer in Nachrichten, Freitextfeldern oder als Inhalt von Dateien von sich aus übermitteln ☐ Besondere personenbezogene Daten gem. Art. 9 Abs. 1 DSGVO (rassische und ethnische Herkunft, politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben, genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person): ☐ Weitere Daten: _____
Kategorien betroffener Personen	☒ Kunden bzw. deren Beschäftigte ☐ Lieferanten ☒ Verbraucher / Interessenten ☒ Internetnutzer ☒ Weitere: registrierte Benutzer der Mental Health Week
Subunternehmer	s. Anlage 1.3

1.2 Digitaler Kanal für Produkte (Digitaler Adventskalender, Digitale Gesundheitstage)

Gegenstand der Auftragsverarbeitung	Interessierten Personen soll die Möglichkeit zur Registrierung und zum Abrufen von digitalen Inhalten gewährt werden.
Dauer der Auftragsverarbeitung	Die Dauer der Leistung ergibt sich aus dem Leistungsvertrag.
Art und Zweck der Auftragsverarbeitung	Die personenbezogenen Daten werden erhoben, erfasst, gespeichert, ausgelesen und verwendet. Diese Datenverarbeitung dient der Erfüllung des Leistungsvertrages.
Art der betroffenen Daten	☒ Personenstammdaten (z.B. Anrede, Name, Vorname, Geburtsdatum, Adresse, Titel, Funktion) ☒ Kommunikationsdaten (Telefonnummer, E-Mail-Adressen) ☐ Vertragsstammdaten (z.B. Vertragsbeziehungen, Produkt- und Vertragsinteresse, Bewerbungsunterlagen) ☐ Kundenhistorie (z.B. Käufe, Angebote, Anfragen, Kaufverhalten) ☐ Vertragsstamm-, Vertragsabrechnungs- und Zahlungsdaten (letztere – außer bei Zahlungsart „Vorkasse“ beschränkt darauf, ob Zahlung beim Zahlungsanbieter erhalten wurde oder nicht) ☐ Planungs- und Steuerungsdaten ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen) ☒ Technische Protokolldaten (z.B. Login, IP, Zeitstempel) ☒ Daten, die Nutzer in Nachrichten, Freitextfeldern oder als Inhalt von Dateien von sich aus übermitteln ☐ Besondere personenbezogene Daten gem. Art. 9 Abs. 1 DSGVO (rassische und ethnische Herkunft, politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben, genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person): ☐ Weitere Daten: _____
Kategorien betroffener Personen	☒ Kunden bzw. deren Beschäftigte ☐ Lieferanten ☒ Verbraucher / Interessenten ☒ Internetnutzer ☒ Weitere: registrierte Benutzer der Mental Health Week
Subunternehmer	s. Anlage 1.3

1.3 Gesundheitsberichte

Gegenstand der Auftragsverarbeitung	Aufbereitung und Auswertung von pseudonymisierten Daten unter anderem auch von Mitgliedern der des Auftraggebers zur Erstellung von kassenübergreifenden betrieblichen Gesundheitsberichten für Unternehmen sowie die Erstellung der Gesundheitsberichte an sich.
Dauer der Auftragsverarbeitung	Die Dauer der Leistung ergibt sich aus dem Leistungsvertrag.
Art und Zweck der Auftragsverarbeitung	Die personenbezogenen Daten werden erhoben, erfasst, gespeichert, ausgelesen und verwendet. Diese Datenverarbeitung dient der Erfüllung des Leistungsvertrages.
Art der betroffenen Daten	Gegenstand der Verarbeitung für Berichte nach Betriebsnummer sind folgende Datenarten/ -kategorien: Nachstehende Mitgliederdaten (für jedes Mitglied eine Datenzeile): • Technische ID des Versicherten/ Personennummer (pseudonymisiert; 12 Stellen) • Versicherungsbeginn (TTMMJJ) • Versicherungsende (TTMMJJ) • Versicherungsart (1 = pflichtversichert/ 2 = freiwillig versichert) • Betriebsnummer des auszuwertenden Unternehmens (8 Stellen) • Geburtsjahr (JJJJ) • Geschlecht (1 = Männer/ 2 = Frauen/ 4 = unbestimmtes Geschlecht) und Daten der Arbeitsunfähigkeit: • Technische ID des Versicherten/ Personennummer (pseudonymisiert; 12 Stellen) • Beginn der AU (TTMMJJJJ) • Ende der AU (TTMMJJJJ) • ICD-Schlüssel (Erst- bzw. Hauptdiagnose; 3 Stellen z.B. A01) • Krankheitsursache (1 = Arbeits- oder Wegeunfall/ 0 = alle anderen) Darüber hinaus sind folgende Datenarten /-kategorien zusätzlicher Gegenstand der Verarbeitung, soweit es sich nicht um einen Bericht nach Betriebsnummer handelt: • RV-Nummer des Mitgliedes / des Versicherten (wird vorliegend vor Übermittlung an den Auftragnehmer durch die Technische ID des Versicherten pseudonymisiert) • Auswertungseinheit des Unternehmens

Kategorien betroffener Personen	Mitglieder des Auftraggebers (pseudonymisiert), welche bei dem Unternehmen beschäftigt sind, für das der Gesundheitsbericht erstellt wird
Subunternehmer	s. Anlage 1.3

