

19. Nachtrag

**zum Datenstellenvertrag vom 01. Juli 2008 zur Durchführung der Disease-Management-
Programme in Hamburg**

zwischen

der Arbeitsgemeinschaft DMP Hamburg (ARGE)

der Kassenärztlichen Vereinigung Hamburg (KVH)

und

der AOK Rheinland/Hamburg – Die Gesundheitskasse

**dem BKK-Landesverband NORDWEST
zugleich für die Sozialversicherung für Landwirtschaft, Forsten und Gartenbau (SVLFG)
als Landwirtschaftliche Krankenkasse (LKK),**

der IKK – Die Innovationskasse,
zugleich handelnd für die Innungskrankenkassen, die diesem Vertrag beigetreten sind,

der KNAPPSCHAFT

und

den nachfolgend benannten Ersatzkassen

- **Techniker Krankenkasse (TK)**
- **BARMER**
- **DAK-Gesundheit**
- **Kaufmännische Krankenkasse – KKH**
- **Handelskrankenkasse (hkk)**
- **HEK – Hanseatische Krankenkasse**

gemeinsamer Bevollmächtigter mit Abschlussbefugnis:
Verband der Ersatzkassen e. V. (vdek),
vertreten durch die Leiterin der vdek-Landesvertretung Hamburg

der Gemeinsamen Einrichtung DMP Hamburg (GE)
(Auftraggeber)

und

**der Firma IQVIA Health System Services GmbH,
Sommerfelder Straße 120, 04316 Leipzig
(Datenstelle)**

Hinweis: Die Veröffentlichung steht unter dem Vorbehalt der Unterzeichnung des Nachtrages; das Unterschriftenverfahren wird derzeit durchgeführt.

Mit Wirkung ab 01.10.2026 wird der o.g. Vertrag wie folgt geändert:

1. Aktualisierung Datenstellenvertrag – Vertragstext

Der Vertragstext wird auf die als „20261001_DSV_HH_Lesefassung Vertrag“ dieses Nachtrages beigefügte Fassung geändert.

1.1. Die DAVASO GmbH wird umbenannt in IQVIA Health System Services GmbH.

1.2. Benennung Anlagen:

1.2.1. Anlage 5 heißt zukünftig „Bestimmungen zum Datenschutz und zur Datensicherheit bei der Datenverarbeitung im Auftrag inklusive der Anhänge A bis D“

1.3. Präambel:

In der Präambel wird als Indikation das DMP Rheumatoide Arthritis (Oktober 2026) ergänzt.

2. Anlage 1 „Aufgabenbeschreibung für die Datenstelle“

Die Anlage 1 sowie die Anhänge 2, 3 und 3a werden durch die beigefügten aktuellen Fassungen ersetzt.

3. Anlage 2 „Kommunikationsmatrix“

Die Anlage 2 wird durch die beigefügte aktuelle Fassung ersetzt.

4. Anlage 4 „Datensatzbeschreibung Vergütungsdatei“

Die Anlage 4 wird durch die beigefügte aktuelle Fassung ersetzt.

5. Anlage 5 „Bestimmungen zum Datenschutz und zur Datensicherheit bei der Datenverarbeitung im Auftrag inklusive der Anhänge A bis D“

Die Anlage 5 wird durch die beigefügte aktuelle Fassung ersetzt.

6. Anlage 6 „Verzeichnis der datenannehmenden Stellen der Krankenkasse“

Die Anlage 6 wird durch die beigefügte aktuelle Fassung ersetzt.

7. Anlage 10 „Musterschreiben an DMP-Ärzte“

Die Anlage 10 wird durch die beigefügte aktuelle Fassung ersetzt.

8. Anlage 11 „Prüfkatalog für Teilnahme- und Einwilligungserklärungen“

Die Anlage 11 wird durch die beigefügte aktuelle Fassung ersetzt.

Hamburg / Leipzig, den

.....
Kassenärztliche Vereinigung Hamburg*

.....
AOK Rheinland/Hamburg – Die Gesundheitskasse*

.....
BKK-Landesverband NORDWEST*
Zugleich für die SVLFG als LKK

.....
IKK – Die Innovationskasse*

.....
KNAPPSCHAFT*
Regionaldirektion Nord, Hamburg

.....
Verband der Ersatzkassen e. V. (vdek)*
Die Leiterin der vdek-Landesvertretung Hamburg

.....
IQVIA Health System Services GmbH

*Gleichermaßen handelnd als Mitglieder der Arbeitsgemeinschaft und der Gemeinsamen Einrichtung

**Datenstellenvertrag
zur Durchführung der Disease-Management-Programme
in Hamburg**

**in der Fassung des 19. Nachtrages vom 01.10.2026
zwischen**

der Arbeitsgemeinschaft DMP Hamburg (ARGE)

der Kassenärztlichen Vereinigung Hamburg (KVH)

und

der AOK Rheinland/Hamburg – Die Gesundheitskasse

dem BKK-Landesverband NORDWEST

zugleich für die Sozialversicherung für Landwirtschaft, Forsten und Gartenbau (SVLFG)
als Landwirtschaftliche Krankenkasse (LKK),

der IKK classic,

zugleich handelnd für die Innungskrankenkassen, die diesem Vertrag beigetreten sind,

der KNAPPSCHAFT

und

den nachfolgend benannten Ersatzkassen

- **Techniker Krankenkasse (TK)**
- **BARMER**
- **DAK-Gesundheit**
- **Kaufmännische Krankenkasse – KKH**
- **Handelskrankenkasse (hkk)**
- **HEK – Hanseatische Krankenkasse**

gemeinsamer Bevollmächtigter mit Abschlussbefugnis:

Verband der Ersatzkassen e. V. (vdek),

vertreten durch die Leiterin der vdek-Landesvertretung Hamburg

der Gemeinsamen Einrichtung DMP Hamburg (GE)

(Auftraggeber)

und

der Firma

**IQVIA Health System Services GmbH,
Sommerfelder Straße 120, 04316 Leipzig
(Datenstelle)**

Inhaltsverzeichnis

Erläuterungen

Begriffsbestimmungen

Präambel

Abschnitt I - Ziele, Vertragsgegenstand und Geltungsbereich

§ 1 Ziele

§ 2 Vertragsgegenstand

§ 3 Geltungsbereich

Abschnitt II - Datenmanagement

§ 4 Aufgabenbeschreibung

§ 5 Ausführungsfristen

§ 6 Statusdatensatz/Workflow-Daten

§ 7 Mitwirkung der Verbände der Krankenkassen in Hamburg und der KVH

§ 8 Grundsätze der Zusammenarbeit

§ 9 Änderung der zu erbringenden Leistung

Abschnitt III - Datenschutz

§ 10 Datenschutzmaßnahmen, Subunternehmer

§ 11 Datentransport

§ 12 Pflichten der Auftraggeber und der KVH

§ 13 Haftung bei Verletzung von Datenschutzbestimmungen

Abschnitt IV - Datenstellenprüfung

§ 14 Prüfung der Datenstelle und Prüfung der Versichertenzeiten nach § 20 Abs. 4 RSAV

Abschnitt V - Zusammenarbeit, Qualitätssicherung, Vertraulichkeit

§ 15 Grundsätze der Zusammenarbeit

§ 16 Qualitätssicherungsaktivitäten

§ 17 Förderung der elektronischen Dokumentation (eDMP)

§ 18 Vertraulichkeit

Abschnitt VI - Vergütung, Abrechnung und Pflichtverletzung

§ 19 Vergütung

§ 20 Abrechnung

§ 21 Fälligkeit der Zahlungen

§ 22 Pflichtverletzung, Haftung

§ 23 Freistellung von Ansprüchen Dritter

§ 24 Vertragsstrafe

Abschnitt VII - Sonstige Bestimmungen, Laufzeit

§ 25 Verdingungsunterlagen

§ 26 Erstreckung des Vertrages auf weitere DMP

§ 27 Rechte an Ergebnissen

§ 28 Schriftform

§ 29 Salvatorische Klausel

§ 30 Gerichtsstand

§ 31 Laufzeit, Kündigung

Begriffsbestimmungen

Arbeitsgemeinschaft DMP	Arbeitsgemeinschaft Disease-Management nach § 219 SGB V in der Region Hamburg
Auftraggeber	sind die im Rubrum aufgeführten Vertragsparteien
Arbeitstag	Als Arbeitstage gelten die Wochentage von Montag bis Freitag mit Ausnahme der gesetzlichen Feiertage
BDSG	Bundesdatenschutzgesetz
BSNR	Betriebsstättennummer
Bundeseinheitliche Vorgaben	Evaluation - Datensatzbeschreibung für die vereinbarten DMP Indikationen, Datensatzbeschreibungen, Formulare der Teilnahme- und Einwilligungserklärungen des Versicherten (TE/EWE), Plausibilitätsrichtlinien, Technische Anlage (einschließlich Anhänge), Aufbau Statusdatensatz/Workflow-Daten in der jeweils von der Arbeitsgemeinschaft DMP beauftragten Fassung
BAS	Bundesamt für Soziale Sicherung
Datensatz (Erst-/Folge-dokumentation)	Dokumentationsdaten entsprechend der jeweiligen Anlage der DMP-A-RL
Datenstelle	IQVIA Health System Services GmbH
DMP-A-RL	DMP-Anforderungen-Richtlinie in der jeweils gültigen Fassung
DMP-Datenzentrum des jeweiligen Verbandes der Krankenkassen/der jeweiligen Krankenkasse	Datenannahmestelle für die Dokumentationsdaten der Datenstelle
DMP-Krankenhäuser	Krankenhäuser, die vertraglich in die jeweiligen DMP-Vereinbarungen eingebunden sind und der Datenstelle mitgeteilt wurden
DS-GVO	Datenschutz-Grundverordnung
eDMP	Elektronische Datenübermittlung im Zuge von DMP
G-BA	Gemeinsamer Bundesausschuss der gemeinsamen Selbstverwaltung der Ärzte, Zahnärzte, Psychotherapeuten, Krankenhäuser und Krankenkassen in Deutschland.
Gemeinsame Einrichtung	Gemeinsame Einrichtung Hamburg nach § 25 Abs. 2 Satz 1 Nr. 1c RSAV

Koordinierende Ärzte	Ärzte, die vertraglich zur Koordination der DMP-Teilnehmer in die jeweiligen DMP-Vereinbarungen eingebunden sind
KVH	Kassenärztliche Vereinigung Hamburg
LANR	Lebenslange Arztnummer
RSAV	Risikostrukturausgleichsverordnung in der jeweils gültigen Fassung
SGB V	5. Sozialgesetzbuch in der jeweils gültigen Fassung
SGB X	10. Sozialgesetzbuch in der jeweils gültigen Fassung
TE/EWE	Teilnahme-/Einwilligungserklärung des Versicherten in der jeweils von der Arbeitsgemeinschaft DMP beauftragten Fassung, auf welcher der koordinierende Arzt auch die der Einschreibung zugrunde liegende Diagnose bestätigt.
Verbände der Krankenkassen in Hamburg	AOK Rheinland/Hamburg – die Gesundheitskasse BKK - Landesverband NORDWEST IKK classic KNAPPSCHAFT Sozialversicherung für Landwirtschaft, Forsten und Gartenbau (SVLFG) als Landwirtschaftliche Krankenkasse Verband der Ersatzkassen e. V. (vdek)
Vertragsärzte	Ärzte, die vertraglich zur Koordination der DMP-Teilnehmer in die jeweiligen DMP-Vereinbarungen eingebunden sind

Die rechtlichen Grundlagen bezeichnen immer die aktuelle gültige Fassung, sofern sie nicht um ein konkretes Datum ergänzt sind.

Personenbezeichnungen werden nachfolgend zur besseren Lesbarkeit in der männlichen Form verwendet. Es sind jedoch immer gleichrangig Personen jedweden Geschlechts gemeint.

Anlagen

Anlage 1	Aufgabenbeschreibung für die Datenstelle
Anhang 1	entfällt ersatzlos
Anhang 2	eDMP: Übermittlung der elektronischen DMP-Dokumentationen
Anhang 3	eDMP: Kurzbeschreibung DMPonline
Anhang 3a	eDMP: Antragsformular DMPonline
Anlage 2	Kommunikationsmatrix
Anlage 3	unbesetzt
Anlage 4	Datensatzbeschreibung zur Vergütungsdatei
Anlage 5	Bestimmungen zum Datenschutz und zur Datensicherheit bei der Datenverarbeitung im Auftrag inklusive der Anhänge A bis D
Anlage 6	Verzeichnis der datenannehmenden Stellen der Krankenkasse
Anlage 7	unbesetzt
Anlage 8	unbesetzt
Anlage 9	Verdingungsunterlagen
Anlage 10	Musterschreiben an DMP-Ärzte
Anlage 11	Prüfkatalog für Teilnahme- und Einwilligungserklärungen

Präambel

Zur Verbesserung der Versorgungssituation von chronisch erkrankten Patienten entwickelt der Gemeinsame Bundesausschuss die medizinischen Grundlagen für Disease-Management-Programme. Für folgende Indikationen haben die Verbände der Krankenkassen in Hamburg und die Kassenärztliche Vereinigung Hamburg strukturierte Behandlungsprogramme in Hamburg eingeführt:

- Diabetes mellitus Typ 2 (Juli 2003),
- Brustkrebs (April 2004),
- Koronare Herzkrankheit (KHK) (Februar 2006),
- Diabetes mellitus Typ 1 (Juli 2008)
- Asthma bronchiale sowie chronisch obstruktive Lungenerkrankungen (COPD) (Juli 2007),
- Osteoporose (Januar 2025),
- Rheumatoide Arthritis (Oktober 2026).

Die Umsetzung des DMP-Datenmanagements wird von der Datenstelle übernommen. Diese übernimmt Aufgaben im Zusammenhang mit TE/EWE und Dokumentationsdaten. Sie unterstützt Arztpraxen bei der Erstellung von Dokumentationen und übermittelt Daten an die jeweiligen Partner dieser Vereinbarung. Die Arbeitsabläufe in der Arztpraxis werden durch Nutzung der elektronischen Dokumentation (eDMP) vereinfacht. Um die Prozesse zu verbessern und weitere Erleichterungen in den Arbeitsabläufen in der Arztpraxis zu erzielen, wird das Datenmanagement laufend auf Optimierungsmöglichkeiten analysiert.

Dieser Vertrag ist eine Aktualisierung des bereits seit dem 01.03.2006 praktizierten Rechtsverhältnisses zwischen den Vertragspartnern und berücksichtigt die Zulassungsanforderungen nach der Risikostrukturausgleichsverordnung (RSAV) und der DMP-Anforderungen-Richtlinie (DMP-A-RL) in ihrer jeweils gültigen Fassung, jedoch nur, soweit auch der zugelassene DMP-Vertrag für die jeweilige Diagnose bereits an Änderungen der Anforderungen angepasst wurde.

Abschnitt I

Ziele, Vertragsgegenstand und Geltungsbereich

§ 1

Ziele

Die Partner dieser Vereinbarung verfolgen das Ziel, dass die Umsetzung der DMP durch ein möglichst optimales Datenmanagement vereinfacht wird. Auch eine möglichst hohe Zielerreichung von Qualitätssicherungsindikatoren soll durch das Datenmanagement unterstützt werden. Arztpraxen sollen zudem zielgerichtete Hilfen erhalten, damit der Arbeitsaufwand weiter reduziert werden kann.

§ 2

Vertragsgegenstand

- (1) Mit dieser Vereinbarung wird der Datenstelle die Umsetzung des Datenmanagements von den Auftraggebern übertragen. Die nähere Ausgestaltung der Beauftragung ist in der Anlage 1 geregelt. Hierzu gehören Aufgaben im Zusammenhang mit TE/EWE sowie Dokumentationsdaten.
- (2) Ferner sind Gegenstand dieses Vertrages die Qualitätssicherung des Datenmanagements - einschließlich der elektronischen Dokumentation (eDMP) - und die Prüfung der Datenstelle.

§ 3

Geltungsbereich

- (1) Diese Vereinbarung gilt für
 1. koordinierende Ärzte, die an der jeweiligen DMP-Vereinbarung in Hamburg teilnehmen,
 2. Krankenkassen, die in Hamburg ein zugelassenes DMP durchführen.
- (2) Die Vertragsärzte erklären die Teilnahme an dem jeweiligen DMP schriftlich gegenüber der KVH. Der koordinierende Vertragsarzt genehmigt mit seiner Unterschrift den Datenstellenvertrag.
- (3) Diese Vereinbarung gilt für alle zwischen den Vertragspartnern getroffenen DMP-Vereinbarungen (Diabetes mellitus Typ 2, Brustkrebs, Koronare Herzkrankheit, Diabetes mellitus Typ 1, Asthma bronchiale und COPD) sowie für im Rahmen der Laufzeit nach § 31 neu vereinbarte DMP. Zu den DMP Osteoporose, Herzinsuffizienz und Rheumatoide Arthritis

wurde der Auftragnehmer gemäß § 26 von den Auftraggebern ebenfalls mit der Umsetzung beauftragt. Die Umsetzung beginnt mit Inkrafttreten des jeweiligen Hauptvertrages für die Region Hamburg.

Abschnitt II

Datenmanagement

§ 4

Aufgabenbeschreibung

- (1) Die Datenstelle ist verpflichtet, die im Datenstellenvertrag vom 01.07.2008 in der Fassung des jeweils aktuellen Nachtrags beschriebenen Leistungen unter Berücksichtigung der aktualisierten Aufgabenbeschreibung nach Anlage 1 für alle vereinbarten DMP zu erbringen. Hierbei sind insbesondere die Regelungen zur Qualitätssicherung zu berücksichtigen.
- (2) Die in Anlage 1 beschriebenen Dienstleistungen werden unter Berücksichtigung der Anforderungen der DMP-A-RL, RSAV sowie des SGB X und der DS-GVO in ihrer jeweils geltenden Fassung erbracht.