1.4 Versorgungsforschung / Bonusevaluation / Evaluation von Wahltarifen

Gegenstand der Auftragsverarbeitung	Datenaufbereitung, -prüfung und -zusammenführung und Durchführung statistischer Analysen mit Mitteln der Gesundheitsökonomie, Statistik, Mathematik, Volkswirtschaft und Biologie. Evaluation von versichertenbezogenen Bonusprogrammen und Wahltarifen.
Dauer der Auftragsverarbeitung	Die Dauer der Leistung ergibt sich aus dem Leistungsvertrag.
Art und Zweck der Auftragsverarbeitung	Daten, die zur Durchführung der o.g. Analysen sowie zur Erstellung der Evaluationen benötigt werden. Team Gesundheit erhält hierbei pseudonymisierte Daten, die aufgrund der technischen und organisatorischen Bedingungen anonymisierten Daten gleichkommen. Diese werden gespeichert, organisiert, geordnet, ausgelesen, abgefragt und verwendet. Die Anonymität wird auch bei der Ergebnisdarstellung gewahrt. Diese Datenverarbeitung dient der Erfüllung des Leistungsvertrages.
Art der betroffenen Daten	☐ Personenstammdaten (z.B. Anrede, Name, Vorname, Geburtsdatum, Adresse, Titel, Funktion) ☐ Kommunikationsdaten (Telefonnummer, E-Mail-Adressen) ☐ Vertragsstammdaten (z.B. Vertragsbeziehungen, Produkt- und Vertragsinteresse, Bewerbungsunterlagen) ☐ Kundenhistorie (z.B. Käufe, Angebote, Anfragen, Kaufverhalten) ☐ Vertragsstamm-, Vertragsabrechnungs- und Zahlungsdaten (letztere – außer bei Zahlungsart „Vorkasse“ beschränkt darauf, ob Zahlung beim Zahlungsanbieter erhalten wurde oder nicht) ☐ Planungs- und Steuerungsdaten ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen) ☐ (Technische) Protokolldaten ☐ Daten, die Nutzer in Nachrichten, Freitextfeldern oder als Inhalt von Dateien von sich aus übermitteln ☐ Besondere personenbezogene Daten gem. Art. 9 Abs. 1 DSGVO (rassische und ethnische Herkunft, politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben, genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person): ☒ Abrechnungsdaten (Inanspruchnahme von Leistungen der Krankenkasse) ☐ Weitere Daten: _____

Kategorien betroffener Personen	☒ Versicherte der teilnehmenden Krankenkasse ☐ Lieferanten ☐ Verbraucher / Interessenten ☐ Internetnutzer ☐ Weitere: ☐ Kunden bzw. deren Beschäftigte
Subunternehmer	s. Anlage 1.3

1.5 Mitarbeitendenbefragungen

Gegenstand der Auftragsverarbeitung	Teilnehmende Personen werden zu einer Befragung eingeladen. Die Antworten werden zusammengeführt und ausgewertet.
Dauer der Auftragsverarbeitung	Die Dauer der Leistung ergibt sich aus dem Leistungsvertrag.
Art und Zweck der Auftragsverarbeitung	Die personenbezogenen Daten werden erhoben, erfasst, gespeichert, geordnet, ausgelesen, verwendet und übermittelt. Diese Datenverarbeitung dient der Erfüllung des Leistungsvertrages.
Art der betroffenen Daten	☒ Personenstammdaten (z.B. Anrede, Name, Vorname, Geburtsdatum, Adresse, Titel, Funktion) ☒ Kommunikationsdaten (Telefonnummer, E-Mail-Adressen) ☐ Vertragsstammdaten (z.B. Vertragsbeziehungen, Produkt- und Vertragsinteresse, Bewerbungsunterlagen) ☐ Kundenhistorie (z.B. Käufe, Angebote, Anfragen, Kaufverhalten) ☐ Vertragsstamm-, Vertragsabrechnungs- und Zahlungsdaten (letztere – außer bei Zahlungsart „Vorkasse“ beschränkt darauf, ob Zahlung beim Zahlungsanbieter erhalten wurde oder nicht) ☐ Planungs- und Steuerungsdaten ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen) ☒ Technische Protokolldaten (z.B. Login, IP, Zeitstempel) ☒ Daten, die Nutzer in Nachrichten, Freitextfeldern oder als Inhalt von Dateien von sich aus übermitteln ☐ Besondere personenbezogene Daten gem. Art. 9 Abs. 1 DSGVO (rassische und ethnische Herkunft, politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben, genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person): ☐ Weitere Daten: _____
Kategorien betroffener Personen	☒ Kunden bzw. deren Beschäftigte ☐ Lieferanten ☐ Verbraucher / Interessenten ☐ Internetnutzer ☒ Weitere: registrierte Benutzer der Befragung
Subunternehmer	s. Anlage 1.3