§ 5

Ausführungsfristen

Die Ausführungsfristen richten sich nach der Aufgabenbeschreibung nach Anlage 1 und der Kommunikationsmatrix nach Anlage 2. Für die schriftliche Kommunikation mit Ärzten nutzt die Datenstelle die Musterschreiben nach der Anlage 10.

§ 6

Statusdatensatz/Workflow-Daten

Die Datenstelle liefert den DMP-Datenzentren der am DMP teilnehmenden Krankenkassen täglich (oder wöchentlich nach Vereinbarung) Informationen zum Stand der Verarbeitung der Dokumentationen mittels Statusdatensatz/Workflow-Daten (bundeseinheitliche Vorgabe). Der Aufbau des Statusdatensatzes/der Workflow-Daten richtet sich nach zwischen den Kassenorganisationen auf Bundesebene vereinbarten Datensatz in der jeweils gültigen Fassung. Die jeweils beauftragte Version des Statusdatensatzes wird der Datenstelle von der Geschäftsstelle der Arbeitsgemeinschaft DMP zur Verfügung gestellt.

§ 7

Mitwirkung der Verbände der Krankenkassen in Hamburg und der KVH

- (1) Die Verbände der Krankenkassen in Hamburg teilen der Datenstelle die Kostenträgerkennungen der von ihnen vertretenen, an den DMP-Vereinbarungen teilnehmenden Krankenkassen sowie die Adresse des jeweiligen DMP-Datenzentrums unverzüglich mit.
- (2) Die KVH stellt der Datenstelle mindestens zweimal monatlich und auf gesonderte Anforderung Vertragsarztnummern (LANR und BSNR), Namen angestellter Ärzte, Anschriften und möglichst Telefonnummern (Vertragsärzterverzeichnis) der an den jeweiligen DMP-Vereinbarungen teilnehmenden koordinierenden Ärzte mit Beginn und Ende der Teilnahme zur Verfügung. Änderungen von Vertragsarztnummern werden gesondert ausgewiesen.

§ 8

Grundsätze der Leistungserbringung

- (1) Die Datenstelle erbringt ihre Leistungen frei von Sach- und Rechtsmängeln
 - nach Maßgabe der vertraglichen Regelungen (einschließlich der Anlagen) und von der Geschäftsstelle der Arbeitsgemeinschaft DMP zur Verfügung gestellten bundeseinheitlichen Vorgaben und
 - dem allgemein anerkannten aktuellen Stand der Wissenschaft und Technik.

Die Datenstelle wird jeden Auftraggeber über - nach Vertragsabschluss eintretende - Änderungen des Standes von Wissenschaft und Technik, die möglicherweise Auswirkungen auf den Vertragsgegenstand haben, informieren.

- (2) Die von der Datenstelle zur Erfüllung ihrer Leistungen eingesetzten Mitarbeiter müssen die zur ordnungsgemäßen Vertragserfüllung notwendigen Kenntnisse und Erfahrungen besitzen sowie zur Beachtung der datenschutzrechtlichen Bestimmungen gemäß Anlage 5 verpflichtet sein. Dies gilt insbesondere für die Verpflichtung zur Verschwiegenheit hinsichtlich der patientenbezogenen Informationen.
- (3) Die Leistungserbringung durch die Datenstelle hat im Einklang mit den rechtlichen Vorschriften zu erfolgen. Insbesondere sind die Vorgaben des ärztlichen Standesrechts, des Wettbewerbsrechts sowie des Datenschutzrechts einzuhalten. Die Datenstelle hat die Einhaltung der rechtlichen Vorschriften und die sich aus Abschnitt III dieses Vertrages sowie Anlage 5 ergebenden datenschutzrechtlichen Verpflichtungen zu gewährleisten.
- (4) Die Datenstelle muss durch entsprechende organisatorische Vorkehrungen eine kontinuierliche orts- und zeitnahe Zusammenarbeit mit den jeweiligen Auftraggebern, der KVH und der Gemeinsamen Einrichtung ermöglichen. Eine Ansprechbarkeit zu den üblichen Bürozeiten (08:00 Uhr bis 18:00 Uhr) an Arbeitstagen ist zu gewährleisten.

- (5) Die Datenstelle ist jedem Auftraggeber über die vertragsgemäße Ausführung der Leistungen auskunftspflichtig und ermöglicht ihm zu den üblichen Bürozeiten insbesondere in die ihn betreffenden Datenbanken Einsicht.

§ 9

Änderung der zu erbringenden Leistung

- (1) Die Auftraggeber gemeinsam haben das Recht, die Aufgaben der Datenstelle zu ändern oder zu ergänzen, zu verringern oder zu erweitern, soweit dies insbesondere bei Änderungen der gesetzlichen oder rechtlichen Bestimmungen zu den DMP, die die Basis dieses Vertrages bilden, erforderlich wird oder es aufgrund der technischen Abwicklung für die Auftraggeber wirtschaftlicher ist, dass von der Datenstelle geschuldete Leistungen durch die Teilnehmer am DMP selbst erbracht werden. Die Auftraggeber können insbesondere

1. die Teilnahme-/Einwilligungserklärung und die Dokumentationsdaten,
2. das Format, in dem die Dokumentationsdaten übermittelt werden sollen,
3. die Plausibilitätsprüfrichtlinien
4. die Protokollierungen / den Statusdatensatz und
5. die Evaluationsdatensätze aktualisieren.

Die in der Aufzählung (1-5) genannten Formate müssen den bundeseinheitlichen Vorgaben in der jeweils beauftragten Fassung entsprechen.

- (2) Stellvertretend für die Auftraggeber ist die Geschäftsstelle der Arbeitsgemeinschaft DMP befugt, die Umsetzung der bundeseinheitlichen Vorgaben sowie von Sachverhalten die sich aus der Aufgabenbeschreibung (Anlage 1 zu diesem Vertrag) ergeben, gegenüber der Datenstelle zu beauftragen. Die Datenstelle wird von der Geschäftsstelle der Arbeitsgemeinschaft DMP über deren Sitz und Amtsdauer zu Beginn der Geschäftsführung schriftlich informiert. Für die Umsetzung von bundeseinheitlichen Vorgaben gem. Abs. 1 wird von den Auftraggebern und der Datenstelle ein formularbasiertes Änderungsverfahren verwendet. Die Einzelheiten hierzu werden im Schriftverkehr geregelt.
- (3) Ferner hat ein Auftraggeber das Recht, die Aufgaben der Datenstelle zu ändern oder zu ergänzen, sofern er durch gesetzliche, richterliche oder aufsichtsbehördliche Vorgaben hierzu verpflichtet ist. Die entsprechenden Informationen werden der Datenstelle unverzüglich zur Verfügung gestellt. Für die Umsetzung der Aufgaben wird der Datenstelle eine angemessene Frist eingeräumt.
- (4) Sofern sich durch gemeinsam vereinbarte Änderungen oder Ergänzungen kein wesentlicher Mehr- oder Minderaufwand für die Datenstelle ergibt, ändert sich die Vergütung nicht. Andernfalls ist die Vergütung entsprechend dem veränderten Aufwand einvernehmlich anzupassen.

Abschnitt III

Datenschutz

§ 10

Datenschutzmaßnahmen, Subunternehmer

- (1) Der Schutz der Daten bei der Datenverarbeitung im Auftrag erfolgt unter besonderer Berücksichtigung des Artikels 28 DS-GVO und des § 80 SGB X. Näheres ist in Anlage 5 geregelt.
- (2) Die von der Datenstelle vertragsgemäß vorzuhaltenden personenbezogenen oder personenbeziehbaren Daten und Dokumente werden nach der erfolgreichen Übermittlung an die Krankenkassen von der Datenstelle archiviert. Die Datenstelle archiviert die Originaldokumente bzw. Datensätze gemäß § 5 Abs. 2 Buchstabe b DMP-A-RL. Sie werden nach Ablauf dieser Frist unverzüglich, spätestens aber innerhalb eines Zeitraums von sechs Monaten von der Datenstelle gelöscht.
- (3) Die Datenstelle liefert den Auftraggebern die für die Meldung nach § 80 Abs. 3 SGB X erforderlichen Angaben.

§ 11

Datentransport

- (1) Daten sind über Datenfernübertragung (DFÜ) entweder per FTAM/IP oder SFTP-Server auszutauschen. Die Initiative für den DFÜ-Kommunikationsvorgang übernimmt der Absender. Der Absender hat sicherzustellen, dass der Kommunikationspartner die für den Empfang der Daten berechtigte Stelle ist. Dies kann über die Vergabe entsprechender Logins und Passwörter oder Datenaustauschschlüssel geschehen. Im Falle von Übertragungsabbrüchen gilt, dass die betroffene Datei vom Absender erneut übertragen wird. Zur Einrichtung des Datenaustausches per FTAM/IP oder SFTP müssen die Verbindungsparameter zwischen den Austauschpartnern vereinbart und jede Änderung im Folgenden den beteiligten Partnern gemeldet werden; jede Änderung ist unverzüglich und rechtzeitig im Voraus den beteiligten Stellen bekanntzugeben. Zur Sicherstellung eindeutiger Partnernamen im DFÜ-Datenaustausch werden die jeweiligen IK-Nummern der Partner verwendet.

§ 12

Pflichten der Auftraggeber

- (1) Die Auftraggeber entscheiden über die Zulässigkeit der Datenverarbeitung und bleiben in jeder Phase der Datenverarbeitung jeweils verantwortlich für die Wahrung der Rechte derjenigen, deren Daten verarbeitet werden. Die Krankenkassen/Ersatzkassen behalten deshalb das alleinige Verfügungsrecht über die Daten.
- (2) Aufträge werden von den Auftraggebern schriftlich bzw. in Textform erteilt. Die Auftraggeber haben auf Anforderung der Datenstelle Aufträge, Weisungen und Erläuterungen zu präzisieren.
- (3) Die Auftraggeber sind verpflichtet und berechtigt, erforderlichenfalls Weisungen nach § 80 Abs. 2 SGB X betreffend die Ergänzung der bei der Datenstelle vorhandenen technischen und organisatorischen Maßnahmen schriftlich zu erteilen.
- (4) Die weisungs-, empfangs- und kontrollberechtigten Personen - im Rahmen des Auftragsverhältnisses - sind der Datenstelle von den Auftraggebern schriftlich zu benennen. Sie haben sich bei der Ausübung ihrer Befugnisse zu legitimieren.

§ 13

Haftung bei Verletzung von Datenschutzbestimmungen

Die Haftung richtet sich nach § 22 dieses Vertrages und den gesetzlichen Bestimmungen. Die Datenstelle bestätigt, sich gegen die Inanspruchnahme wegen Verletzung von Datenschutzvorschriften versichert zu haben. Die Versicherungssumme beträgt mindestens 500.000,00 EUR.

Abschnitt IV

Datenstellenprüfung

§ 14

Prüfung der Datenstelle und Prüfung der Versichertenzeiten nach § 20 Abs. 4 RSAV

- (1) Die Auftraggeber können die vertragsgemäße Ausführung der Leistung in den Räumen der Datenstelle prüfen. Weitere Prüfverfahren sind mit der Datenstelle abzustimmen. Diese Prüfungen umfassen sowohl alle DMP als auch sämtliche Prozessabläufe. Inhalte der Datenstellenprüfung sind insbesondere:
- die Qualität der Dokumentationsdaten (Erst- und Folgedokumentationen) in Bezug auf:
 - Dokumentation des Posteinganges,
 - Prüfung des fristgerechten Eingangs,
 - Prüfung der Vollständigkeit und Plausibilität unter Berücksichtigung der Plausibilitätsrichtlinien der Kassenorganisationen auf Bundesebene,
 - die vertragsgemäße Umsetzung des Korrekturverfahrens unter Berücksichtigung der Anforderungen des Bundesamtes für Soziale Sicherung:
 - die Richtigkeit der Erfassung der Daten,
 - vollständige und lückenlose Archivierung der Dokumentationsdaten und des Schriftwechsels zum Korrekturverfahren.
- (2) Die Qualitätsprüfungen werden durch von der Arbeitsgemeinschaft DMP autorisierte Mitarbeiter der Mitglieds-kassen vorgenommen. Die für die Prüfungen autorisierten Mitarbeiter erhalten ein Merkblatt über die Dienstpflichten der Angestellten und geben vor Aufnahme ihrer Tätigkeit die Erklärung zum Datengeheimnis/Sozialgeheimnis gegenüber der Geschäftsstelle der Arbeitsgemeinschaft DMP ab. Die datenschutzrechtlichen Verpflichtungen gemäß Anlage 5 gelten auch im Verhältnis zur abordnenden Stelle und nach der Beendigung der Prüfung.
- (3) Die Prüfung erfolgt auf Basis von Stichproben aus dem in die Prüfung einbezogenen Datenbestand.
- (4) Es werden grundsätzlich 100 Fälle geprüft. Die Stichprobenfälle werden der Datenstelle zwei Wochen vor Beginn der Qualitätsprüfung bekannt gegeben. Im Fokus steht das sogenannte Image-Verfahren.
- (5) Die Prüfung erfolgt durch den Abgleich der den Krankenkassen übermittelten Datensätze mit den bei der Datenstelle vorliegenden Unterlagen.

- (6) Die Durchführung der Qualitätsprüfungen sowie deren Feststellungen sind fallbezogen zu dokumentieren. Feststellungen zu Einzeldatensätzen sind so zu pseudonymisieren, dass der Rückgriff auf die Daten der Datenstelle sowie der Daten der jeweiligen Krankenkasse möglich bleibt.
- (7) Das Ergebnis wird den Auftraggebern sowie der Datenstelle in Form eines Prüfberichtes bekannt gegeben. Die Prüfberichte sowie die dokumentierten Maßnahmen zur Umsetzung der Prüfergebnisse sind von der Datenstelle sowie der Arbeitsgemeinschaft DMP sieben Jahre, beginnend mit dem dem Prüfzeitraum folgenden Kalenderjahr, zu archivieren.
- (8) Die ergänzenden Regelungen/Aufgaben im Zuge der Prüfung der Versichertenzeiten nach § 20 Abs. 4 RSAV sind in der Anlage 1 zusammengefasst.
- (9) Den Aufsichtsbehörden und Prüfdiensten der Krankenversicherung ist seitens der Datenstelle ein umfassendes Prüfrecht einzuräumen, sofern dies zur Wahrung ihrer gesetzlich zugewiesenen Aufgaben notwendig ist.

Abschnitt V

Zusammenarbeit, Qualitätssicherung, Vertraulichkeit

§ 15

Grundsätze der Zusammenarbeit

- (1) Die Vertragsparteien verpflichten sich, zur Erfüllung dieses Vertrages konstruktiv und loyal zusammenzuarbeiten. Die Vertragspartner werden sich wechselseitig unverzüglich über alle Umstände und Geschehnisse informieren, die für die Zusammenarbeit nach diesem Vertrag bedeutsam sind oder sein könnten.
- (2) Die Auftraggeber haben gegenüber den von der Datenstelle eingesetzten Personen kein Weisungsrecht; zwischen ihnen besteht kein Arbeitsverhältnis.
- (3) Die Auftraggeber werden Anforderungen und/oder Weisungen ausschließlich an die von der Datenstelle zum Zeitpunkt des Vertragsschlusses schriftlich benannten verantwortlichen Personen richten. Änderungen der verantwortlichen Personen wirken gegenüber den Auftraggebern nur, wenn diese zuvor sämtlichen Auftraggebern schriftlich angezeigt wurden.

§ 16

Qualitätssicherungsaktivitäten

- (1) Die Ausführungsfristen der Aufgabenbeschreibung nach § 4 sind zwingend einzuhalten. Sofern Störungen in den Datenprozessen eintreten, sind die Auftraggeber hierüber umgehend zu informieren (z. B. per E-Mail).
- (2) Die Datenstelle prüft die Dokumentationsdaten vor Versand an die Auftraggeber, KVH und Gemeinsame Einrichtung in einem zusätzlichen Prüfungslauf. Eine abschließende Verlagerung der Haftungs- und Rügepflicht auf die Datenstelle ist damit nicht verbunden.
- (3) Vor Versand von Schreiben an die koordinierenden Ärzte werden diese regelmäßig stichprobenartig geprüft.
- (4) Die Datenstelle stellt die Qualifikation und Fortbildung ihrer Mitarbeiter sicher. Hierzu gehört insbesondere die Vermittlung von Fachwissen, wie z. B. Regelungen der RSAV und DMP-A-RL in der jeweils gültigen Fassung sowie Bestimmungen des Bundesamtes für Soziale Sicherung.
- (5) Die Geschäftsstelle der Arbeitsgemeinschaft DMP informiert die Datenstelle unverzüglich über notwendige Anpassungen der Datenflüsse aufgrund von Regelungen der RSAV und Bestimmungen des Bundesamtes für Soziale Sicherung.
- (6) Die Datenstelle bietet den DMP teilnehmenden Ärzten ihre Unterstützung bei Fragen zum Erstellen von Dokumentationen an. Ferner informiert sie anfragende Ärzte zu den DMP-Prozessen Einschreibung, Arztwechsel, Neueinschreibung etc. Informationen zur DMP-Vergütung sind ausschließlich der KVH vorbehalten.
- (7) Anregungen und Beschwerden von an den DMP teilnehmenden Ärzten werden dokumentiert und an die Geschäftsstelle der Arbeitsgemeinschaft DMP übermittelt. Die Aufzeichnung wird von der Datenstelle und der Geschäftsstelle der Arbeitsgemeinschaft DMP wahrgenommen. Ärzte erhalten kurzfristig - möglichst innerhalb von 48 Stunden - eine Rückmeldung zu ihren Anregungen / Beschwerden. Die Aufzeichnungen werden von der Geschäftsstelle der Arbeitsgemeinschaft DMP aufbewahrt und in den Gesprächen mit der Datenstelle erörtert.
- (8) Die Datenstelle dokumentiert ihre Qualitätssicherungsmaßnahmen und informiert die Verbände der Krankenkassen in Hamburg monatlich über Auffälligkeiten; liegen keine vor, gibt sie dazu eine kurze Information.
- (9) Um weitere Optimierungen des Datenmanagements zu erreichen, führen die Auftraggeber einmal jährlich Qualitätssicherungsgespräche mit der Datenstelle.