1.6 Longevity Day

Gegenstand der Auftragsverarbeitung	Interessierten Personen soll die Möglichkeit zur Registrierung und zum Abrufen von digitalen Inhalten im Rahmen der Longevity Days gewährt werden.
Dauer der Auftragsverarbeitung	Die Dauer der Leistung ergibt sich aus dem Leistungsvertrag.
Art und Zweck der Auftragsverarbeitung	Die personenbezogenen Daten werden erhoben, erfasst, gespeichert, ausgelesen und verwendet. Diese Datenverarbeitung dient der Erfüllung des Leistungsvertrages.
Art der betroffenen Daten	☒ Personenstammdaten (z.B. Anrede, Name, Vorname, Geburtsdatum, Adresse, Titel, Funktion) ☒ Kommunikationsdaten (Telefonnummer, E-Mail-Adressen) ☐ Vertragsstammdaten (z.B. Vertragsbeziehungen, Produkt- und Vertragsinteresse, Bewerbungsunterlagen) ☐ Kundenhistorie (z.B. Käufe, Angebote, Anfragen, Kaufverhalten) ☐ Vertragsstamm-, Vertragsabrechnungs- und Zahlungsdaten (letztere – außer bei Zahlungsart „Vorkasse“ beschränkt darauf, ob Zahlung beim Zahlungsanbieter erhalten wurde oder nicht) ☐ Planungs- und Steuerungsdaten ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen) ☒ Technische Protokolldaten (z.B. Login, IP, Zeitstempel) ☒ Daten, die Nutzer in Nachrichten, Freitextfeldern oder als Inhalt von Dateien von sich aus übermitteln ☐ Besondere personenbezogene Daten gem. Art. 9 Abs. 1 DSGVO (rassische und ethnische Herkunft, politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben, genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person): ☐ Weitere Daten: _____
Kategorien betroffener Personen	☒ Kunden bzw. deren Beschäftigte ☐ Lieferanten ☒ Verbraucher / Interessenten ☒ Internetnutzer ☒ Weitere: registrierte Benutzer des Longevity Days
Subunternehmer	s. Anlage 1.3

Anhang 1.2 - Übersicht der Ansprechpartner

Ansprechpartner des **Auftragnehmers** sind:

Fachliche Zuständigkeit Mental Health Week, Digitale Kanäle, Longevity Day	
Name, Vorname:	Vullhorst, Daniel
Funktionsbezeichnung:	Teamleitung Digitale Gesundheitsförderung
Erreichbarkeit:	digitale-gesundheitsfoerderung@teamgesundheit.de

Fachliche Zuständigkeit Gesundheitsberichte	
Name, Vorname:	Atabek, Yvonne
Funktionsbezeichnung:	Teamleitung Gesundheitsberichte und Mitarbeitendenbefragungen
Erreichbarkeit:	gesundheitsberichterstattung@teamgesundheit.de

Fachliche Zuständigkeit Mitarbeitendenbefragungen	
Name, Vorname:	Haschke, Alina
Funktionsbezeichnung:	Mitarbeitendenbefragungen
Erreichbarkeit:	mitarbeitendenbefragung@teamgesundheit.de

Fachliche Zuständigkeit Bonusevaluation	
Name, Vorname:	Friedel, Dr. Heiko
Funktionsbezeichnung:	Leitung Versorgungsforschung und Gesundheitsökonomie
Erreichbarkeit:	bonusevaluation@teamgesundheit.de

Fachliche Zuständigkeit Evaluation von Wahltarifen	
Name, Vorname:	Friedel, Dr. Heiko
Funktionsbezeichnung:	Leitung Versorgungsforschung und Gesundheitsökonomie
Erreichbarkeit:	wahltarife@teamgesundheit.de

Datenschutzbeauftragter:	
Name, Vorname:	Schabio, Tim
Funktionsbezeichnung:	Datenschutz Ruhr GmbH
Erreichbarkeit:	0201 - 890 66 123, schabio@datenschutz-ruhr.de

Ansprechpartner für Datenschutzverletzungen:	
Name, Vorname:	Schabio, Tim

Funktionsbezeichnung:	Datenschutz Ruhr GmbH
Erreichbarkeit:	0201 - 890 66 123, schabio@datenschutz-ruhr.de

Anhang 1.3 - Übersicht eingesetzter Unterauftragsverarbeiter

Stand: März 2025

Der Auftragnehmer setzt zur Erbringung der vertraglich vereinbarten Leistungen folgende Unterauftragnehmer ein (Name/Firma, Anschrift).

Im Fall eines Datentransfers in ein Drittland muss die geeignete Garantie und das Ergebnis der jeweiligen Einzelfall-Prüfung mitgeteilt werden, soweit kein Angemessenheitsbeschluss der EU-Kommission vorliegt (EuGH Schrems II Rspr.).

Unterauftragnehmer	Leistungsgegen-stand	Tätigkeiten	Zeitraum	AV-Vertrag
Unique Projects GmbH & Co. KG Schifferstraße 200, 47059 Duisburg	Allgemein	IT Support 2nd & 3rd Level	Seit 10.2019	Liegt vor
Unique Cloud GmbH Schifferstraße 200, 47059 Duisburg	Allgemein	Erbringung von Cloud-Leistungen (Hosting)	Seit 04.2023	Liegt vor
Drekopf Recyclingzentrum Essen GmbH, Schürmannstraße 19b, 45136 Essen	Allgemein	Aktenvernichtung	Seit 11.2022	Liegt vor
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Mental Health Week Digitale Kanäle Longevity Day	Verwaltung Datenbankserver	Seit 02.2023	Liegt vor
sli.do s. r. o. Vajnorska 100/A 831 04 Bratislava (Slowwakei)	Mental Health Week	Organisation von Q&A-Sessions	Seit 03.2025	Liegt vor
Base-t GmbH & Co. KG, Max-Keith-Str. 11, 45136 Essen	Digitale Kanäle Longevity Day Mental Health Week	Verwaltung Datenbankserver	Seit 09.2018	Liegt vor
united-domains AG, Gautinger Straße 10, 82319 Starnberg	Digitale Kanäle	Domainverwaltung und Mailversand	Seit 05.2019	Liegt vor
ALL-INKL.COM - Neue Medien Münnich, Hauptstraße 68, 02742 Friedersdorf	Mental Health Week Digitale Kanäle Longevity Day	Domainverwaltung und Mailversand	Seit 07.2021	Liegt vor
Sendinblue GmbH, Köpenicker Straße 126, 10179 Berlin	Mental Health Week Digitale Kanäle Longevity Day	E-Mail-Dienstleistungen	Seit 05.2019	Liegt vor
rapidmail GmbH, Wentzingerstr. 21, 79106 Freiburg	Mental Health Week	E-Mail-Dienstleistungen	Seit 02.2025	Liegt vor