§ 17

Sicherstellung der elektronischen Dokumentation (eDMP)

- (1) Die Datenstelle unterstützt Vertragsärzte bei Fragen zu eDMP. Hierzu gehören auch Hilfen bei Fragen zur Praxissoftware.
- (2) Die Datenstelle stellt ein Online-Erfassungsverfahren für die DMP-Dokumentationen bereit. Dabei werden insbesondere die Regelungen des Datenschutzes beachtet. Die Online-Dokumentation steht den Vertragsärzten kostenfrei zur Verfügung.
- (3) Im Übrigen sind die Regelungen zu eDMP in den Anhängen zur Aufgabenbeschreibung nach Anlage 1 zusammengefasst.

§ 18

Vertraulichkeit

Die Vertragsparteien verpflichten sich gegenseitig, über alle von ihnen in Zusammenhang mit der Durchführung dieses Vertrages erlangten Kenntnisse und Informationen auch über das Ende der Vertragslaufzeit hinaus Stillschweigen zu bewahren. Alle vom Auftraggeber zur Verfügung gestellten Auskünfte und erlangten Informationen jeglicher Art dürfen ausschließlich bei der Zusammenarbeit der Vertragsparteien zur Erfüllung dieses Vertrages verwendet werden. Die Vertragsparteien werden diese Verpflichtungen auch ihren Mitarbeitern auferlegen. Die Vertragsparteien werden alle in Zusammenhang mit der Durchführung dieses Vertrages erlangten Kenntnisse und Informationen nur für den vertraglichen Zweck nutzen, zu dem sie übermittelt worden sind und nicht ohne die vorherige schriftliche Zustimmung des jeweiligen anderen Vertragspartners Dritten zugänglich zu machen oder gegenüber Dritten verwenden. Das Zustimmungserfordernis gilt nicht für gesetzlich vorgesehene Auskünfte gegenüber Behörden.

Abschnitt VI
Vergütung, Abrechnung und Pflichtverletzung

§ 19
Vergütung

(1) Die Datenstelle erhält für die von ihm nach diesem Vertrag geschuldeten Leistungen eine Vergütung wie folgt:

a) Im Falle der beleghaften Dokumentation:

für jeden vollständig und fehlerfrei abgeschlossenen Datenvorgang im Zusammenhang mit der TE/EWE, incl. der Weiterleitung des Originals und jeder Verbesserung in Papierform EUR 0,72414,

b) Im Falle der beleglosen Dokumentation:

(ba) für jeden vollständig und fehlerfrei abgeschlossenen Datenvorgang im Zusammenhang mit der Erstdokumentation EUR 0,78448,

(bb) für jeden vollständig und fehlerfrei abgeschlossenen Datenvorgang im Zusammenhang mit der Folgedokumentation EUR 0,78448.

Der Vergütungsanspruch versteht sich als Nettopreise ohne gesetzliche Mehrwertsteuer unter Einschluss sämtlicher Personal-, Sach-, Material-, Einrichtungs- und sonstigen Nebenkosten. Nicht im Pauschalpreis enthalten sind lediglich die anfallenden Portokosten für Nachforderungen. Die tatsächlichen Portokosten der Nachforderungen legt die Datenstelle im Verhältnis der betroffenen Versicherten auf die an diesem Vertrag beteiligten Krankenkassen um.

(2) Die vorstehenden Vergütungsansprüche der Datenstelle entstehen – für die TE/EWE - mit Eingang der TE/EWE bei der jeweiligen Krankenkasse bzw. nach vollständigem und fehlerfreiem Abschluss des Datenvorgang im Zusammenhang mit einer Erst- oder Folgedokumentation sowie der Versendung des Arzt-Reminders bei dem jeweiligen Auftraggeber bzw. der jeweiligen Krankenkasse. Die Fälligkeit des Anspruchs richtet sich nach unten genannten Absatz 5.

(3) Die vorstehenden Vergütungsansprüche der Datenstelle entstehen mit der Erfüllung des Datenmanagements nach der Aufgabenbeschreibung.

(4) Kann ein Datenvorgang innerhalb der Ausführungsfristen durch die Datenstelle nicht vertragsgerecht abgeschlossen werden, weil der koordinierende Vertragsarzt die Daten - obwohl die Datenstelle diese in dem von ihm geschuldeten Umfang nachgefordert hat - nicht

vollständig bzw. plausibel übermittelt, steht der Datenstelle für diesen eingeleiteten Datenvorgang ebenfalls die vollständige Vergütung nach Absatz 1 zu.

- (5) Die Vergütungsansprüche bestehen jeweils nur gegen die Krankenkassen. Vergütungsansprüche nach diesem Vertrag können gegenüber der Arbeitsgemeinschaft DMP, den koordinierenden Ärzten, der Gemeinsamen Einrichtung und der KVH nicht geltend gemacht werden. Die Auftraggeber haften nur für ihre eigenen Kosten nach § 20. Eine gesamtschuldnerische Haftung der Auftraggeber besteht nicht.
- (6) Die Fehlerfreiheit der Leistungserbringung ist von der Datenstelle nachzuweisen.
- (7) Der Wegfall oder die Minderung des Vergütungsanspruchs steht einem Schadensersatzanspruch nicht entgegen. Auf den Vertragsstrafenanspruch nach § 24 sind sie nicht anzurechnen.

§ 20

Abrechnung

- (1) Die Datenstelle erstellt monatlich einmal eine Rechnung an den jeweiligen Auftraggeber über die für diesen im Vormonat erbrachten Leistungen. Für Krankenkassen mit geringem Datenaufkommen ist eine quartalsweise einmalige Rechnungslegung für erbrachte Leistungen aus dem Vorquartal möglich.
- (2) Die Rechnungen müssen folgende Angaben enthalten:
 - Anzahl der weitergeleiteten TE/EWE;
 - Angabe über die Zahl vollständig und fehlerfrei abgeschlossener Datenvorgänge im Rechnungszeitraum, gegliedert nach der Art der Dokumentationsdaten (Erst- und Folgedokumentation);
 - die Anzahl der Datenvorgänge im Rechnungszeitraum, die trotz im geschuldeten Umfang erfolgter Nachforderung durch die Datenstelle nicht vollständig und/oder fehlerfrei abgeschlossen werden konnten.

Auf Anfrage eines Auftraggebers sind auch das Datum von Eingang und Ausgang der in Rechnung gestellten TE/EWE bei der Datenstelle anzugeben. Für die Rechnungsprüfung übermittelt die Datenstelle im Statusdatensatz/im Workflow-Datensatz die Rechnungsnummer.

Darüber hinaus ist den jeweiligen Rechnungen eine separate Liste beizufügen, in der unter Nennung der Arztnummer des jeweiligen kooperierenden Vertragsarztes und der Versi-

chertennummern mitgeteilt wird, welche Datenvorgänge für Versicherte des jeweiligen Auftraggebers vollständig und fehlerfrei abgeschlossen wurden. Der jeweilige Auftraggeber kann den Umfang der an ihn zu übermittelnden Informationen erweitern.

§ 21

Fälligkeit der Zahlungen

Die nach Maßgabe von § 20 erstellten Rechnungen sind vom jeweiligen Auftraggeber innerhalb von 15 Arbeitstagen nach Eingang der Rechnung bei diesem zu begleichen. Die Datenstelle kann nach Ablauf von 12 Monaten nach Eingang der jeweiligen Rechnung beim jeweiligen Auftraggeber keine Nachforderungen für den abgerechneten Zeitraum mehr erheben.

§ 22

Pflichtverletzung, Haftung

- (1) Erbringt die Datenstelle fällige Leistungen nach diesem Vertrag bzw. nach Kapitel II der Verdingungsunterlagen (Anlage 9) nicht oder nicht wie geschuldet innerhalb der für die jeweilige Leistung vereinbarten Ausführungsfrist, kann der jeweilige Auftraggeber die Leistung selbst vornehmen und Ersatz der erforderlichen Aufwendungen, Minderung, Schadensersatz oder gemäß § 284 BGB Ersatz vergeblicher Aufwendungen verlangen, nachdem er der Datenstelle eine angemessene Frist zur Erfüllung seiner Leistung aufgegeben hat. Dies gilt nicht, wenn die Datenstelle die Pflichtverletzungen nicht zu vertreten hat.
- (2) Darüber hinaus haftet die Datenstelle dem jeweiligen Auftraggeber für alle Schäden, die dem jeweiligen Auftraggeber durch eine Pflichtverletzung der Datenstelle entstehen, es sei denn, die Datenstelle hat die Pflichtverletzung nicht zu vertreten. Dies gilt insbesondere für Verletzungen der Pflichten der Datenstelle nach Abschnitt III dieses Vertrages sowie Anlage 5. Die Datenstelle übernimmt die Haftung für Schäden des jeweiligen Auftraggebers und Dritter, die bei der unzulässigen Erhebung, Verarbeitung oder Nutzung der Daten entstehen.

§ 23

Freistellung von Ansprüchen Dritter

- (1) Die Datenstelle hat jeden Auftraggeber von allen gesetzlichen Ansprüchen Dritter freizustellen, die sich im Zusammenhang mit diesem Vertrag aus einer fehlerhaften Leistung oder sonstigem Vertragsverstoß der Datenstelle ergeben.
- (2) Die Datenstelle verpflichtet sich, zur Abdeckung von Risiken nach Absatz 1 ausreichende Versicherungen abzuschließen. Diese Versicherungen sind gegenüber jedem Auftraggeber nachzuweisen.

§ 24

Vertragsstrafe

- (1) Erbringt die Datenstelle schuldhaft die von ihr nach diesem Vertrag sowie insbesondere nach der Aufgabenbeschreibung geschuldeten Leistungen nicht oder nicht fehlerfrei innerhalb der für die jeweilige Leistung vereinbarten Ausführungsfrist, steht dem jeweils betroffenen Auftraggeber bei verspäteter Leistungserbringung für jeden Tag der Fristüberschreitung ein Vertragsstrafenanspruch in folgender Höhe zu:
 - im Zusammenhang mit der Teilnahmeerklärung / Einwilligungserklärung:
1,00 EUR je Teilnahme-/Einwilligungserklärung;
 - im Zusammenhang mit der Erst- oder Folgedokumentation, soweit die Leistungen gegenüber dem jeweiligen Auftraggeber geschuldet sind:
2,00 EUR je Dokumentationsvorgang;
 - im Zusammenhang mit der Erst- und Folgedokumentation, soweit die Leistungen gegenüber der Arbeitsgemeinschaft DMP geschuldet sind:
1,00 EUR je Dokumentationsvorgang.
- (2) Der Vertragsstrafenanspruch ist der Höhe nach begrenzt auf 10 v. H. der Rechnungssumme, die der Datenstelle im Falle einer fehlerfreien Leistungserbringung gegenüber sämtlichen Auftraggebern in dem Zeitraum, für den eine Vertragsstrafe beansprucht wird, zustände.

Abschnitt VII

Sonstige Bestimmungen, Laufzeit

§ 25

Verdingungsunterlagen

Die Verdingungsunterlagen in der Fassung des Datenstellenvertrags vom 01.03.2006 in der Fassung des 7. Nachtrags vom 26.06.08 sind als Anlage 9 Bestandteil dieses Vertrags und gelten für die Laufzeit des Vertrags gemäß § 31 unverändert fort, soweit in diesem Vertrag keine ausdrücklichen abweichenden Regelungen vereinbart wurden.

§ 26

Erstreckung des Vertrages auf weitere DMP

Die Datenstelle verpflichtet sich, das Datenmanagement im Rahmen der Einführung weiterer DMP zu übernehmen. Die Vergütung der Datenstelle bestimmt sich in diesem Fall nach § 19.

§ 27

Rechte an Ergebnissen

Die Datenstelle räumt den Auftraggebern unentgeltlich und unwiderruflich das ausschließliche, dauerhafte und übertragbare Recht ein, sämtliche im Rahmen des Vertrags erbrachten Leistungsergebnisse auf alle Arten, soweit gesetzlich zugelassen, zu nutzen.

§ 28

Schriftform

Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für einen etwaigen Verzicht auf das Erfordernis der Schriftform selbst. Mündliche Nebenabreden bestehen nicht.

§ 29

Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden oder sollte eine Lücke dieses Vertrages offenbar werden, so berührt dies nicht die Wirksamkeit der übrigen Bestimmungen dieses Vertrages. Die Vertragsparteien sind in einem solchen Fall verpflichtet, die unwirksame oder fehlende Bestimmung durch eine solche zu ersetzen, die

wirksam ist und dem mit der unwirksamen oder fehlenden Bestimmung angestrebten wirtschaftlichen Zweck soweit wie möglich entgegen kommt.

§ 30

Gerichtsstand

Ausschließlicher Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist Hamburg.

§ 31

Laufzeit, Kündigung

- (1) Dieser Vertrag löst den bisherigen Datenstellenvertrag vom 01.03.2006 in der Fassung des 7. Nachtrags ab und tritt mit Wirkung ab 01.07.2008 in Kraft.
- (2) Die Laufzeit dieses Vertrages ist unbefristet. Er kann mit einer Frist von 3 Monaten zum Ende eines Kalenderjahres gekündigt werden. Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt. Als ein wichtiger Grund gelten stets die Verletzung von gesetzlichen oder vertraglichen Datenschutzbestimmungen durch die Datenstelle sowie die vertragswidrige Übermittlung von Daten durch den Auftragnehmer an Staaten, 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 DS-GO vorliegt oder die Kündigung der DMP-Verträge mit der Kassenärztlichen Vereinigung Hamburg.
- (3) Die Auftraggeber können den Vertrag gemeinsam mit einer Frist von 3 Monaten zum Quartalsende kündigen, wenn die Erforderlichkeit der von der Datenstelle durchgeführten Tätigkeiten aufgrund von gesetzlichen oder sonstigen rechtlichen Änderungen der für DMP maßgeblichen Gesetze und Verordnungen entfällt.
- (4) Jeder Verband der Krankenkassen kann den Vertrag ganz oder teilweise mit Wirkung für eine DMP-Diagnose mit einer Frist von 3 Monaten zum Quartalsende kündigen, wenn eines der von ihm durchgeführten DMP, insbesondere wegen der nicht oder nicht mehr durch das BAS erteilten Akkreditierung, für ihn endet. Kündigt einer der Verbände der Krankenkassen in Hamburg für sich, berührt dies den Fortbestand des Vertrages gegenüber den übrigen Vertragspartnern nicht.
- (5) Kündigt einer oder kündigen sämtliche Verbände der Krankenkassen in Hamburg diesen Vertrag aus außerordentlichem Grund, den die Datenstelle zu vertreten hat, hat die Datenstelle den kündigenden Verbänden der Krankenkassen den Schaden zu ersetzen, der ihnen jeweils infolge der Kündigung entsteht.

Hamburg, den

Kassenärztliche Vereinigung
Hamburg*

AOK Rheinland/Hamburg*

BKK Landesverband NORDWEST*
- zugleich für die SVLFG als LKK -

IKK classic*

KNAPPSCHAFT*
- Regionaldirektion Nord, Hamburg -

Verband der Ersatzkassen e.V. (vdek)*
- Die Leiterin der vdek-Landesvertretung
Hamburg -

DAVASO GmbH

* Gleichermaßen handelnd als Mitglieder der Arbeitsgemeinschaft und der Gemeinsamen Einrichtung

Anlage 1

**Disease-Management-Programme
in Hamburg**

Aufgabenbeschreibung für die Datenstelle

Inhaltsverzeichnis

1	Einleitung	5
2	Verarbeitung der Teilnahme- und Einwilligungserklärungen (TE/EWE)	6
2.1	Entgegennahme der TE/EWE	6
2.2	Scannen der TE/EWE	6
2.3	Weiterleitung der TE/EWE	7
2.4	Prüfung der TE/EWE einschließlich Korrekturverfahren	7
2.4.1	Erfassung der TE/EWE	7
2.4.2	Prüfung der TE/EWE auf Vollständigkeit	8
2.4.3	Anforderung unvollständiger TE/EWE	8
2.4.4	Weiterleitung der TE/EWE	8
2.4.5	Verarbeitung von nicht vertraglich vereinbarten TE/EWE	9
2.4.6	Elektronische Archivierung der TE/EWE	9
3	Leistungen im Zusammenhang mit der Verarbeitung der Erst- und Folgedokumentationen (ED und FD)	10
3.1	Annahme der Dokumentationen	10
3.2	Archivierung der Dokumentationen	11
3.2.1	Archivierung bei belegloser Dokumentation	12
3.2.2	Archivierung bei beleghafter Dokumentation	13
3.3	Prüfung der Berechtigung des Arztes zur Erstellung von Dokumentationen	13
3.4	In Vertretung erstellte Dokumentation	14
3.5	Prüfung der Dokumentationen auf Einhaltung der Frist	14
3.6	Prüfung der Dokumentationen auf Mehrfachdokumentationen	15
3.7	Zwischenspeicherung der Dokumentationen	15
3.8	Pseudonymisierung der Datensätze	16
3.9	Prüfung der Dokumentationen auf Vollständigkeit und Plausibilität	16
3.10	Nachforderung für unvollständige bzw. nicht plausible Dokumentationen	17
3.11	Weiterleitung der Dokumentationen	19
4	Fallführung und Rückmeldeverfahren	19
4.1	Zweckgebundenheit des DMP-Falles	19
4.2	Generierung und Pflege des DMP-Falles	19
4.3	Definition und Speicherung des DMP-Falles	21
4.4	Meldungen der Krankenkassen	21
4.4.1	Meldung der Krankenkasse bei einem Wechsel der Kostenträgerkennung	22

4.4.2	Meldung der Krankenkasse bei Beendigung, Stornierung oder Reaktivierung von DMP-Einschreibungen	22
4.4.3	Beendigung von DMP-Fallverläufen durch die Datenstelle	23
5	Weiterleitung der Daten	23
5.1	Weiterleitung der Daten an die Krankenkasse	23
5.2	CSV-Satzformat der TE/EWE	24
5.2.1	Filterung nicht aktiver Diagnosen im CSV-Satzformat	24
5.2.2	Übertragung des Korrekturdatums im CSV-TE/EWE-Format	24
5.3	Weiterleitung der Daten an die Gemeinsame Einrichtung bzw. KVH	25
5.3.1	Erstellen des Arzt-Reminders	25
5.3.2	Datenweitergabe an den externen Evaluator	25
5.4	Testdatenlieferungen	27
5.5	Besonderheiten BKK'n	27
5.6	Besonderheiten IKK'n	27
6	Leistungen bei Prüfungen gem. § 20 Abs. 4 RSAV	28
6.1	Anforderung der zur Durchführung der Prüfung nach § 20 Abs. 4 RSAV relevanten Unterlagen	28
6.2	Definition Umfang und Zeitraum der vorzulegenden Unterlagen	29
6.3	Definition der vorzulegenden Unterlagen	29
6.4	Sortierfolge der Unterlagen	30
6.5	Versand der vorzulegenden Unterlagen	30
6.6	Verschlüsselung von Daten	30
6.7	Lieferschein	30
6.8	Nachforderung von Prüfunterlagen	31
7	Informationen an die Auftraggeber	31
7.1	Online-Recherche	31
7.2	Statusdatensatz	32
7.3	Verbandsstatistik	32
7.4	Information an den koordinierenden Arzt	33
7.5	Abrechnungsstatistiken	33
7.5.1	Vergütungsdatei für die Kassenärztliche Vereinigung	33
7.5.2	Rechnungsbegründende Unterlagen für die Krankenkassen	34

Hinweis

Die in dieser Aufgabenbeschreibung genannten Anlagen bezeichnen die Anlagen zum Datenstellenvertrag.

1 Einleitung

Der koordinierende Arzt erstellt für die Einschreibung von Versicherten eine TE/EWE sowie eine Erstdokumentation (auch erstmalige Dokumentation genannt) und bestätigt die Diagnose. Im weiteren Verlauf der DMP-Teilnahme erstellt er ausschließlich Folgedokumentationen (auch Verlaufsdokumentationen genannt). Bei der Diagnose Brustkrebs besteht die Besonderheit, dass nach einer präoperativen Erstdokumentation eine ergänzende postoperative Erstdokumentation erstellt werden kann. Die TE/EWE und die Dokumentationen leitet er an die Datenstelle weiter.

Die Datenstelle nimmt die TE/EWE an und leitet diese an die jeweiligen Krankenkassen weiter. Die Dokumentationsdaten aus den von den koordinierenden Ärzten übermittelten Erst- und Folgedokumentationen werden von der Datenstelle erfasst, sowie hinsichtlich ihrer fristgerechten Übermittlung, ihrer Vollständigkeit und Plausibilität geprüft. Entsprechend der detaillierten Beschreibung in den folgenden Gliederungspunkten fordert die Datenstelle notwendige Ergänzungen bzw. Berichtigungen der Dokumentationsdaten beim koordinierenden Arzt an.

Über die Erfassung, Prüfung und Weiterleitung von Dokumenten hinaus stellt die Datenstelle den Auftraggebern sowie den koordinierenden Ärzten Statistiken, Auswertungen und ein geschütztes Online-Rechercheverfahren bereit, welches Aufschluss über den Stand der Datenverarbeitung gibt. Bei Fragen zur Erfassung und Korrektur von Dokumentationen, werden die Ärzte durch eine telefonische Hotline unterstützt.

2 Verarbeitung der Teilnahme- und Einwilligungserklärungen (TE/EWE)

Der koordinierende Arzt sendet die vom Arzt und Versicherten (oder dessen gesetzlichen Vertreter) unterschriebene TE/EWE im Original (in Papierform, dazu zählt auch ein Ausdruck der TE/EWE aus der PVS) oder per Telefax an die Datenstelle. Sind auf dem Telefax technisch keine Übermittlungsdaten eingefügt worden, muss das Fax als solches gekennzeichnet und mit einem Eingangsvermerk versehen werden. Auf einem PC empfangene Faxe (Fax-Server) werden anerkannt, wenn sie qualifiziert elektronisch signiert sind oder mit den oben genannten Daten als Ausdruck vorliegen. Der PVS-Ausdruck sollte einen Formularschlüssel enthalten. Weist die ausgedruckte TE/EWE keinen Formularschlüssel auf, erfolgt eine Sichtprüfung, ob die TE/EWE den derzeit gültigen Vordrucken entspricht (z.B. eine Versichertenunterschrift usw. enthält). Wenn die TE/EWE der aktuell gültigen entspricht, erfolgt eine Verarbeitung analog des normalen Vordrucks. Ist die ausgedruckte TE/EWE offensichtlich fehlerhaft, ist diese zurückzuweisen.

2.1 Entgegennahme der TE/EWE

Die Datenstelle nimmt die TE/EWE an und versieht sie auf der Vorderseite mit einem Eingangsstempel. Dabei ist ein Stempel zu verwenden, der das Institutionskennzeichen der Datenstelle beinhaltet. Änderungen bzw. Ergänzungen der TE/EWE werden von der Datenstelle nicht vorgenommen.

2.2 Scannen der TE/EWE

Alle bei der Datenstelle eingehenden TE/EWE werden eingescannt. Die Images werden den Krankenkassen auf Anforderung zur Verfügung gestellt. Nur soweit einzelne Krankenkassen die Datenstelle mit der Erbringung der unter Punkt 2.4 beschriebenen Prüfung der TE/EWE einschließlich Korrekturverfahren beauftragt haben, sind die Images auch versichertenbezogen zur Verfügung zu stellen.

2.3 Weiterleitung der TE/EWE

Die Datenstelle sortiert innerhalb eines Arbeitstages die nach Punkt 2.1 angenommenen TE/EWE nach den an den DMP teilnehmenden Krankenkassen je DMP und leitet diese zweimal wöchentlich auf gesichertem Transportweg im Original an das DMP-Datenzentrum bzw. die jeweilige Krankenkasse weiter.

2.4 Prüfung der TE/EWE einschließlich Korrekturverfahren

2.4.1 Erfassung der TE/EWE

Die TE/EWE werden vor dem Scannen (vgl. Punkt 2.2) auf der Vorderseite eindeutig mit einem Barcode gekennzeichnet. Alle bei der Datenstelle eingegangenen und eingescannten TE/EWE werden elektronisch als Datensätze erfasst. Für jede TE/EWE werden folgende Felder erfasst:

- Kopfdaten
 - Kostenträgerkennung
 - Lebenslange Arztnummer (LANR)
 - Betriebsstättennummer (BSNR)
 - Krankenversichertennummer
 - Kopfdatum
 - Diagnose
 - Name des Versicherten
 - Vorname des Versicherten
 - Geburtsdatum des Versicherten
 - Status des Versicherten
- Unterschriftsdatum TE/EWE Versicherter
- Unterschrift TE/EWE Versicherter vorhanden (J/N)
- Unterschriftsdatum Arzt
- Unterschrift Arzt vorhanden (J/N)
- Formularschlüssel

Das Vorhandensein eines Arztstempels ist nicht erforderlich, sofern die LANR und die BSNR in den Kopfdaten eindeutig erkennbar sind. Die LANR und die BSNR können auch vom Arztstempel übernommen werden, wenn diese nicht in den Kopfdaten enthalten sind.

Bei Nichtvorhandensein des Unterschriftsdatums vom Arzt und / oder vom Versicherten ist ersatzweise das Posteingangsdatum bei der Datenstelle maßgeblich.

Bei mehreren angekreuzten Diagnosen auf der TE/EWE ist für jede Diagnose ein gesonderter Datensatz mit Bezug zum Urbeleg anzulegen, sofern das jeweilige Datensatzformat dies zulässt.

Hat der koordinierende Arzt auf der TE/EWE ausschließlich eine Diagnose angegeben, für die zu dem Zeitpunkt keine Verarbeitung durch diesen Datenstellenvertrag erfolgt, wird ein einmaliges Korrekturverfahren nach Punkt 2.4.3 eingeleitet. Bei der gleichzeitigen Angabe einer bestehenden DMP-Indikation und einer neuen DMP-Indikation erfolgt kein Korrekturverfahren.

Sofern es sich um einen Korrekturbogen der TE/EWE handelt, werden lediglich die fehlerhaften Felder neu erfasst.

2.4.2 Prüfung der TE/EWE auf Vollständigkeit

Die erfassten TE/EWE werden auf Vollständigkeit geprüft. Die Prüfung erfolgt gemäß den in der Anlage 11 des Datenstellenvertrages (Prüfkatalog für Teilnahme- und Einwilligungserklärungen) beschriebenen Regeln.

2.4.3 Anforderung unvollständiger TE/EWE

Die unvollständigen oder fehlenden Angaben auf den TE/EWE werden bei den koordinierenden Ärzten gemäß Punkt 3.10 angefordert. Eingehende Korrekturen werden ebenfalls nach Punkt 2.2 gescannt.

2.4.4 Weiterleitung der TE/EWE

Der elektronische Datensatz der TE/EWE wird an die datenannehmende Stelle der jeweiligen Krankenkasse weitergeleitet. Zusätzlich zu den nach Punkt 2.3 weitergeleiteten TE/EWE werden auch die bei der Datenstelle eingehenden Korrekturbögen der TE/EWE im Original an das DMP-Datenzentrum bzw. die jeweiligen Krankenkassen übermittelt.

2.4.5 Verarbeitung von nicht vertraglich vereinbarten TE/EWE

Für die TE/EWE ist nur das aktuelle, den bundeseinheitlichen Vorgaben entsprechende Formular zugelassen.

Werden TE/EWE mit Hilfe einer Praxissoftware erstellt und entsprechen diese inhaltlich dem oben benannten Formular, sind diese ebenso anzunehmen und zu verarbeiten. Fehlt lediglich der Formularschlüssel, sind die Formulare ebenso zu verarbeiten (siehe Punkt 2).

Sofern die koordinierenden Ärzte TE/EWE übermitteln, welche nicht zulässig sind, werden diese dennoch von der Datenstelle verarbeitet und an die Krankenkassen mit dem Statushinweis „nicht plausibel“ weitergeleitet.

Die Ärzte werden im Rahmen des Korrekturverfahrens mittels eines Textbausteins sowie der Visualisierung der entsprechenden Belege (gekreuzte Images) auf die Verwendung ungültiger Vordrucke hingewiesen und zur Neuausstellung aufgefordert.

2.4.6 Elektronische Archivierung der TE/EWE

Alle bei der Datenstelle für TE/EWE erfassten Datensätze und erstellten Images werden elektronisch archiviert. Für die Archivierung gilt, dass

- für die Vertragsregion Hamburg ein von den übrigen Vertragsregionen getrenntes Archiv angelegt wird;
- nur befugte Personen der Datenstelle Zugriff auf die archivierten Datensätze und Images haben;
- die datenschutzrechtlichen Regelungen zur Archivierung von Daten gemäß Anlage 5 zu beachten sind;
- die Datensätze und Images analog der Aufbewahrungsfrist für Dokumentationen zu archivieren sind;
- die eingesetzten Archivierungstechnologien den aktuellen Erkenntnissen zur Haltbarkeit/Datensicherheit entsprechen und eine verlustfreie Rekonstruktion der erfassten Daten zulassen;
- nach Ablauf der Aufbewahrungsfrist die archivierten Datensätze und Images unverzüglich zu löschen sind, spätestens aber innerhalb eines Zeitraums von 6 Monaten;
- die Datenstelle ein Archivierungskonzept vorzulegen hat, welches sie mit den Auftraggebern abstimmt.

3 Leistungen im Zusammenhang mit der Verarbeitung der Erst- und Folgedokumentationen (ED und FD)

Die Dokumentationen werden in belegloser Form (eDMP) bei der Datenstelle eingereicht.

Beim eDMP erfasst der koordinierende Arzt die Dokumentationen in seiner Praxis (Ort der Leistungserbringung). Die erfassten Dokumentationen werden in einer Übermittlungsdatei zusammengefasst, verschlüsselt und an die Datenstelle übermittelt. Die Übermittlungsdatei wird elektronisch über KV-Portal, DMPonline, KV Connect (Abschaltung zum 20.10.2025) oder KIM¹ an die Datenstelle übersandt. Die von der Arztpraxis als Datensatz an die Datenstelle übermittelten Dokumentationen müssen der zwischen den Kassenorganisationen auf Bundesebene und der Kassenärztlichen Bundesvereinigung abgestimmten Schnittstellenbeschreibung in der jeweils beauftragten Fassung entsprechen. Die Datenstelle wird über neue oder angepasste Schnittstellenbeschreibungen von den Auftraggebern rechtzeitig informiert.

Sofern bei der Datenstelle beleghafte Dokumentationen oder solche, die per Datenträger (CD-ROM, Diskette, DVD) übermittelt wurden, eingehen, wird der koordinierende Arzt über die Ungültigkeit informiert und aufgefordert, die Dokumentationsübermittlung erneut elektronisch durchzuführen.

3.1 Annahme der Dokumentationen

Die Datenstelle gewährleistet die unveränderte Übernahme der von den koordinierenden Ärzten elektronisch übermittelten Dokumentationsdaten in ihr EDV-System. Dabei dokumentiert sie elektronisch den Eingang der einzelnen Dokumentationen.

Sind die von einem koordinierenden Arzt übermittelten Daten unverschlüsselt und/oder mehrfach komprimiert worden, hat die Datenstelle diese Daten wie ordnungsgemäß übermittelte Daten zu behandeln. Die Datenstelle klärt die Ursachen der Nichtverschlüsselung bzw. der Mehrfachkomprimierung telefonisch mit dem koordinierenden Arzt.

Sofern das Handling in der Arztpraxis nicht ursächlich für die Nichtverschlüsselung bzw. die Mehrfachkomprimierung oder andere Auffälligkeiten in Bezug auf die Arztsoftware ist, informiert die Datenstelle die Hersteller der Arztpraxissoftware, die Geschäftsstelle der Arbeitsgemeinschaft DMP sowie die KVH über die bestehende Problematik.

¹ Es wird ein zeitlich begrenzter Parallelbetrieb von KV Connect und KIM vom 10.06.25 bis zum 20.10.2025 umgesetzt.

Sofern eine übermittelte Dokumentation nicht verarbeitet werden kann, jedoch zu ermitteln ist, welche Dokumentation betroffen ist, wird der Arzt telefonisch gebeten, diese Dokumentation erneut an die Datenstelle zu übermitteln.

Für nicht einlesbare Datenträger werden alle verfügbaren Möglichkeiten der Identifikation des betroffenen Arztes, wie ggf. vorhandenes Label, Anschreiben des Arztes, Briefumschlag etc. ausgenutzt. Sofern der betroffene Arzt zu ermitteln ist, wird er von der Datenstelle telefonisch darüber informiert, dass der Datenträger nicht lesbar ist, und gleichzeitig aufgefordert, die betroffenen Datensätze erneut elektronisch zu übermitteln. Sollte eine Identifikation des betroffenen Arztes nicht möglich sein, wird der Datenträger vernichtet; über die Zahl der betroffenen Datenträger wird die Geschäftsstelle der Arbeitsgemeinschaft DMP sowie die KVH monatlich informiert.