Cloudflare, Inc. 101 Townsend St, San Francisco, CA 94107	Mental Health Week Digitale Kanäle Longevity Day	Streamingfunktion, Lastenverteilung und Performance-Optimierung für Webinhalte	Seit 10.2023	Liegt vor
Rezeptprüfstelle Duderstadt GmbH, Adenauerring 25, 37115 Duderstadt	Gesundheitsberichte	Datenzusammenführung und Pseudonymisierung	Seit 04.2022	Liegt vor
DearEmployee GmbH, Bleicherstr. 14, 78467 Konstanz	Mitarbeitenden-befragung	Anbieter der Befragungsplattform	Seit 05.2024	Liegt vor
smartEvents GmbH Hermann-Mende-Straße 4 01099 Dresden	Longevity Day Mental Health Week	Plattform zur Veranstaltungs-durchführung	Seit 01.2026	Liegt vor

Anhang 2 - Übersicht der Standorte des Auftragnehmers

Standorte	postalische Anschrift	Telefonnummer E-Mail-Adresse
Team Gesundheit Gesellschaft für Gesundheitsmanagement mbH	Rellinghauser Straße 93 45128 Essen	Telefon: 0201/8 90 70 – 801 E-Mail: service@teamgesundheit.de

Anhang 3 - Übersicht der technischen und organisatorischen Maßnahmen (TOM)

Beschreibung der technischen und organisatorischen Maßnahmen

Angaben zum Verantwortlichen (Art. 30 Abs. 1 lit. a DS-GVO):

Verantwortlicher:
Team Gesundheit GmbH
Rellinghauser Str. 93, 45128 Essen (Deutschland)

Gesetzlicher Vertreter:
Dr. Carsten Stephan

Datenschutzbeauftragter:
Tim Schabio
Tel: 0201 / 890 66 123
E-Mail: schabio@datenschutz-ruhr.de

Stand: Dezember.2024
Version: 1.0

M.1 Maßnahmen zur Vertraulichkeit

M.1.1 Beschreibung der Zutrittskontrolle:

- Alarmanlage - Einsatz einer Alarmanlage (mit Meldung an Sicherheitsdienst) [umgesetzt]
- Besucherausweise - Vergabe von Besucherausweisen bei deren Anmeldung [umgesetzt]
- Besucherprotokollierung - Protokollierung der Besucher (Besucherbuch) [umgesetzt]
- Bewegungsmelder - Bewegungsmelder in Verbindung mit der Alarmanlage [umgesetzt]
- Permanente Begleitung bzw. Beaufsichtigung von Besuchern - Permanente Begleitung bzw. Beaufsichtigung von Besuchern [umgesetzt]
- Schließanlage - Einsatz einer Schließanlage mit Token-Zugangssytem [umgesetzt]
- Schlüsselverwaltung - Schlüsselregelung mit Dokumentation der Schlüssel (Schlüsselbuch); Schlüssel der IT zum Serverraum im Tresor [umgesetzt]
- Separater Serverraum - Baulich separierter, abschließbarer, beschränkt zugänglicher Serverraum mit
- eigenständiger Klimaanlage und Brandmeldern [umgesetzt]
- Sorgfältige Auswahl Reinigungspersonal - Reinigungspersonal ist sorgfältig ausgewählt und zur Verschwiegenheit verpflichtet [umgesetzt]
- Token-Zugangssystem - Einsatz eines Token-Zugangssystems und Schlüsseln der Schließanlage, die einen Zu- gang nur für Berechtigte ermöglichen [umgesetzt]
- Zutritt Serverraum reglementiert - Schlüssel zum Serverraum wird nur nach Kontrolle der Berechtigung durch eine befugte Person gegen Unterschrift herausgegeben; regelmäßig finden Zugänge zum Serverraum nur unter Anwesenheit des IT-Verantwortlichen statt. [umgesetzt]
- Erläuterung:
- Der Zutritt über den Haupteingang und die Etagentüren wird über RFID-Token autorisiert. Die Token sind nicht beschriftet und können entsprechend dem Gebäude nicht zugeordnet werden. [umgesetzt]
- Die Geschäftsräume der Team Gesundheit GmbH sind über (alarmgesicherte) Etagentüren vom Treppenhaus getrennt. Die Fenster im Erdgeschoss sind mit Funkmeldesystemen ausgestattet, mit Meldung an Sicherheitsdienst. [umgesetzt]
- Der Zutritt bzw. die Zufahrt zu einem Parkplatz im Hinterhof erfolgt über ein Tor. [umgesetzt]
- Einsatz eines Wach- und Schutzdienstes außerhalb der üblichen Arbeitszeiten. [umgesetzt]

M.1.2 Beschreibung der Zugangskontrolle:

- Authentifikation mit Benutzer + Passwort - [umgesetzt]
- Automatische Sperrung - Automatische Sperrung anhand definierter Zeiten und technischer Maßnahmen und
- zusätzlich auf Basis einer Arbeitsanweisung [umgesetzt]