3.2 Archivierung der Dokumentationen

Alle bei der Datenstelle eingegangenen Dokumentationsdaten und –belege werden archiviert. Für die Archivierung gilt, dass

- alle eingegangenen Belege (Dokumentationen, Korrekturen von Dokumentationen, eDMP-Versandlisten bzw. Bestätigungsschreiben etc.) sowohl physisch, als auch als Image zu archivieren sind. Die Datenstelle hat sicherzustellen, dass jederzeit eine Verbindung in beide Richtungen zwischen Originalbeleg und Image hergestellt werden kann;
- für die Vertragsregion Hamburg ein von den übrigen Vertragsregionen getrenntes Archiv angelegt wird;
- nur befugte Personen der Datenstelle Zugriff auf die archivierten Dokumentationen bzw. Datensätze haben;
- die datenschutzrechtlichen Regelungen zur Archivierung von Daten gemäß Anlage 5 zu beachten sind;
- die eingegangenen Dokumentationen, alle eingegangenen Kopien mit Datenkorrekturen/ -ergänzungen sowie alle dazugehörigen eDMP-Versandlisten bzw. Bestätigungsschreiben und von der Datenstelle erzeugten Versandlisten bzw. Bestätigungsschreiben (in Dateiform) physisch gemäß § 5 Abs. 2 Buchstabe b DMP-A-RL zu archivieren sind. Begleitende personenbezogene Daten im Zusammenhang mit der Dokumentation, die sich aus den operativen Umsetzungsprozessen ergeben, dürfen nicht länger als die Dokumentationsdaten aufbewahrt werden;

- die Belege, Images bzw. Datensätze so zu archivieren sind, dass sie jederzeit und innerhalb von 4 Wochen für Prüfzwecke durch die Prüfdienste der Krankenversicherung der jeweiligen Krankenkasse zur Verfügung gestellt werden können
- die Datenstelle gewährleistet, dass die jeweiligen Prüfdienste der Krankenversicherung die Prüfung in den Räumlichkeiten der Datenstelle vornehmen kann. Erfolgt auf Wunsch der Prüfdienste der Krankenversicherung eine Prüfung der archivierten Dokumentationen bzw. Datensätze außerhalb der Räumlichkeiten der Datenstelle, gewährleistet die Datenstelle, dass ausschließlich die mit der Prüfung beauftragten Mitarbeiter der Prüfdienste der Krankenversicherung die entsprechenden Unterlagen erhalten. Diese Mitarbeiter werden der Datenstelle rechtzeitig vom Auftraggeber bzw. von den Prüfdiensten der Krankenversicherung benannt;
- die eingesetzten Archivierungstechnologien den aktuellen Erkenntnissen zur Haltbarkeit/Datensicherheit entsprechen und eine verlustfreie Rekonstruktion der erfassten Daten zulassen;
- nach Ablauf der Aufbewahrungsfrist gemäß § 5 Abs. 2 Buchstabe b DMP-A-RL die archivierten Belege, Images bzw. Datensätze unverzüglich zu vernichten bzw. zu löschen sind; spätestens aber innerhalb eines Zeitraums von 6 Monaten nach Beauftragung;
- abweichend von den vorstehenden Regelungen die Datenstelle personenbezogene Daten zu Dokumentationen umgehend löscht, wenn bis spätestens 18 Monate (beginnend ab dem Erstellungsdatum der Dokumentation) keine TE/EWE (Einwilligung des Versicherten in die Datenverarbeitung) vorliegt. Die Löschung der Daten basiert auf einer Rückmeldung der jeweiligen Krankenkasse bzw. auf weitergehenden Prozessen, welche zwischen Krankenkassen und Datenstelle im Zusammenhang mit der Prüfung auf Vorhandensein einer TE/EWE vereinbart sind;
- die Datenstelle ein Archivierungskonzept vorzulegen hat, welches sie mit den Auftraggebern abstimmt.

3.2.1 Archivierung bei belegloser Dokumentation

Beim beleglosen Dokumentationsverfahren werden die in elektronischer Form eingegangenen Dokumentationen in elektronischer Form gespeichert. Für die Archivierung der elektronischen Daten gilt, dass

- die Datensätze gemäß den Standards der elektronischen Datenarchivierung im Sozialversicherungssektor auf einem dazu geeigneten und gesetzlich erlaubten Medium zu speichern sind;

- die Datensätze mit einem Read-Only-Schutz zu speichern sind;
- die unzulässig übermittelten Datenträger (Diskette, CD-ROM, DVD) nicht archiviert, sondern zeitnah vernichtet werden müssen.

3.2.2 Archivierung bei beleghafter Dokumentation

Die Papierbelege werden direkt nach dem Scannen im Archiv eingelagert und können über die eindeutige Kennzeichnung jederzeit gefunden werden.

3.3 Prüfung der Berechtigung des Arztes zur Erstellung von Dokumentationen

Die Datenstelle führt die von der KVH übermittelten Informationen zur Berechtigung der Ärzte zur Erstellung von Dokumentationen in einer historisierten Arztliste zusammen. Für die vom 01.07.2008 an geltenden LANR und BSNR nach dem Vertragsarztrechtsänderungsgesetz historisiert die Datenstelle die Zuordnung zwischen koordinierendem Arzt und Betriebsstätte sowie der Berechtigung, Dokumentationen zu erstellen.

Bei Dokumentationen ist zu prüfen, ob der Arzt am betreffenden DMP teilnimmt und in der angegebenen Betriebsstätte zur Erbringung von DMP-Leistungen zugelassen ist. Sofern die Kombination aus LANR und BSNR nicht in der aktuellen Arztliste enthalten oder sie laut aktueller Arztliste nicht mehr gültig ist, wird die KVH per E-Mail informiert. Wird erst nach Erstellung der Dokumentation, jedoch noch innerhalb der geltenden Frist (vgl. Punkt 3.5) die Teilnahme des koordinierenden Arztes am DMP erklärt, ist die Dokumentation als gültig zu bewerten. Bei negativem Prüfergebnis wird hierüber die KVH informiert. Sofern die KVH die Berechtigung zur Dokumentationserstellung bis zum Ende der Frist bestätigt, wird die Dokumentation weiterverarbeitet.

Bei fehlender LANR und bekannter BSNR werden die fehlenden Daten im Rahmen des Korrekturverfahrens bei der Betriebsstätte angefordert. Bei fehlender BSNR und bekannter LANR werden die fehlenden Daten im Rahmen des Korrekturverfahrens beim betreffenden Arzt angefordert. In beiden Fällen erfolgt keine Information an die KVH.

Endet die Teilnahme eines koordinierenden Arztes, werden die während seiner Teilnahme erstellten und fristgemäß (vgl. Punkt 3.5) bei der Datenstelle eingegangenen Dokumentationen von der Datenstelle angenommen.

3.4 In Vertretung erstellte Dokumentation

Die Datenstelle prüft bei jeder eingehenden Dokumentation, ob das Kennzeichen „Dokumentation in Vertretung“ auf der Dokumentation vorhanden ist. Ist die Dokumentation von einem vertretenden Arzt erstellt worden, so wird die Dokumentation verarbeitet, sofern der vertretende Arzt am DMP teilnimmt.

3.5 Prüfung der Dokumentationen auf Einhaltung der Frist

Jede in der Datenstelle eingegangene Dokumentation wird auf Einhaltung der 52-Tage-Frist (10 Tage + 6 Wochen) geprüft. Die Frist beginnt nach Ablauf der Dokumentationszeiträume. Fällt das Ende der Frist auf einen Samstag, Sonn- oder Feiertag, endet die Frist mit dem folgenden Werktag. Maßgeblich für diese Prüfung ist das Posteingangsdatum der Datenstelle. Soweit Dokumentationen vom Arzt irrtümlich einer falschen Datenstelle zugesandt worden sind, ist es ausreichend, dass die Dokumentationen innerhalb der Frist bei der unzuständigen Datenstelle eingehen.

Dokumentationen müssen innerhalb der Frist vollständig und plausibel der Datenstelle vorliegen.

Die Datenstelle prüft auch die Einhaltung der Dokumentationsintervalle zwischen den Dokumentationen. Dabei gelten zu früh übermittelte Dokumentationen als gültig. Der Reminder setzt dann auf die letzte gültige Dokumentation auf.

Liegt das Posteingangsdatum außerhalb der Frist, wird die Dokumentation als „verfristet“ gekennzeichnet. Ist eine Dokumentation unvollständig und/oder unplausibel, führt die Datenstelle das Korrekturverfahren bis zum Ende der Frist durch. Nach Ablauf der Frist werden Dokumentationen mit unvollständigem und/oder unplausiblen Datensatz ebenfalls als „verfristet“ gekennzeichnet.

Für jede verfristete Dokumentation werden folgende Schritte von der Datenstelle durchgeführt:

- der jeweilige Arzt wird über die Verfristung der Dokumentation informiert (vgl. Punkt 7.4),
- die jeweilige Krankenkasse wird durch den Statusdatensatz über die Verfristung der Dokumentation informiert (vgl. Punkt 7.2).

Verfristete Dokumentationen werden nicht an die jeweilige Krankenkasse, die KVH und den jeweiligen Evaluator weitergeleitet.

3.6 Prüfung der Dokumentationen auf Mehrfachdokumentationen

Die Datenstelle prüft, ob eine eingegangene Dokumentation eine Mehrfachdokumentation ist. Eine Mehrfachdokumentation liegt vor, wenn eine Dokumentation eingeht, für die im selben Quartal bereits eine vollständige und plausible Dokumentation gleichen Typs vom selben Arzt bzw. der gleichen Betriebsstätte für denselben Versicherten und für dieselbe Diagnose vorliegt.

Sofern innerhalb eines Quartals vollständige und plausible Erst- und Folgedokumentationen wiederholt vom selben Arzt bzw. der gleichen Betriebsstätte für das gleiche DMP für einen Versicherten eingehen, sind diese Mehrfachdokumentationen von der Datenstelle nicht weiterzuverarbeiten und nicht dem gebildeten DMP-Fall zuzuordnen. Dies gilt auch, wenn die Mehrfachdokumentationen mit einem Korrekturkennzeichen gekennzeichnet sind und/oder ein abweichendes Ausstellungsdatum aufweisen.

Abweichend hiervon führt die Datenstelle bei der Diagnose Brustkrebs die Prüfung auf Mehrfachdokumentationen bei Folgedokumentationen nicht durch.

3.7 Zwischenspeicherung der Dokumentationen

Die erfassten Daten werden nach der Erfassung bei der Datenstelle in folgenden Zwischenspeichern gespeichert:

- Zwischenspeicher 1

Alle erfassten Datensätze werden in einer Datenbank unverändert (d. h. nicht pseudonymisiert, mit Arzt- und Versichertenbezug) gespeichert.

- Zwischenspeicher 2

Die für die Gemeinsame Einrichtung und die KVH bestimmten Datensätze mit Arztbezug und pseudonymisiertem Versichertenbezug (vgl. Punkt 3.8) werden auf einem von dem Zwischenspeicher 1 getrennten Medium gespeichert. Hierbei ist von der Datenstelle eine EDV-Lösung einzusetzen, die keinen Lese- bzw. Schreibzugriff von Zwischenspeicher 2 auf Zwischenspeicher 1 erlaubt.

Es ist zu beachten, dass sich die zwischengespeicherten Datensätze stets auf einem im Sinne des Datenschutzes sicheren Medium befinden. Auf schriftliche Mitteilung der jeweiligen Datenempfänger können die Daten auf dem Zwischenspeicher 2 mit einem Löschkennzeichen versehen oder gelöscht werden.

3.8 Pseudonymisierung der Datensätze

Bei der Übernahme der Daten in den Zwischenspeicher 2 ist der Versichertenbezug zu pseudonymisieren. Alle Versichertenstammdaten mit Ausnahme des Geburtsjahres (also Vorname, Nachname, Geburtstag und Geburtsmonat) werden gelöscht. Die Datenstelle stellt in diesem Zusammenhang sicher, dass die Zuordnung Krankenversichertennummer zum Pseudonym eindeutig ist und ein Pseudonym nicht unterschiedlichen Versicherten zugeordnet wird.

Zur Pseudonymisierung ist das von den Kassenorganisationen auf Bundesebene entwickelte Pseudonymisierungsverfahren anzuwenden. Dieses sieht insbesondere vor, dass

- die Krankenversichertennummer bis zu 12 Stellen umfassen kann;
- das zu erzeugende Pseudonym genau 21 Stellen umfasst, sich aus der 9-stelligen unverschlüsselten Kostenträgerkennung und einem 12-stelligen Chiffre (pseudonymisierte Krankenversichertennummer) zusammensetzt;
- das Pseudonym ausschließlich Ziffern enthalten darf und
- die Pseudonymisierung der Krankenversichertennummer mittels Zufallszahl erfolgt.

Die Datenstelle stellt durch geeignete Zuordnungstabellen sicher, dass eine Krankenversichertennummer ausschließlich einmal pseudonymisiert und einem Versicherten genau ein Pseudonym zugeordnet wird. Bei Änderungen der Kostenträgerkennung ohne Wechsel der Krankenkasse, bleibt das ursprünglich vergebene Pseudonym für den Versicherten erhalten.

3.9 Prüfung der Dokumentationen auf Vollständigkeit und Plausibilität

Alle erfassten Dokumentationen werden auf Vollständigkeit und Plausibilität geprüft. Die Prüfung erfolgt auf Basis der von den Kassenorganisationen auf Bundesebene erstellten Plausibilitätsrichtlinien in der jeweils beauftragten Fassung. Die jeweils beauftragten Richtlinien werden der Datenstelle von den Auftraggebern (Geschäftsstelle der Arbeitsgemeinschaft DMP) rechtzeitig zur Verfügung gestellt.

3.10 Nachforderung für unvollständige bzw. nicht plausible Dokumentationen

Für fristgerecht eingereichte unvollständige und/oder unplausible Dokumentationen bzw. TE/EWE fordert die Datenstelle die entsprechenden Daten beim koordinierenden Arzt an. Soweit es sich hierbei um einen Vertretungsarzt handelt, werden die Daten beim Vertretungsarzt angefordert.

Soweit der koordinierende Arzt Nachfragen hat, leistet die Datenstelle Unterstützung bei der Fehlerkorrektur. Die Datenstelle stellt sicher, dass eine persönlich besetzte Hotline in der Zeit von 8:00 Uhr bis 18:30 Uhr an Arbeitstagen erreichbar ist. Daneben stehen den koordinierenden Ärzten die Kontaktwege Fax und E-Mail zur Verfügung.

Korrekturen von Dokumentationen können über vier mögliche Verfahren erfolgen:

1. die beleghafte Korrektur des Datensatzes vom koordinierenden Arzt auf einem, von der Datenstelle zur Verfügung gestellten Ausdruck und dessen Rücksendung an die Datenstelle
2. die erneute Übermittlung der korrigierten Version des einzelnen unvollständigen und/oder unplausiblen Datensatzes vom koordinierenden Arzt an die Datenstelle
3. die Übermittlung der korrigierten Version des einzelnen unvollständigen und/oder unplausiblen Datensatzes mit einem entsprechenden Korrekturkennzeichen vom koordinierenden Arzt an die Datenstelle
4. die erneute Übermittlung der gesamten Datenlieferung, welche unvollständige und/oder unplausible Datensätze enthalten hatte, vom koordinierenden Arzt an die Datenstelle

Die Datenstelle fordert den koordinierenden Arzt innerhalb von 10 Werktagen nach Eingang eines unvollständigen und/oder unplausiblen Dokumentationsdatensatzes mittels eines von den Auftraggebern zur Verfügung gestellten Musterbriefes zur Korrektur auf. Dabei werden dem koordinierenden Arzt die vorliegenden Dokumentationsdaten auf einem Ausdruck als Korrekturbogen unter Angabe der Korrekturhinweise zur beleghaften Korrektur zur Verfügung gestellt.

Die Datenstelle fordert den koordinierenden Arzt ebenfalls zur Korrektur eines Dokumentationsdatensatzes auf, wenn dieser innerhalb des angegebenen Status des Versicherten das Kennzeichen für Asylbewerber aufweist.

An ausstehende Korrekturen des koordinierenden Arztes wird bis zum Ablauf der Frist aller 10 Werktage mittels eines von den Auftraggebern zur Verfügung gestellten Musterbriefes erinnert. Auf Anforderung des koordinierenden Arztes ist die Versendung des Bogens zur beleghaften Korrektur von der Datenstelle zu wiederholen.

Die Verarbeitung der eingegangenen Korrekturbögen erfolgt grundsätzlich analog der Verarbeitung von Originaldokumenten (Entgegennahme, Posteingangskennzeichnung, Prüfung auf Vollständigkeit und Plausibilität, Scannen, Archivierung) durch die Datenstelle. Bei Eingang der beleghaften Korrektur wird insbesondere geprüft, ob der Bogen mit Korrekturdatum des koordinierenden Arztes versehen worden ist. Bei Nichtvorhandensein wird ersatzweise das Posteingangsdatum bei der Datenstelle als Korrekturdatum in die Datenbank übernommen. Soweit für den Versicherten vom koordinierenden Arzt eine plausible Dokumentation (ggf. auch mit einem anderen Erstellungsdatum innerhalb desselben Dokumentationszeitraumes) eingeht, ist das Korrekturverfahren für die unvollständige/unplausible Dokumentation zu beenden.

Übermittelt der koordinierende Arzt eine elektronische Dokumentation unter Angabe des Korrekturkennzeichens, wird die Korrektur der Originaldokumentation zugeordnet und die Dokumentationsparameter der Originaldokumentation entsprechend aktualisiert, sofern die Originaldokumentation bisher nicht vollständig und plausibel ist. Anderenfalls erfolgt keine Weiterverarbeitung einer elektronischen Dokumentation mit Korrekturkennzeichen durch die Datenstelle.

Übermittelt der koordinierende Arzt eine elektronische Dokumentation unter Angabe des Korrekturkennzeichens und liegt keine zuordenbare Originaldokumentation vor, wird die Dokumentation ohne Beachtung des Korrekturkennzeichens durch die Datenstelle weiterverarbeitet.

Sofern der koordinierende Arzt eine elektronische Dokumentation unter Angabe eines Korrekturkennzeichens übermitteln möchte, obwohl der Datenstelle bereits eine zuordenbare Originaldokumentation im plausiblen Status vorliegt, muss der koordinierende Arzt vor Übermittlung der Dokumentation die Datenstelle über die beabsichtigte Korrekturlieferung telefonisch informieren. Anderenfalls erfolgt keine Aktualisierung der Dokumentationsparameter durch die Datenstelle. Übermittelt der koordinierende Arzt trotz Ankündigung keine weitere plausible Dokumentation bis zum Ende der Frist (vgl. Punkt 3.5), wird die zuerst übermittelte plausible Dokumentation für die weitere Verarbeitung berücksichtigt.

Für unvollständige und/oder unplausible TE/EWE führt die Datenstelle das beleghafte Korrekturverfahren mit dem koordinierenden Arzt bis zu acht Mal wie beschrieben durch. Als Korrekturbogen kommt hierbei allerdings ein Imageausdruck der eingereichten TE/EWE zur Anwendung.

3.11 Weiterleitung der Dokumentationen

Die Dokumentationsdaten werden gemäß Beschreibung im Punkt 5 an die DMP-Datenzentren der Krankenkassen, die KVH und die Gemeinsamen Einrichtung weitergeleitet.

4 Fallführung und Rückmeldeverfahren

Nachfolgend werden die Aufgaben der Datenstelle im Zusammenhang mit der Generierung und Pflege eines DMP-Falles für den Versicherten einer Krankenkasse sowie die Umsetzung des Rückmeldeverfahrens beschrieben.

4.1 Zweckgebundenheit des DMP-Falles

Der gebildete DMP-Fall dient primär als Basis für die Nachvollziehbarkeit von Dokumentationsverläufen im Zusammenhang mit der Bereitstellung der Datensätze zur Evaluation sowie dem Heraussuchen und der Bereitstellung der zur Durchführung der Prüfung nach § 20 Abs. 4 RSAV relevanten Unterlagen. Gleichzeitig soll durch den DMP-Fall und das Rückmeldeverfahren ein valides Reminding ermöglicht werden.

4.2 Generierung und Pflege des DMP-Falles

Ausgehend von jeder Erstdokumentation für einen Versicherten und teilnehmender Krankenkasse je DMP bildet die Datenstelle einen DMP-Fall. Diesem DMP-Fall werden alle nachfolgenden Folgedokumentationen für das gleiche DMP zugeordnet. Die Datenstelle unterstellt dabei, dass für jeden so gebildeten Fallverlauf bei der jeweiligen Krankenkasse eine Einschreibung vorliegt. Der Fallverlauf wird von der Datenstelle beendet, wenn die Krankenkasse die Datenstelle über eine vorgenommene Ausschreibung informiert (vgl. Punkt 4.4.2).

Zudem hat die Datenstelle sicherzustellen, dass eine im selben Dokumentationszeitraum erstellte Folgedokumentation ebenfalls verarbeitet wird.

Ein Fallverlauf bestimmt sich grundsätzlich nach der LANR in Kombination mit der BSNR. Abweichend hiervon bestimmt sich der DMP-Fall bis zum Eingang der nächsten Dokumentation wenn

- der dokumentierende Arzt das Kennzeichen“ Dokumentation in Vertretung“ gesetzt hat; in diesem Fall wird keine Änderung am DMP-Fallverlauf vorgenommen; oder
- die Krankenkasse einen abweichenden DMP-Fallverlauf gemeldet hat.

Gehen bei der Datenstelle für einen Versicherten für dasselbe DMP im Fallverlauf vom selben koordinierenden Arzt bzw. von derselben Betriebsstätte (gleichfalls nach Arztwechsel mittels Folgedokumentation vom aktuell koordinierenden Arzt bzw. dessen Betriebsstätte) Erstdokumentationen ein, werden diese nur weiterverarbeitet und dem DMP-Fall zugeordnet, wenn zuvor zwei Folgedokumentationen gefehlt haben (vgl. Punkt 4.4.3) oder eine Ausschreibungsmitteilung der Krankenkasse vorgelegen hat. In allen anderen Fällen werden die Erstdokumentationen im laufenden DMP-Fall von der Datenstelle nicht weiterverarbeitet, jedoch gespeichert. Die Krankenkasse hat im Einzelfall die Möglichkeit, eine betreffende Erstdokumentation zu reaktivieren (mit allen Folgeprozessen). Die koordinierenden Ärzte werden über die nicht weiter verarbeiteten Erstdokumentationen informiert.

Bei der Diagnose Brustkrebs besteht die Besonderheit, dass nach einer präoperativen Erstdokumentation eine ergänzende postoperative Erstdokumentation in einem DMP-Fall vom gleichen oder von einem anderen koordinierenden Arzt erstellt werden kann. Die Datenstelle hat diese postoperative Erstdokumentation ebenfalls zu verarbeiten und dem gebildeten DMP-Fall zuzuordnen. Für den weiteren Fallverlauf ist eine postoperative Erstdokumentation nicht von Bedeutung, wenn bereits eine präoperative Erstdokumentation vorliegt. Sie kann auch eine erforderliche Folgedokumentation nicht ersetzen.

Gehen für einen Dokumentationszeitraum vollständige und plausible Folgedokumentationen von mehreren Ärzten bzw. Betriebsstätten für das gleiche DMP für einen Versicherten ein, sind diese Dokumentationen alle zu verarbeiten und dem gebildeten DMP-Fall zuzuordnen.

4.3 Definition und Speicherung des DMP-Falles

Die Datenstelle gewährleistet, dass der gebildete DMP-Fall folgende Informationen umfasst:

- Angabe zur Diagnose;
- LANR der Erstdokumentation;
- BSNR der Erstdokumentation;
- ggf. Krankenhaus-IK der Erstdokumentation;
- Krankenversichertennummer (alphanumerisch);
- Name des Versicherten;
- Vorname des Versicherten;
- Geburtsdatum des Versicherten;
- Kostenträgerkennung von der elektronischen Gesundheitskarte;
- Haupt-Institutionskennzeichen (IK) der Krankenkasse, das die Datenstelle dem von den Auftraggebern übermittelten Kassenverzeichnis entnimmt;
- Versichertenpseudonym.

Die Datenstelle gewährleistet, dass Versicherte, die nicht über die Krankenversichertennummer eindeutig einem Fallverlauf zugeordnet werden können, über Name und Geburtsdatum identifiziert werden können.

Ebenso ist nicht auszuschließen, dass mehrere unterschiedliche Kostenträgerkennungen von ein und derselben Krankenkasse durch Leistungserbringer oder Krankenkassen übermittelt werden. Bestandteil des primären Ordnungsmerkmals ist deshalb das Haupt-Institutionskennzeichen der Krankenkasse.

Die Datenstelle gewährleistet, dass die Versicherteninformationen zu einem Versichertenpseudonym zusammengeführt werden können.

4.4 Meldungen der Krankenkassen

Die Datenstelle pflegt die DMP-Fälle unter dem Aspekt, dass die Krankenkassen ihre Änderungen zum DMP-Fall über die abgestimmten Verfahren melden.

Die Meldungen werden fall- oder dokumentationsbezogen übermittelt. Die Datenstelle verarbeitet die Meldungen der Krankenkassen innerhalb von 5 Arbeitstagen.

4.4.1 Meldung der Krankenkasse bei einem Wechsel der Kostenträgerkennung

Sachverhalt

Die Krankenkasse stellt fest, dass sich die Kostenträgerkennung für aktuelle bzw. ehemalige DMP-Teilnehmer geändert hat.

Meldung der Krankenkasse

Die Meldung der Krankenkasse besteht aus folgenden Inhalten:

- Datenstellen-Institutionskennzeichen
- KV-Bereich
- Kostenträgerkennung alt
- Kostenträgerkennung neu
- Kostenträgerkennung neu gültig ab

Maßnahme der Datenstelle

Die Datenstelle übernimmt die gemeldete neue Kostenträgerkennung in die Datenbank.

Die Datenstelle gewährleistet eine Verknüpfung des „alten“ und „neuen“ Versichertenstammdatensatzes, um u. a. für spätere Datenlieferungen zur Evaluation und Durchführung der Prüfungen nach § 20 Abs. 4 RSAV komplette Dokumentationsverläufe bereitstellen zu können.

4.4.2 Meldung der Krankenkasse bei Beendigung, Stornierung oder Reaktivierung von DMP-Einschreibungen

Die Krankenkassen informieren die Datenstelle regelmäßig über fall- oder dokumentationsbezogene Änderungen. Diese umfassen folgende Meldungen:

- Beendigung der DMP-Teilnahme (Kündigung der DMP-Teilnahme, Tod, 2 fehlende Folgedokumentationen etc.),
- Stornierung der DMP-Teilnahme,
- Reaktivierung von bereits als beendet bzw. storniert gemeldeten DMP-Teilnahmen,
- Stornierung einer Dokumentation (keine Zuordnung zu einem Versicherten bei der Krankenkasse möglich, Löschung im Bestand der Krankenkasse)

Soweit die Krankenkasse das Ende oder die Stornierung einer DMP-Teilnahme meldet, beendet die Datenstelle in diesen Fällen ihren DMP-Fall sowie alle noch laufenden Reminder- und Korrekturprozesse für diese Einschreibung.

Bei Meldung einer Reaktivierung wird der beendete DMP-Fall bei der Datenstelle wieder aktiviert und ggf. noch nicht abgeschlossene Korrekturprozesse bis zum Ablauf der Frist (vgl. Punkt 3.5) wieder aufgenommen.

4.4.3 Beendigung von DMP-Fallverläufen durch die Datenstelle

Soweit Krankenkassen Fallbeendigungen nicht zeitnah der Datenstelle melden, sind die Fallverläufe von der Datenstelle ohne entsprechende Rückmeldung der Krankenkasse für Reminderaktivitäten nicht mehr zu berücksichtigen, wenn für 2 Dokumentationszeiträume in Folge der Datenstelle keine Folgedokumentation für einen Versicherten vorliegt. Hierzu führt die Datenstelle folgende Prüfung durch:

- Ausgehend von der letzten vorliegenden Dokumentation werden die nächsten beiden Dokumentationszeiträume ermittelt.
- Liegt nach Ablauf der Frist (vgl. Punkt 3.5) für den zweiten Dokumentationszeitraum keine Folgedokumentation für einen der beiden Dokumentationszeiträume vor, ist der Fallverlauf für Reminderaktivitäten durch die Datenstelle nicht mehr zu berücksichtigen.

Bei der Diagnose Brustkrebs hat eine Fallbeendigung durch die Datenstelle nur bei Vorlage einer Ausschreibungsmitteilung der Krankenkasse zu erfolgen.

5 Weiterleitung der Daten

5.1 Weiterleitung der Daten an die Krankenkasse

Eingehende Dokumentationen sind innerhalb von 8 Arbeitstagen abschließend zu bearbeiten. Vollständige, plausible und fristgerechte Dokumentationen sind für die Datenübermittlung an die DMP-Datenzentren der Krankenkassen bereitzustellen. Die zur Übermittlung bereitgestellten Datensätze sind wöchentlich, nach Wahl der Auftraggeber auch in kürzeren Abständen, den DMP-Datenzentren der Krankenkassen zu übermitteln. Die Datensätze werden hierzu in Dateien zusammengefasst und verschlüsselt übertragen. Soweit von einzelnen Krankenkassen erwünscht, sind ihre datenannehmenden Stellen auch mit

unplausiblen Datensätzen zu beliefern. Die Vereinbarung über die Lieferung von unplausiblen Daten wird bilateral zwischen den Auftraggebern und der Datenstelle getroffen.

Die Übermittlung der Datensätze an Krankenkassen muss nach Wahl des jeweiligen Auftraggebers im EDIFACT-, CSV- oder einem anderen, bilateral zwischen den Krankenkassen und der Datenstelle vereinbarten, Format erfolgen. Die Krankenkassen/-verbände geben der Datenstelle die Datensatzbeschreibungen ihrer Mitgliedskassen rechtzeitig bekannt.

Treten bei der Übermittlung der von der Datenstelle generierten Dateien technische Fehler auf, müssen alle von dem Fehler betroffenen Datensätze nach Überprüfung und eventueller Fehlerkorrektur von der Datenstelle erneut an die jeweilige datenannahmende Stelle übermittelt werden.

Im Falle einer Änderung eines Versichertenpseudonyms sind die Dokumentationsdaten nicht erneut an die Datenannahmestelle der Krankenkasse zu übermitteln.

5.2 CSV-Satzformat der TE/EWE

5.2.1 Filterung nicht aktiver Diagnosen im CSV-Satzformat

Die Empfängerstellen des TE/EWE-CSV-Formates haben sich darauf verständigt, künftig auf die Übermittlung nicht aktiver Diagnoseangaben auf multimorbid ausgestellten übergreifenden TE/EWE zu verzichten. Das bedeutet, ab dem 01.10.2025 sollen in der TE/EWE Exportschnittstelle nicht aktive Diagnosen herausgefiltert werden. Dies gilt für alle plausiblen Teilnahmeerklärungen, auf denen mindestens eine gültige Diagnose angekreuzt wurde.

5.2.2 Übertragung des Korrekturdatums im CSV-TE/EWE-Format

Das Datum einer Korrektur in einer TE/EWE wird im CSV-Satzformat übermittelt. Hierzu wird kein neues Feld eingeführt, sondern das bestehende Feld „Arztunterschrift“ im CSV-Format genutzt. Das bedeutet, ab dem 01.10.2025 soll in der TE/EWE Exportschnittstelle im Feld „Arztunterschrift“ das Korrekturdatum des Belegs übermittelt werden, sofern dieses vom Arzt explizit als zusätzliches Datum auf dem Formular eingetragen wurde. Ein Ersatz durch das Datum des Posteingangs der Korrektur ist nicht vorgesehen.

5.3 Weiterleitung der Daten an die Gemeinsame Einrichtung bzw. KVH

Die von der Datenstelle angenommenen und im Zwischenspeicher 2 gespeicherten Dokumentationsdaten (vgl. Punkt 3.7) werden an die Gemeinsame Einrichtung und die KVH übermittelt. Die Datensätze werden in Dateien zusammengefasst, verschlüsselt und elektronisch übermittelt. Der KVH und der Gemeinsamen Einrichtung werden ausschließlich plausible und vollständige Datensätze übermittelt.

Treten bei der Übermittlung der von der Datenstelle generierten Dateien technische Fehler auf, müssen alle von dem Fehler betroffenen Datensätze nach Überprüfung und eventueller Fehlerkorrektur von der Datenstelle erneut an die jeweilige datenannehmende Stelle übermittelt werden.

Im Falle der Änderung eines Versichertenpseudonyms sind die Dokumentationsdaten erneut an die Gemeinsame Einrichtung zu übermitteln.

5.3.1 Erstellen des Arzt-Reminders

Die Datenstelle erstellt einmal im Quartal im Auftrag der jeweiligen Gemeinsamen Einrichtung für jeden am DMP teilnehmenden Arzt einen Reminderbrief, in dem dieser über die Dokumentationen, die in diesem Quartal eingehen müssen, informiert wird.

Nach seiner Erstellung wird der Arzt-Reminder an den entsprechenden Arzt verschickt. Der jeweiligen Gemeinsamen Einrichtung wird quartalsbezogen eine arztbezogene Übersicht der versendeten Reminder zur Verfügung gestellt.

5.3.2 Datenweitergabe an den externen Evaluator

Die Datenstelle hat die Aufgabe, alle in der DMP-Datenbank gespeicherten und abgeschlossenen Datensätze an den von den Auftragsgebern bestimmten externen Evaluator zu übermitteln. Die Daten sind mit dem bestehenden Versicherten-Pseudonym sowie mit einem von der Datenstelle erzeugten Arzt-Pseudonym zu übermitteln.

Die Datenstelle hat die Aufgabe, für die Pseudonymisierung des Arztbezugs ein Pseudonymisierungsverfahren zu entwickeln. Das Verfahren muss sicherstellen, dass jeder Arzt immer mit demselben Pseudonym versehen wird. Das Verfahren ist gegenüber dem externen Evaluator offenzulegen, und erst nach ausdrücklicher Genehmigung durch diesen

anzuwenden, gegebenenfalls muss ein vom externen Evaluator vorgeschriebenes Verfahren angewandt werden.

Da die Krankenkassen dem Evaluator weitere Daten mit demselben Pseudonym übermitteln müssen, ist diesem das Pseudonymisierungsmodell von der Datenstelle gleichfalls zur Verfügung zu stellen.

Bei erstmaliger Fallübermittlung sind den Krankenkassen auf Anforderung zum Abgleich als Textdatei folgende Daten zeitnah zur Verfügung zu stellen: Diagnose, KV-Region, Kostenträgerkennung, Krankenversichertennummer; Versichertenpseudonym.

Einzelheiten zur Datenübermittlung (Zeitpunkt, Format usw.) werden zwischen den Kassenorganisationen auf Bundesebene oder von den von ihnen beauftragten Dritten und dem Evaluator abgestimmt. Die Datenstelle wird von den betreffenden Auftraggebern über die Anschrift des Evaluators sowie Einzelheiten zur Datenübermittlung gesondert informiert. Die Datenlieferung erfolgt entsprechend der jeweils beauftragten Datensatzbeschreibung.

5.4 Testdatenlieferungen

Bei Änderungen der Datenformate, neuen Diagnosen, Umstellung interner Prozesse der Auftraggeber oder der Datenstelle, die Auswirkungen auf die Datenlieferungen haben könnten, sendet die Datenstelle auf Anforderung der Auftraggeber Testdaten. Testdaten werden einvernehmlich mit den Auftraggebern vereinbart.

5.5 Besonderheiten BKK'n

Ein Vergütungsanspruch für die Leistungen im Zusammenhang mit der Datenverarbeitung für die teilnehmenden Krankenkassen besteht nur gegenüber der jeweiligen BKK, die gegenüber dem BKK-Landesverband NORDWEST ihren Beitritt erklärt hat.

Der BKK-Landesverband NORDWEST stellt regelmäßig der Datenstelle eine Liste der teilnehmenden Betriebskrankenkassen, welche diese Vereinbarung anerkannt haben, zur Verfügung mit der Information, an welche Adresse die TE/EWE, die Dokumentationsdaten sowie die Rechnungen übersandt werden müssen. BKK'n, die nicht die Zentrale Annahmestelle (ZAS) als datenannehmende Stelle nutzen, werden in dieser Liste besonders kenntlich gemacht und setzen sich mit der Datenstelle in Verbindung, um die entsprechenden Modalitäten der Datenflüsse abzuklären.