- Benutzerberechtigungen - Benutzerberechtigungen verwalten (z.B. bei Eintritt, Änderung, Austritt) [umgesetzt]
- Datenträger unter Verschluss - Die Datenträger werden gesondert und unter Verschluss aufbewahrt [umgesetzt]
- Firewall - Einsatz von Firewalls zum Schutz des Netzwerkes, inklusive regelmäßiger Updates [umgesetzt]
- On- und Offboarding - Bei On- und Offboarding Rücksprache mit IT zur Einrichtung bzw. Sperrung der konkreten Zugänge, ebenfalls bei Veränderung der Befugnisse im laufenden Arbeitsverhältnis [umgesetzt]
- Passwortregelung - Passwörter müssen eine definierte Passwort-Richtlinie erfüllen [umgesetzt]
- Persönliche Benutzerkonten mit individueller Berechtigung - Einrichtung persönlicher Benutzerkonten zur Steuerung individueller Berechtigungen und Entfernung bei Ausscheiden des Benutzers [umgesetzt]
- Protokollierung von Anmeldeversuchen und Sperrung - Protokollierung von Anmeldeversuchen und Sperrung bei fehlgeschlagenen Anmeldeversuchen [umgesetzt]
- Sorgfältige Personalauswahl - Sorgfältige Auswahl von Reinigungspersonal und Sicherheitspersonal [umgesetzt]
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren, je nach Erforderlichkeit in den einzelnen Bereichen [umgesetzt]
- vom Publikumsverkehr getrennter Bereich für Datenverarbeitung - Die Datenverarbeitungsverlagen befinden sich in einem separaten Bereich [umgesetzt]
- Es wird sichergestellt, dass nur autorisierte Mitarbeitende Zugang zu den IT-Systemen, mit denen personenbezogene Daten erhoben bzw. verarbeitet werden oder auf diesen gespeichert sind, erlangen können. Dies betrifft sowohl den Zugang zu den Rechnern als auch zum Netzwerk. Darunter können auch technische Maßnahmen zur Netzwerksicherheit, wie der Betrieb von Firewalls oder Intrusion Detection Systeme fallen. [umgesetzt]
- Bei den organisatorischen Maßnahmen wird die Vergabe von Zugangsberechtigungen zu den Computersystemen (auf der Ebene der Betriebssysteme wie auch der eingesetzten Softwaresysteme und Web- dienste) geprüft. Auch Dienstanweisungen zum Umgang mit Passwörtern fallen entsprechend unter die Zugangskontrolle. [umgesetzt]
- Erläuterung: Der Server befindet sich in einem separaten, fensterlosen und klimatisierten Serverraum im Keller, für den nur die Administratoren eine Zugangsberechtigung haben. Die Kellerräume sind alarmgesichert. [umgesetzt]
- Zugehörige Dienstanweisung: Zugang zum Gebäude und zu den Geschäftsräumen
    - Der Zugang zum Gebäude und zu den Geschäftsräumen der Team Gesundheit GmbH ist durch elektronische Zugangsschlüssel geregelt. [umgesetzt]
    - Schlüssel dürfen nicht mit einem Namens- oder Adressetikett versehen werden. [umgesetzt]

    - Wenn ein Schlüssel verloren geht, muss dieser Verlust dem Sicherheitsdienst unverzüglich gemeldet werden. Das gilt auch an Wochenenden und an Feiertagen! Entsprechende Schlüssel und Token werden nach Verlust unmittelbar gesperrt.
    - Wenn Schlüssel übergeben oder zurückgegeben werden, wird ein entsprechendes Protokoll ausgefertigt. [umgesetzt]
- Umgang mit vertraulichen Unterlagen
    - Bei Verlassen der Diensträume, auch bei vorübergehender Abwesenheit, muss darauf geachtet werden, dass die Fenster verschlossen sind und durch eingeschaltete Elektrogeräte kein Schaden entstehen kann. [umgesetzt]
    - Akten und Vorgänge mit sensiblen Daten sind nach den Grundsätzen der DSGVO, des Sozialdatenschutzes und des Bundesdatenschutzgesetzes zu verwahren, d. h. bei Abwesenheit unter Verschluss zu halten. D.h. Schränke und Schreibtische sind abzuschließen. [umgesetzt]
    - Die Schlüssel zu Schränken und Schreibtischen sind so aufzubewahren, dass sie nicht in unbefugte Hände gelangen können. [umgesetzt]

M.1.3 Beschreibung der Zugriffskontrolle:

- Berechtigungskonzept - Erstellen und Einsatz eines Berechtigungskonzepts [umgesetzt]
- Datenlöschung - Sichere Löschung von Datenträgern vor deren Wiederverwendung (z.B. durch mehrfaches Überschreiben) [umgesetzt]
- Einsatz von Aktenvernichtern - Einsatz von Aktenvernichtern (min. Sicherheitsstufe 4 und Schutzklasse 3) [umgesetzt]
- Einsatz von Dienstleistern - Einsatz von Dienstleistern zur Akten- und Datenvernichtung mit DIN 66399 Zertifikat [umgesetzt]
- Passwortlichtlinien - Passwortrichtlinie inkl. Länge, Komplexität und Wechselhäufigkeit [umgesetzt]
- Sichere Aufbewahrung - Sichere Aufbewahrung von Datenträgern [umgesetzt]
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren [umgesetzt]
- Die Mitarbeitenden haben keinen Zugriff auf personenbezogene Daten, es sei denn, dies ist zur Erfüllung ihrer Aufgaben unbedingt erforderlich. Falls technisch und organisatorisch umsetzbar, ist einer möglichst geringen Anzahl an Mitarbeitenden eine entsprechende Zugriffsberechtigung zu erteilen. [umgesetzt]
- Alle Mitarbeitenden der Team Gesundheit GmbH sind durch die „Verpflichtung auf Vertraulichkeit“ zum sicheren Umgang mit Daten verpflichtet. [umgesetzt]
- Alle Rechner sind passwortgeschützt. Bildschirmschoner mit Passwort werden nach 5 Minuten aktiviert. Die Passwörter werden in Abständen von 12 Wochen erneuert (Erinnerung erfolgt automatisch). [umgesetzt]
- Folgende Anforderung werden an Passwörter gestellt: mindestens 8 Zeichen, Groß- und Kleinbuchstaben sowie Zahlen und Sonderzeichen. Das erste Passwort wird durch den

IT-Verantwortlichen vergeben. Es existiert eine Passworthistorie, um die Mehrfachverwendung von Passwörtern zu unterbinden. [umgesetzt]
- Papierunterlagen werden mit geeigneten Aktenvernichtern (DIN 66399) und entsprechender Schutzklasse 3 und Sicherheitsstufe 4 vernichtet. [umgesetzt]
- Auf jeder Etage im Hauptsitz in Essen sowie an allen Standorten stehen im Drucker-/Technikraum verschlossene Papiercontainer für Dokumente mit personenbezogenen Daten, welche durch den externen Dienstleister, die Firma Drekopf, datenschutzrechtlich entsorgt werden. [umgesetzt]

Maßnahmen zur Zugriffsverhinderung durch Löschen

- Die Löschung von Daten erfolgt unverzüglich, sofern ein derartiges Verlangen eines Betroffenen eingeht, etwaige zugrunde liegende Aufbewahrungsfristen überschritten, defekte Datenträger entsorgt werden oder sonstige Ereignisse eintreten, die eine Löschung nötig werden lassen. [umgesetzt]
- Die Löschung der Daten erfolgt rekursiv, d.h. alle Daten des Betroffenen werden gelöscht, es sei denn, die Löschung erfolgt aufgrund einer Überschreitung von Aufbewahrungsfristen oder spezialisierten Ereignissen, die ein selektives Löschen ermöglichen, d.h. Daten werden getrennt voneinander gelöscht und Teile der Daten eines Betroffenen verbleiben im System, sofern die Zweckmäßigkeit Bestand hat.
- Bei der Löschung ist dafür Sorge zu tragen, dass eine Wiederherstellung der Daten, insbesondere auf Datenträgern, verhindert wird. Dazu sind Systemfunktionen oder von der IT- Abteilung vorgeschriebene Programme zu nutzen, welche die Daten unbrauchbar machen („schreddern"). Erfolgt die Löschung auf dem System eines Benutzers, ist dieser für die Überprüfung der erfolgreichen Löschung selbst verantwortlich. [umgesetzt]

- Sperren - An die Stelle einer Löschung tritt eine Sperrung, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen, Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist. Personenbezogene Daten sind außerdem zu sperren, wenn die Richtigkeit seitens des Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt. [umgesetzt]

- Es gibt eine gesonderte Handhabung des täglichen WLAN-Schlüssels. [umgesetzt]

M.1.4 Beschreibung der Weitergabekontrolle:

- E-Mail-Verschlüsselung - E-Mail-Verschlüsselung mit S/MIME oder PGP Verfahren (oder anderen, dem Stand der Technik entsprechenden Verfahren), hier: Inhaltsverschlüsselung sensibler Anhänge, Passwortschutz [umgesetzt]

- Sichere Transportbehälter - Sichere Transportbehälter und -verpackungen [umgesetzt]
- SSL / TLS Verschlüsselung - Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet [umgesetzt]
- VPN-Tunnel - Einrichtungen von VPN-Tunneln zur Einwahl ins Netzwerk von außen [umgesetzt]
- Die Mitarbeitenden sind verpflichtet personenbezogene Daten nicht unbefugt auf Datenträgern zu speichern oder unautorisiert an Dritte weiterzugeben. Es wird durch geeignete technische Maßnahmensichergestellt, dass personenbezogene Daten bei einer elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. [umgesetzt]

  Anmerkung:
- Im Falle einer vereinbarten Übermittlung von personenbezogenen Daten dürfen diese nur verschlüsselt und mit einem ausreichend sicherem Passwort versehen an die bzw. von der Team Gesundheit GmbH übergeben werden. [umgesetzt]
- Die Speicherung der Daten erfolgt auf verschlüsselten Serverfestplatten. Der Zugang zu diesen Daten ist passwortgeschützt. Zugang zu den Daten haben nur Mitarbeitende der Team Gesundheit GmbH, die direkt mit der Bearbeitung der Daten betraut sind. [umgesetzt]
- Nach dem Erlöschen des Zwecks der Datenerhebung, werden die Daten unwiderruflich gelöscht. [umgesetzt]
- Eine automatisierte Datenweitergabe existiert im Unternehmen nicht. [umgesetzt]
- Für einen etwaigen Datentransport existieren verschlüsselte USB-Sticks, die in einer Liste vermerkt sind. Nutzungen der Sticks sind in der Liste zu vermerken. [umgesetzt]

M.1.5 Beschreibung des Trennungsgebots:

- Logische Mandantentrennung - Logische Mandantentrennung (softwareseitig) [umgesetzt]
- Physikalische Trennung der Daten - Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern [umgesetzt]
- Produktiv- und Testsystem - Trennung von Produktiv- und Testsystem [umgesetzt]
- Die Team Gesundheit GmbH gewährleistet, dass zu unterschiedlichen Zwecken erhaltene Daten getrennt verarbeitet werden. Dies geschieht durch:
    - Logische Datentrennung auf Basis von Kunden- und Auftragsnummern. [umgesetzt]
    - Logische und physikalische Trennung bzw. Verteilung der Applikationen und Daten auf verschiedene Server. [umgesetzt]
    - Vergabe von Zugriffsrechten. [umgesetzt]
- Die Team Gesundheit GmbH ist räumlich, organisatorisch und personell von den kooperierenden Krankenkassen und dem Unternehmen getrennt. [umgesetzt]
- In der Team Gesundheit GmbH gibt es keinen unkontrollierten Publikumsverkehr. [umgesetzt]