5.6 Besonderheiten IKK'n

Ein Vergütungsanspruch für die Leistungen im Zusammenhang mit der Datenverarbeitung für die teilnehmenden Krankenkassen besteht nur gegenüber der jeweiligen IKK, die gegenüber der IKK classic ihren Beitritt erklärt hat. Sofern die jeweilige IKK nicht mehr am Vertrag teilnehmen möchte, gelten für sie die Kündigungsfristen dieses Datenstellenvertrages. Die Kündigung erfolgt gegenüber der Datenstelle und der IKK classic.

Die IKK classic stellt regelmäßig der Datenstelle eine Liste der teilnehmenden Innungskrankenkassen, welche diese Vereinbarung anerkannt haben, zur Verfügung mit der Information, an welche Adresse die TE/EWE, Dokumentationen sowie die Rechnungen übersandt werden müssen.

Sofern nichts Abweichendes von der IKK classic mitgeteilt wurde, sind die Daten und TE/EWE sowie Rechnungen der außerhamburgischen Innungskrankenkassen direkt an die Clearingstelle bzw. zukünftig an die jeweilige IKK zu senden.

Sollten Innungskrankenkassen die IKK classic nicht zur Antragstellung auf Zulassung der strukturierten Behandlungsprogramme Asthma bronchiale, Brustkrebs, Chronic Obstructive Pulmonary Disease (COPD), Diabetes mellitus Typ 2, Diabetes mellitus Typ 1, Koronare Herzkrankheit und ggf. weiterer strukturierten Behandlungsprogramme bevollmächtigt haben oder den Antrag selbst stellen oder gegenüber der IKK classic keinen Beitritt zum Datenstellenvertrag erklärt haben, gilt abweichend, dass diese Kassen in der Liste besonders kenntlich gemacht werden und sich mit der Datenstelle in Verbindung setzen, um die entsprechenden Modalitäten der Datenflüsse abzuklären.

Rechnungsbegründende Anlagen sind tabellarisch im Excel-Format oder im CSV- bzw. TXT-Format zur tabellarischen Weiterverarbeitung in Excel/Access an die benannte Abrechnungsstelle der jeweiligen IKK zu liefern, sofern sie dies wünscht.

6 Leistungen bei Prüfungen gem. § 20 Abs. 4 RSAV

Nachfolgend werden die Aufgaben der Datenstelle zur Vorbereitung der Prüfung nach § 20 Abs. 4 RSAV beschrieben. Es gelten die jeweils aktuellen Vorgaben der Prüfbehörden des Bundes und/oder der Länder sowie die Beauftragung der Auftraggeber.

6.1 Anforderung der zur Durchführung der Prüfung nach § 20 Abs. 4 RSAV relevanten Unterlagen

Die Prüfdienste der Krankenversicherung informieren jede Krankenkasse separat und zu unterschiedlichen Zeitpunkten über die in das Prüfverfahren einzubeziehenden Versicherten anhand der Krankenversicherungsnummer und unter Angabe der zu prüfenden Jahre (Ausgleichsjahre).

Die Krankenkassen fordern die zur Durchführung der Prüfung nach § 20 Abs. 4 RSAV relevanten Unterlagen mit einer angemessenen Bearbeitungsfrist von mindestens 2 Wochen vor dem von den Krankenkassen bestimmten Liefertermin bei der Datenstelle in Form von Datensätzen an. Dazu wird das von den Kassenorganisationen auf Bundesebene vereinbarte Datenformat in der jeweils beauftragten Fassung verwendet.

6.2 Definition Umfang und Zeitraum der vorzulegenden Unterlagen

Das zu prüfende Ausgleichsjahr ergibt sich aus der Festlegung der Prüfdienste der Krankenversicherung. Für die Prüfung sind jeweils Unterlagen des zu prüfenden Ausgleichsjahres, des diesem vorangegangenen und des diesem nachfolgenden Kalenderjahres vorzulegen.

6.3 Definition der vorzulegenden Unterlagen

Sofern durch die Prüfdienste der Krankenversicherung nichts anderes bestimmt ist, sind folgende Unterlagen den Prüfdiensten der Krankenversicherung je in das Prüfverfahren einbezogenen Versicherten vorzulegen:

- Erstdokumentationen als visualisierte Dokumentationsdatensätze in Form von Images in vom jeweiligen Prüfdienst abgestimmten eigenentwickelten Formularen oder als mit dem XML-Reader der KBV erzeugten HTML-Dateien;
- Folgedokumentationen als visualisierte Dokumentationsdatensätze in Form von Images vom jeweiligen Prüfdienst abgestimmten in eigenentwickelten Formularen oder als mit dem XML-Reader der KBV erzeugten HTML-Dateien;
- sämtliche Korrekturbelege für alle einbezogenen Erstdokumentationen und Folgedokumentationen als Originale oder als Images mit einer qualifizierten elektronischen Signatur (Sollte im Einzelfall auf dem letzten Korrekturbeleg der gesamte Korrekturverlauf nachvollziehbar sein, ist dieser Korrekturbeleg ausreichend.). Darüber hinaus werden auch Images als Belege zu RSA-Prüfzwecken anerkannt, wenn sie revisionssicher in einem entsprechenden Archivierungsmedium gespeichert wurden und so die Anforderungen an die Authentizität und Integrität der gespeicherten Daten erfüllen.

Images werden auf einer CD-ROM oder per elektronischer Übermittlung (FTP-Server, membox, E-Mail) nach Vorgaben des jeweiligen Prüfdienstes grundsätzlich in schwarz-weiß bereitgestellt. Dabei ist darauf zu achten, dass die bildliche Wiedergabe mit den Originalunterlagen übereinstimmt. Images, bei denen die Felder des Vordruckes ausgeblendet sind, können nicht anerkannt werden. Der Dateiname des Images muss dem folgenden Standard entsprechen:

Kostenträgerkennung, Krankenversichertennummer, Ordnungsmerkmal bei der Datenstelle, Erstellungsdatum.

Die Prüfdienste der Krankenversicherung behalten sich vor, in Einzelfällen die Übereinstimmung mit den Originalen bzw. Originaldatensätzen zu prüfen. Für die Prüfdienste der Krankenversicherung ist eine Erklärung der Datenstelle zur Datenintegrität erforderlich.

6.4 Sortierfolge der Unterlagen

Die Datenstelle sortiert die zur Durchführung der Prüfung nach § 20 Abs. 4 RSAV bereitzustellenden relevanten Unterlagen je Fall nach

- der Kostenträgerkennung und
- innerhalb dieser Kostenträgerkennung nach der Krankenversichertennummer.

6.5 Versand der vorzulegenden Unterlagen

Die Datenstelle verpflichtet sich, den Versand der Prüfunterlagen unter Einhaltung der datenschutzrechtlichen Bestimmungen an den von den Krankenkassen genannten Adressaten (Prüfdienste der Krankenversicherung oder Krankenkasse) per Paketkurier und gegen Empfangsbekanntnis oder elektronisch vorzunehmen. Die Krankenkassen teilen der Datenstelle den Adressaten bei jeder Anforderung mit.

Die Vertragspartner gewährleisten in enger Abstimmung und Zusammenarbeit eine fristgerechte Lieferung der relevanten Prüfunterlagen an den zuständigen Prüfdienst der Krankenversicherung.

6.6 Verschlüsselung von Daten

Sofern die Datenstelle die zur Durchführung der Prüfung nach § 20 Abs. 4 RSAV relevanten Unterlagen in Form von Dateien auf einem Datenträger an den zuständigen Prüfdienst der Krankenversicherung versendet, ist die Datei als ZIP-Datei mit Kennwortschutz zu übermitteln.

6.7 Lieferschein

Die an die Prüfdienste der Krankenversicherung übermittelten Daten und Unterlagen sind von der Datenstelle durch einen Lieferschein zu dokumentieren. Der Lieferschein wird der anfordernden Krankenkasse zur Verfügung gestellt.

Der Lieferschein umfasst folgende Mindestangaben:

- KV-Bereich;
- Diagnose;

- Kostenträgerkennung;
- Krankenversichertennummer;
- Name des Versicherten;
- Vorname des Versicherten;
- Geburtsdatum des Versicherten;
- Belegart (Erst- oder Folgedokumentation);
- Datensatz-ID;
- Belegform (Image, Datensatz, Papieroriginal, Papierkopie);
- Image-Name;
- LANR/BSNR;
- Datum der Erstellung der Dokumentation;
- Doku-ID der Datenstelle.

6.8 Nachforderung von Prüfunterlagen

Sofern seitens eines Auftraggebers nachträglich ergänzende oder fehlende Prüfunterlagen nachgefordert werden, stellt die Datenstelle die Bereitstellung der Unterlagen innerhalb der seitens des Auftraggebers gesetzten Frist sicher.

7 Informationen an die Auftraggeber

Die Datenstelle erstellt für die Auftraggeber diverse Statistiken und Auswertungen, welche im Folgenden beschrieben sind.

Zu jeder versandten Statistik und Auswertung werden die jeweiligen Empfänger per E-Mail informiert. Dies gilt auch für Statistiken und Auswertungen, die von der Datenstelle online (vgl. Punkt 7.1) erstmalig zur Verfügung gestellt werden. Die genauen Erstellungs- und Versandtermine aller Statistiken und Auswertungen werden zwischen den Auftraggebern und der Datenstelle vereinbart.

7.1 Online-Recherche

Die Datenstelle stellt den Auftraggebern auf Anforderung die Möglichkeit zur Verfügung, über gesicherte Kommunikationsverbindungen zeitnah nach administrativen und steuerungsrelevanten Daten zu recherchieren.

Den einzelnen Auftraggebern stehen dabei jeweils nur ihre eigenen Daten zur Verfügung.

Diese Daten werden mindestens einmal wöchentlich aktualisiert und auf einem separaten EDV-System zur Verfügung gestellt. Dabei ist für einen Transfer der Daten das in der GKV eingesetzte Verschlüsselungsverfahren zu verwenden und für Onlineabfragen die Verbindung mittels Secure Socket Layer (SSL) zu verschlüsseln.

Erbringt die Datenstelle Leistungen hinsichtlich der Prüfung der TE/EWE einschließlich Korrekturverfahren (vgl. Punkt 2.4), sind die Images der TE/EWE aufzublenden. Darüber hinaus sind die Dokumentationen anzuzeigen. Versichertenbezogen wird eine Auflistung aller Dokumente mit Aussagen zu Plausibilität und Eingangsfristen sowie fehlender Dokumentationen je DMP ermöglicht.

7.2 Statusdatensatz

Die Datenstelle erstellt für alle Krankenkassen den Statusdatensatz. Aufbau und Versand richten sich nach dem zwischen den Kassenorganisationen auf Bundesebene abgestimmten Format. Die Datensätze werden den DMP-Datenzentren der jeweiligen Krankenkassen täglich zur Verfügung gestellt. Die Datenstelle wird von der Geschäftsstelle der Arbeitsgemeinschaft DMP über neue oder angepasste Schnittstellenbeschreibungen rechtzeitig informiert.

7.3 Verbandsstatistik

Die Datenstelle stellt über das Online-Retrieval-System (ORS) jedem Auftraggeber getrennt nach Diagnosen und Kassenart sowie krankenkassenspezifisch eine Statistik zur Verfügung, die folgende Angaben enthält:

- TE/EWE
- Erstdokumentationen
 - Gesamt
 - Datensatz plausibel und vollständig
 - verfristet
- Folgedokumentationen
 - Gesamt
 - Datensatz plausibel und vollständig
 - verfristet

Es wird immer ein kumulierter Gesamtstand je Kalenderjahr sowie die Veränderung gegenüber der Vorwoche für jede einzelne o. g. Position sowie für jede Diagnose und Dokumentationsart ausgewiesen.

7.4 Information an den koordinierenden Arzt

Der Arzt erhält Informationen über die von ihm in den letzten 14 Tagen eingereichten Dokumentationen, die wie folgt aufgebaut und alphabetisch nach Namen des Versicherten sortiert sind:

- a) Übersicht über vollständige und plausible Erst- und Folgedokumentationen
- b) Übersicht über verfristete Erst- und Folgedokumentationen
- c) Übersicht über nicht weiterverarbeitete Erstdokumentationen, die durch den in Punkt 4.2 beschriebenen Prozess bedingt sind.

Versandturnus/-Termin: 14-tägig

Mindestinhalt:

- (Diagnose des) DMP
- Name (des Versicherten)
- Vorname (des Versicherten)
- Krankenversichertennummer
- Krankenkasse
- DMP-Fallnummer
- Belegart
- Unterschriftsdatum Arzt / Erstellungsdatum / Datum Beleg

7.5 Abrechnungsstatistiken

7.5.1 Vergütungsdatei für die Kassenärztliche Vereinigung

Die Datenstelle erstellt, getrennt nach DMP, elektronisch einen arztbezogenen Nachweis der eingegangenen Dokumentationen gemäß Anlage 4.

Die Auswertungen sind spätestens 8 Wochen nach Ablauf des jeweiligen Quartals an die KVH zu übermitteln.

7.5.2 Rechnungsbegründende Unterlagen für die Krankenkassen

Die Datenstelle erstellt gegenüber den Krankenkassen monatliche Rechnungen für die erbrachten Leistungen; für diese Rechnungen sind rechnungsbegründende Unterlagen zu erstellen, aus denen die abgerechneten Mengen und Preise hervorgehen.

Die zahlungsbegründenden Unterlagen werden mittels Statusdatensatz zur Verfügung gestellt.

Anhang 2 zur Anlage 1 „Aufgabenbeschreibung“ zum Datenstellenvertrag vom 01.07.2008 i.d.F.d. 18. Nachtrags vom 01.10.2026

Übermittlung der elektronischen DMP-Dokumentationen (eDMP)

Folgende Verfahren zur Übermittlung der elektronischen DMP-Dokumentation stehen den DMP teilnehmenden Ärzten in Hamburg zur Verfügung:

- Kurzbeschreibung einzelner Arbeitsschritte beim eDMP-Datentransfer:

1. Portalübertragung: DMP Portal als Serverlösung über eine gesicherte SSL-Verbindung sowie über das Sichere Netz der KVen (SNK)/Telematikinfrastruktur (TI)

Voraussetzung:

Der teilnehmende DMP-Arzt beantragt die Zugangsdaten (Benutzername und Passwort) zum geschützten Online-Portal der KV Hamburg unter www.ekvvh.de (Webnet) oder <https://portal.kvvh.kv-safenet.de/eHealthPortal> (Safenet/TI). Sobald der KV Hamburg die angeforderten Daten vorliegen, werden die persönlichen Zugangsdaten per Post zugesendet. Nach Erhalt der unterschriebenen Empfangsbestätigung, wird der persönliche Online-Zugang zum geschützten Online-Portal der KV Hamburg freigeschaltet.

Verfahren:

Der teilnehmende DMP-Arzt meldet sich mit seinen persönlichen Zugangsdaten (Benutzername und Passwort) zum geschützten Online-Portal der KVH an. Der Datenaustausch zwischen ärztlichem PC und dem Webserver der KVH erfolgt ausschließlich verschlüsselt und ist somit abhörsicher.

Im geschützten Online-Portal der KV Hamburg gibt es die Möglichkeit, die verschlüsselten eDMP-Daten, die zuvor mit dem Praxisverwaltungssystem erstellt wurden, auf den KVH-Web-Server über die SSL-Verbindung oder über das Sichere Netz der KVen/Telmatikinfrastruktur (TI) zu übertragen.

Von diesen KV-Servern holt die Datenannahmestelle die übertragenen Daten einmal täglich zur internen Verarbeitung ab. Diese Datenverbindung ist ebenfalls verschlüsselt und erfolgt mittels zertifikatbasierter Authentifizierung.

Der Arzt erhält per Email eine Nachricht mit einer Referenznummer für die Datenübermittlung (Abholung und Bearbeitungsstand), unter der seine Daten in der Datenannahmestelle verarbeitet werden.

Die eDMP-Daten werden auf dem KV-Server eine Woche nach der Abholung durch die Datenstelle gelöscht. Auf den KV-Web-Server hat lediglich der verantwortliche Administrator Zugriff.

2. Übertragung der Dokumentationsdaten über KV-Connect (Integrierte Übertragung) bis zum 20.10.2025.
3. Übermittlung von eDMP-Daten über den Kommunikationsstandard KIM (Kommunikation im Medizinwesen) – Integrierte Übertragung ab dem 10.06.2025

Die verschlüsselten DMP-Dokumentationsdaten können aus dem Praxisverwaltungssystem auf direktem Weg über die Anwendung KIM innerhalb des Sicheren Netzes der KVen /Telematikinfrastruktur (TI) an die Datenstelle übertragen werden. Es gelten die Spezifikationen des KIM Anwendungsdienstes „eDMP“ in der jeweils aktuellen Fassung.

Anhang 3 eDMP: Kurzbeschreibung DMPOnline

Kurzbeschreibung DMPOnline

- Der koordinierende Arzt meldet sich mit Benutzernamen und Kennwort im geschützten Internetbereich der Datenstelle an (<https://inter-forum.de/DMPonline/>) an. Der Datenaustausch zwischen der Arztpraxis (PC) und dem Webserver der Datenstelle erfolgt ausschließlich verschlüsselt.
- Im geschützten Internetbereich der Datenstelle gibt es die Möglichkeit, die DMP-Daten in einer Erfassungsmaske einzugeben. Nach der erfolgreichen Plausibilisierung werden die eDMP-Daten dort automatisch verschlüsselt, signiert und in das Datenbanksystem der Datenstelle übernommen.
- Die eDMP-Daten werden auf dem Datenstellen-Server sofort nach der Übernahme in der DMP-Datenbank gelöscht. Lediglich die Stammdaten des Versicherten stehen für die mögliche Übernahme in weitere Folgedokumentationen zur Verfügung. Über eine Druckfunktion kann der Arzt die erstellte Dokumentation für den Patienten ausdrucken. Auf den Webserver hat lediglich der verantwortliche Administrator der Datenstelle Zugriff.