M.1.6 Beschreibung der Pseudonymisierung:

- IP-Adressen pseudonymisiert - Pseudonymisierte Erfassung von IP-Adressen (z.B. bei Marketing) [umgesetzt]
- Kennziffern - Verwendung von Kennziffern für Kunden, Patienten oder Personal anstatt Namen (in der Regel bereits seitens der Auftraggeber) [umgesetzt]
- Trennung Kontaktdaten - Trennung von Kontaktdaten und anderen Daten, insbesondere auch zwischen den einzelnen Unternehmensbereichen [umgesetzt]
- Trennung Stammdaten - Trennung von Kundenstammdaten und Auftragsdaten, insbesondere auch zwischen den einzelnen Unternehmensbereichen [umgesetzt]
- Die Team Gesundheit GmbH verarbeitet teils pseudonymisierte Daten für Krankenkassen. Auf Basis der angelieferten Daten und ihrer Auswertungen wäre potentiell und im Einzelfall ein Rückschluss aus den pseudonymisierten Daten auf einzelne Personen möglich. Daher werden Unternehmensteile mit weniger als 50 Mitgliedern zu größeren Einheiten zusammengefasst und Krankheitsarten mit weniger als 5 AU-Fällen im Tabellenband aus Datenschutzgründen unkenntlich gemacht. [umgesetzt]
- Da die einzubeziehenden Daten in der Regel in verschiedenen Datenkreisen organisiert vorliegen, muss sichergestellt sein, dass sie individuenbezogen zusammengeführt werden können. Die Datenzusammenführung und Datenpseudonymisierung erfolgt nach einer entwickelten Vorgehensweise (Verschlüsselungsalgorithmus wie AES 256 Bit). [umgesetzt]

M.1.7 Beschreibung der Verschlüsselung:

- Speicherung - Verschlüsselte Datenspeicherung (z.B. Dateiverschlüsselung nach AES256 Standard) [umgesetzt]
- Übertragung - Verschlüsselte Datenübertragung (z.B. E-Mailverschlüsselung nach PGP oder S/Mime, VPN, verschlüsselte Internetverbindungen mittels TLS/SSL, Einsatz FTAPI - Datentransfertool) [umgesetzt]

M.2 Maßnahmen zur Integrität

M.2.1 Beschreibung der Eingabekontrolle:

- Personalisierte Benutzernamen - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) [umgesetzt]
- Protokollierung - Protokollierung der Eingabe, Änderung und Löschung von Daten [umgesetzt]
- Zugriffsrechte - Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe. [umgesetzt]

- Sofern die Team Gesundheit GmbH im Rahmen ihrer Tätigkeit personenbezogene Daten erhebt oder durch Mitarbeitende verarbeiten (verändern) lässt, muss nachträglich feststellbar sein, ob und von wem Sozialdaten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. [umgesetzt]

Anmerkung:

- Die Datenverarbeitung erfolgt auf einem redundanten, zentralen Server. Es erfolgen regelmäßige zentrale Back-ups zur Datensicherung. Damit ist eine Eingabekontrolle im Wege eines Datenabgleichs möglich. [umgesetzt]

- Die Eingabe, evtl. Veränderungen und Löschung der Daten wird protokolliert. Dies gilt insbesondere für das eingesetzte CRM-System Vertec, in dem wiedergegeben ist, welche Person welchen Datensatz angelegt hat. [umgesetzt]

M.3 Maßnahmen zur Verfügbarkeit und Belastbarkeit

M.3.1 Beschreibung der Verfügbarkeitskontrolle:

- Antivirensoftware - Einsatz von Antivirensoftware zum Schutz vor Malware [umgesetzt]
- Auslagerung Datensicherung - Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort [umgesetzt]
- Backup- und Recoverykonzept - Erstellen eines Backup- & Recoverykonzepts [umgesetzt]
- Brandmeldeanlagen - Feuer- und Rauchmeldeanlagen [umgesetzt]
- Feuerlöschgeräte - CO_2 Feuerlöschgeräte in Serverräumen [umgesetzt]
- IT-Notfallplan - Erstellung und Anwendung von IT-Notfallplänen [umgesetzt]
- Klimaanlage - Klimaanlage in Serverräumen [umgesetzt]
- Redundante Datenhaltung - Redundante Datenhaltung (z.B. gespiegelte Festplatten, RAID 1 oder höher, gespiegelter Serverraum) [umgesetzt]
- Schutzsteckdosenleisten - Schutzsteckdosenleisten in Serverräumen [umgesetzt]
- Temperaturüberwachung - Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen [umgesetzt]
- Unterbrechungsfreie Stromversorgung - (USV) Unterbrechungsfreie Stromversorgung [umgesetzt]
- Die Team Gesundheit GmbH gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Dies geschieht durch:
    - Regelmäßige Anfertigung von Datensicherungen und die Möglichkeit der Wiederherstellung anhand eines Backup-Konzeptes. [umgesetzt]
    - Tägliche dezentrale Auslagerung von Datensicherungen innerhalb eines brandgeschützten Serverraumes. [umgesetzt]
    - Nutzung redundanter Speichermechanismen (RAID). [umgesetzt]
    - Serverraum mit eigenständiger Klimaanlage und Brandmeldern. [umgesetzt]

    - Betriebssystem: Windows-Server. [umgesetzt
    - Der redundante Server steht in einem verschlossenen, fensterlosen, alarmgesicherten und klimatisierten Serverraum im Keller der Rellinghauser Str. 93. 45128 Essen, Zugang zu diesem Raum haben nur die Administratoren der Team Gesundheit GmbH. [umgesetzt]
    - Die Festplatten des Servers sind entsprechend dem aktuellen Stand der Technik verschlüsselt. [umgesetzt]
- Datensicherung:
    - Redundante Server, über ein Raid-System gespiegelte Festplatten. Montags bis Freitags täglich ein volles Backup auf externen Festplatten, das verschlüsselt außerhalb der normalen Geschäftsräume sicher verwahrt wird. [umgesetzt]
    - Monatlich ein volles Backup. [umgesetzt]
- Webserver „Online-Befragung“:
    - Zur Durchführung von Online-Befragungen wird ein Server der Base-T GmbH genutzt. Ansprechpartner ist der Geschäftsführer Herr Orlik. Auf diesem Server ist die Befragungsplattform LimeSurvey installiert. Es werden täglich Backups durchgeführt. Ein Vertrag zur Auftragsdatenverarbeitung zwischen der Team Gesundheit GmbH und der Base- T GmbH besteht. Die Base-T GmbH betreibt nur das Hosting des Befragungssystems. Die Auswertung der erhobenen Daten erfolgt ausschließlich bei der Team Gesundheit GmbH. [umgesetzt]
- Webserver „Zentrale Prüfstelle Prävention“:
    - Zur Zertifizierung im Rahmen der Datenbank wird ein Server der ITSC GmbH genutzt. Es werden täglich Backups durchgeführt. Ein Vertrag zur Auftragsdatenverarbeitung zwischen der Team Gesundheit GmbH und ITSC GmbH besteht. [umgesetzt]
- Clients:
    - Notebooks und Standrechner mit Windows 10
    - Abgesichert über Firewall, aktuellen Virenwächter
    - Anmeldung über Passwort
    - Automatische Sperrung nach 5 Minuten Stillstand, Reaktivierung nur nach erneuter Passworteingabe
    - Verschlüsselung der Festplatten bei Notebooks und Standrechnern, die bei der Bearbeitung von Rohdaten genutzt werden
    - Software:MS-Office, SPSS, Teleform. [umgesetzt]

M.3.2 Beschreibung der raschen Wiederherstellbarkeit:

- Datenwiederherstellungen - Regelmäßige und dokumentierte Datenwiederherstellungen [umgesetzt]
- Notfallpläne - IT-Notfallpläne und Wiederanlaufpläne [umgesetzt]

M.4 Weitere Maßnahmen zum Datenschutz

M.4.1 Beschreibung der Auftragskontrolle:

- Audits - Regelmäßige Datenschutzaudits des externen Datenschutzbeauftragten [umgesetzt]
- Auswahl - Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) [umgesetzt]
- AV-Vertrag - Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO. [umgesetzt]
- DSB - Benennung eines Datenschutzbeauftragten [umgesetzt]
- Laufende Überprüfung - Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten [umgesetzt]
- Schulung - Schulungen aller zugriffsberechtigten Mitarbeiter. Regelmäßig stattfindende Nachschulungen. [umgesetzt]
- Verpflichtung - Verpflichtung auf die Vertraulichkeit gem. Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO [umgesetzt]

M.4.2 Beschreibung des Managementsystems zum Datenschutz:

- Audits - Durchführung regelmäßiger interner Audits [umgesetzt]
- Incident-Response-System - Incident-Response-System zur Nachvollziehbarkeit von Sicherheitsverstößen und Problemen [umgesetzt]
- Managementsystem Datenschutz - Managementsystem zum Datenschutz (z.B. in Anlehnung an VdS 10010) [umgesetzt]
- Managementsystem Informationssicherheit - Managementsystem zur Informationssicherheit (z.B. in Anlehnung an ISO 27001 oder VdS 3473) [umgesetzt]
- Schwachstellenanalysen - Durchführung regelmäßiger IT-Schwachstellenanalysen (z.B. Penetrationstest) [umgesetzt]
- Software Voreinstellungen - Einsatz von Software mit datenschutzfreundlichen Voreinstellungen gem. (Art. 25 Abs. 2 DS-GVO) [umgesetzt]
- Softwaregestützte Tools - Einsatz softwaregestützter Tools zur Einhaltung der datenschutzrechtlichen Anforderungen (z.B. audatis MANAGER, Privacy Guard) [umgesetzt]

Datenschutz-Managementsystem

- Die Team Gesundheit GmbH stellt sicher, dass die datenschutzrechtliche und datensicherheitstechnische Organisation der Datenverarbeitung gewährleistet ist. [umgesetzt]

Dies geschieht u.a. durch:

- Einsatz eines Datenschutzbeauftragten und einer internen Datenschutzkoordinatorin. [umgesetzt]
- Bewertung und Anpassung aller datenschutzrechtlichen Sachverhalte, insbesondere der technischen und organisatorischen Maßnahmen im Rahmen eines regelmäßigen Austauschs mit den Verantwortlichen. [umgesetzt]
- Anweisung aller Mitarbeitenden der Team Gesundheit GmbH, jegliche Veränderungen im Umgang mit personenbezogenen Daten an die interne Datenschutzkoordinatorin zu kommunizieren. [umgesetzt]
- Führung eines Verzeichnisses der Verarbeitungstätigkeiten. [umgesetzt]
- Verpflichtung aller Mitarbeitenden auf das Datengeheimnis und Durchführung regelmäßiger Schulungen aller Mitarbeitenden im Umgang mit personenbezogenen Daten. [umgesetzt)