Bitte nach Möglichkeit an die Telefax-Nummer +49 341 25920-22 zurücksenden
(bei Versendung per Telefax ist eine Rücksendung per Post nicht notwendig)

IQVIA Health System Services GmbH
Abteilung DMP
Postfach 50 05 55
04305 Leipzig

Antrag zur Erfassung von DMP-Daten im Online-Verfahren
<https://DMPonline.inter-forum.de/>

Nachname:	Vorname:
Institution:	
Lebenslange Arztnummer:	
Betriebsstättennummer/Institutionskennzeichen:	
Anschrift:	
Telefon:	E-Mail-Adresse:

Hiermit beantrage ich den Zugang zur DMPonline-Datenerfassung auf dem Server der DMP-Datenstelle IQVIA Health System Services GmbH (nachfolgend DMP-Datenstelle genannt). Der Vertragsschluss erfolgt durch Übermittlung eines Zugangscodes durch die DMP-Datenstelle, der unter Beachtung der datenschutzrechtlichen Bestimmungen nur durch mich oder durch mich persönlich beauftragte Mitarbeiter eingesetzt wird.

Ist mir eine missbräuchliche Nutzung meiner Zugangsdaten bekannt geworden, melde ich dies unverzüglich der DMP-Datenstelle. Ich erkläre mich damit einverstanden, dass bei auftretenden Sicherheitsproblemen der Zugang durch die DMP-Datenstelle deaktiviert und das Vertragsverhältnis bezüglich der DMPonline-Datenerfassung von DMP-Daten ausgesetzt oder beendet werden kann.

Mir ist bekannt, dass es nach dem heutigen Stand der Technik nicht möglich ist, Computersoftware vollständig fehlerfrei zu erstellen.

Aus diesem Grund schließt die DMP-Datenstelle eine mögliche Haftung für Fehler aus der Erfassung und Plausibilitätsprüfung aus. Dies gilt auch für Datenverluste und Folgeschäden. Wartungsarbeiten können zu einer temporären Nichtverfügbarkeit der DMPonline-Datenerfassung führen.

Ich akzeptiere vorstehende Vertragsbedingungen uneingeschränkt.

Stand: 01.10.2026

Bitte nach Möglichkeit an die Telefax-Nummer +49 341 25920-22 zurücksenden
(bei Versendung per Telefax ist eine Rücksendung per Post nicht notwendig)

Datum

Unterschrift und Arztstempel

DMP-Kommunikationsmatrix im Rahmen des Datenmanagements

Information der Vertragsärzte, KVH und Krankenkassen

Nr.	Information	Details/ Besonderheiten	Frequenz/ Zeitpunkt	Empfänger Arzt	Empfänger KVH	Empfänger Krankenkassen
1	Korrekturverfahren: Rücksendung fehlerhafter Dokumentationen zur Korrektur	Bearbeitung der Korrekturen innerhalb von 8 Arbeitstagen nach Eingang	14-tägig	x		
2	Plausible und vollständige Belege: Plausible Dokumentationsbelege der letzten 14 Tage	tägliche Information der Krankenkassen mittels Statusdatensatz	14-tägig	x		x
3	Korrekturerinnerungen: Nicht plausible Dokumentationsbelege, die bereits zur Korrektur vorliegen		14-tägig	x		
4	Verfahrensbedingte Fehler: Nicht prozesskonforme Belege		14-tägig	x		
5	Komplementärbelege: Fehlende Erstdokumentationen		14-tägig	x		
6	Fehler im Dokumentationsverlauf: Außerhalb des Dokumentationszeitraums eingegangene Dokumentationen	tägliche Information der Krankenkassen mittels Statusdatensatz	14-tägig	x		x
7	Fehler im Dokumentationszeitraum: Folgedokumentationen im falschen zeitlichen Kontext	tägliche Information der Krankenkassen mittels Statusdatensatz	14-tägig	x		x
8	Folgedokumentationsreminder: Zu erstellende Folgedokumentationen im laufenden Quartal (Reminder)		quartalsweise (2. Monat im Quartal)	x		
9	Fehler bei übermittelten DMP-Datenlieferungen: nicht verarbeitbare Datenlieferungen		14-tägig	x		
10	Arztrecherche: Dokumentierender Arzt nicht auf Arztliste	Kumuliert bis Abbruch Information der Krankenkasse mittels Statusdatensatz	wöchentlich		x	x
11	Lieferung beleghafter TE/EWE im Original		zweimal wöchentlich			x
12	Export von Dokumentationsdaten		Übersicht Anlage 6			x
13	KVH-Abrechnung: Vorliegende Dokumentationen des Vorquartals, die vollständig und plausibel bzw. vertragskonform sind	Erstellung unter Berücksichtigung aller Belege eines Quartals	57 Tage nach Quartalsende		x	
14	KVH-Abrechnung: Verfristeter Eingang einer Dokumentation		57 Tage nach Quartalsende		x	
15	KVH-Abrechnung: Außerhalb des Dokumentationszeitraums erstellte Folgedokumentation		57 Tage nach Quartalsende		x	
16	ORS-Aktualisierung		wöchentlich		x	x

Anlage 4: Datensatzbeschreibung zur Vergütungsdatei

Im Rahmen der Quartalsaufstellungen werden der Kassenärztlichen Vereinigung Hamburg 8 Wochen nach Quartalsende des Abrechnungszeitraums übermittelt. Die Datenlieferung umfasst folgende Angaben:

Spaltenname	Erläuterung
Quartal	Abrechnungsquartal (nur aktuelles) YYYYQ
Empfänger	KV
Barcode	Datensatz-Identifikation
DMP Diagnose	Diagnosekürzel AB = Asthma bronchiale; BK = Brustkrebs COPD = Chronisch obstruktive Lungenerkrankungen; DM1 = Diabetes mellitus Typ1; DM2 = Diabetes mellitus Typ2; KHK = Koronare Herzkrankheit OST = Osteoporose RA = Rheumatoide Arthritis
Belegart	E = Erstdokumentation/ F =Folgedokumentation
PraxisNr	Betriebsstättennummer (BSNR)
ArztNr	lebenslange Arztnummer (LANR)
KH_IK	Institutionskennzeichen Krankenhaus
VersNr	Versichertennummer
VersVorname	Vorname Versicherter
VersNachname	Nachname Versicherter
GebDatum	Geburtsdatum Versicherter
IK	Institutionskennzeichen Krankenkasse
Eingang	Eingangsdatum
Datum_Orig	Datum der Erstellung
Datum_Unterschrift	Plausibilisierungsdatum
Belegstatus	1 = plausibel / 0 = fehlerhaft
Verfristet	1 = fristgerecht / 0 = verfristet
Dublette (echte ¹ , unechte ²)	1 = Original / 0 = Dublette
Erneute Erstdokumentation im laufenden DMP-Fall	1 = nein (E korrekt) / 0 = ja (E bereits vorhanden)
Folgedokumentation im beendeten Fall ³	1 = nein (F korrekt) / 0= ja (F im beendeten Fall)
„lose“ Folgedokumentation ⁴	1 = nein (F mit E) / 0 = ja (F ohne E)
Dokumentation ohne Zuordnung zu einem Versicherten bei der Krankenkasse	1 = nein (Zuordnung möglich) / 0 = ja (Zuordnung nicht möglich)
Dokumentation, die im Bestand der Krankenkasse gelöscht wurde	1 = nein (nicht gelöscht) / 0 = ja (gelöscht)
Dokumentation ohne TE/EWE ⁵	1 = nein (TE/EWE vorhanden) / 0 = ja (TE/EWE nicht vorhanden)

¹ Dokumentationen des gleichen Typs für eine Diagnose zu einem Versicherten vom selben Arzt mit identischem Erstellungsdatum (ohne oder mit Korrekturkennzeichen)

² Dokumentationen des gleichen Typs für eine Diagnose zu einem Versicherten vom selben Arzt im gleichen Dokumentationszeitraum mit abweichendem Erstellungsdatum (ohne oder mit Korrekturkennzeichen)

³ Folgedokumentationen, welche einem beendeten DMP-Fall zugeordnet werden; Beendigungsdatum muss vor dem Dokumentationszeitraum liegen, für welchen die Folgedokumentation erstellt wurde

⁴ Folgedokumentationen ohne vorherige Erstdokumentation

⁵ vorliegende Rückmeldung der Krankenkasse über Löschung einer Dokumentation im Bestand der Krankenkasse wegen fehlender TE/EWE oder fehlende TE/EWE bei der Datenstelle für AOK und KNAPPSCHAFT

Anlage 5

**Bestimmungen zum Datenschutz und zur Datensicherheit
bei der Datenverarbeitung im Auftrag
(Art. 28 DSGVO i. V. m. § 80 SGB X)**

– Datenschutzbestimmungen –

§ 1

Gegenstand der Datenschutzbestimmungen

- (1) Diese Datenschutzbestimmungen sind Bestandteil der vereinbarten Leistungen entsprechend des

Datenstellenvertrags zur Durchführung der Disease-Management-Programme in Hamburg

- im Folgenden Datenstellenvertrag genannt - und somit Grundlage für die Abwicklung der zwischen dem Verantwortlichen und dem Auftragsverarbeiter vertraglich vereinbarten Leistungen. Diese Datenschutzbestimmungen regeln den Schutz von Daten bei der Datenverarbeitung im Auftrag unter besonderer Berücksichtigung des Art. 28 DSGVO und des § 80 SGB X.

- (2) Der Auftragsverarbeiter verarbeitet zum Zwecke der Erbringung der nach dem Datenstellenvertrag geschuldeten Leistungen Sozialdaten, personenbezogene Daten und/oder Betriebs- und Geschäftsgeheimnisse (nachfolgend Daten genannt) im Auftrag des Verantwortlichen.

§ 2

Grundsätze

- (1) Geschäftsgrundlage des Rechtsverhältnisses zwischen Auftragsverarbeiter und Verantwortlichem ist, dass der Datenschutz beim Auftragsverarbeiter nach der Art der zu verarbeitenden Daten den Anforderungen genügt, die für den Verantwortlichen gelten. Der Verantwortliche verarbeitet in der Regel Daten einer hohen bis sehr hohen Schutzbedarfskategorie nach den Klassifikationen des Bundesamtes für Sicherheit in der Informationstechnik (BSI).
- (2) Der Verantwortliche, die für ihn zuständigen Aufsichtsbehörden oder von ihm beauftragte externe Prüfeinrichtungen sind berechtigt, sich vor Beginn der Auftragsverarbeitung und anschließend regelmäßig von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen zu überzeugen, vgl. § 9 (Kontrollrechte des Verantwortlichen).

§ 3

Konkretisierung des Auftragsinhalts

- (1) Art und Zweck der vorgesehenen Verarbeitung von Daten werden im Datenstellenvertrag, sowie vor allem in Anlage 1, konkret beschrieben.
- (2) Gegenstand der Datenverarbeitung sind Sozialdaten gemäß § 67 Abs.2 SGB X.
Die betroffenen personenbezogenen Daten sind in Anhang D definiert.

- (3) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
- Versicherte
 - Leistungserbringer (z.B. koordinierender Arzt)
 - Beschäftigte
- (4) Die zur Anzeige nach § 80 SGB X verpflichteten Körperschaften haben auch bezüglich der o. g. Punkte die Rechtmäßigkeit der Datenverarbeitung durch Auftragsverarbeiter zu prüfen.
- (5) Der Auftragsverarbeiter darf keine Verarbeitung von personenbezogenen Daten für eigene Zwecke vornehmen, sondern ausschließlich solche Datenverarbeitungsvorgänge durchführen, die ihm im Rahmen der jeweiligen Vereinbarung erlaubt werden. Der Auftraggeber ist auch nicht befugt die personenbezogenen Daten zu anonymisieren, um danach eine Verarbeitung für eigene oder andere Zwecke vorzunehmen.

§ 4

Allgemeine Pflichten des Auftragsverarbeiters

- (1) Dem Auftragsverarbeiter ist die Verarbeitung von Daten nur zum Zwecke der Erfüllung des Datenstellenvertrages sowie im Rahmen der schriftlichen Weisungen des Verantwortlichen und nach den datenschutzrechtlichen Vorschriften unter Beachtung der technischen und organisatorischen Maßnahmen gem. § 5 dieser Bestimmungen gestattet. Der Auftragsverarbeiter verwendet die Daten und die daraus erzielten Verarbeitungsergebnisse ausschließlich für die Erfüllung des Datenstellenvertrages. Er bewahrt die Daten unter Verschluss bzw. unter Einsatz entsprechender technischer Mittel vor unbefugtem Zugriff gesichert nur solange auf, wie es für die Erfüllung der genannten Leistungen erforderlich ist. Er gibt sie nicht an Dritte weiter.
- (2) Der Auftragsverarbeiter verpflichtet sich, dass die Daten des Verantwortlichen von Daten anderer Verantwortlicher streng getrennt werden. Er verpflichtet sich, keine Kopien oder Duplikate der Datenbestände bzw. Datenbanken ohne Wissen des Verantwortlichen zu erstellen oder die Daten für andere Zwecke zu nutzen. 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.
- (3) Der vom Auftragsverarbeiter bestellte Datenschutzbeauftragte (vgl. Art. 37 Abs. 4 DSGVO i.V.m. § 81 Abs. 4 SGB X) wird zum Zweck der direkten Kontaktaufnahme in Anhang C mit elektronischer Erreichbarkeit mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Verantwortlichen unverzüglich mitgeteilt. Zusätzlich benennt der Auftragnehmer einen internen Datenschutzmanager als zentrale operative Anlaufstelle für Datenschutzfragen. Dieser übernimmt insbesondere die Erstkoordination eingehender Anfragen und ist mit den im Sicherheitshandbuch (Kapitel 1.1) hinterlegten Kontaktdaten (Telefon, Fax, E-Mail) erreichbar.
- (4) Der Auftragsverarbeiter hat den für die Verarbeitung der Daten des Verantwortlichen im Rahmen des Auftragsverhältnisses vorgesehenen Standort/Standorte seiner Geschäftsräume dem Verantwortlichen vor Vertragsschluss in Anhang C schriftlich zu benennen. Eine Veränderung der Standorte oder Räumlichkeiten, in denen Daten des Verantwortlichen verarbeitet werden, oder ein Verlagern der Auftragsdurchführung an eine andere Örtlichkeit als die mit dem Verantwortlichen vereinbarte, bedarf der vorherigen schriftlichen oder elektronischen (Textform) Zustimmung des Verantwortlichen.
- (5) Der Auftragsverarbeiter stellt sicher, dass ein Zugriff auf die Daten des Verantwortlichen von Betriebsstätten/Geschäftsräumen und anderen Orten außerhalb der in Anhang C angegebenen Standorte des Auftragsverarbeiters grundsätzlich ausgeschlossen ist.

- (6) Sollte eine Verarbeitung von Daten des Verantwortlichen unter Nutzung mobiler Arbeitsplätze/Heim- oder Telearbeitsplätze stattfinden, ist sicherzustellen, dass dies unter Beachtung der technischen und organisatorischen Maßnahmen gemäß § 5 dieser Datenschutzbestimmungen erfolgt.
- (7) Der Auftrag zur Verarbeitung von Daten darf nur erteilt werden, wenn die Verarbeitung im Inland, in einem anderen Mitgliedstaat der Europäischen Union, in einem diesem nach § 35 Absatz 7 des Ersten Buches gleichgestellten Staat, oder, sofern ein Angemessenheitsbeschluss gemäß Artikel 45 der Verordnung (EU) 2016/679 vorliegt, in einem Drittstaat oder in einer internationalen Organisation erfolgt. Der Auftragsverarbeiter stellt sicher, dass – sowohl bei gegenwärtigen Verträgen als auch bei künftigen Verträgen – die tatsächliche Datenverarbeitung nach Maßgabe des § 80 Abs. 2 SGB X erfolgt und es zu keiner Datenverarbeitung außerhalb Deutschlands oder des EU-Raumes kommt, soweit für das Drittland kein Angemessenheitsbeschluss besteht.
- (8) Sofern wider Erwarten ein Zugriff auf Sozialdaten beim Auftragsverarbeiter durch Dritte, wie z. B. Behörden eines Drittstaates ohne Geltung der DSGVO oder eines Angemessenheitsbeschlusses, erfolgt, ist jeder Zugriff dem Auftraggeber unverzüglich mitzuteilen. Der Auftragsverarbeiter stellt sicher, dass kein Zugriff auf Sozialdaten durch Dritte, wie z. B. Behörden eines Drittstaates ohne Geltung der DSGVO oder eines Angemessenheitsbeschlusses (Beispiel: Zugriff von US-Behörden), erfolgt und dass die Daten, die Gegenstand der Geschäftsbeziehung zwischen dem Verantwortlichen und dem Auftragsverarbeiter sind, nicht an Dritte im vorbezeichneten Sinne herausgegeben werden. Dies wird insbesondere auch sichergestellt, wenn sich die Beteiligungsverhältnisse eines in Deutschland oder Europa ansässigen Auftragsverarbeiters in der Weise ändern, dass sich auf der Seite des Auftragsverarbeiters die Beteiligungsverhältnisse (unmittelbar oder mittelbar) ändern.
- (9) Der Auftragsverarbeiter ist verpflichtet, den Verantwortlichen zu informieren, wenn Aufsichtsbehörden nach § 40 BDSG tätig werden oder eine zuständige Behörde beim Auftragsverarbeiter oder seinen Unterauftragnehmern ermittelt. Die unverzügliche Information des Verantwortlichen über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens gemäß § 41 ff. BDSG in Bezug auf die Verarbeitung von Daten bei der Auftragsverarbeitung beim Auftragsverarbeiter ermittelt. Der Auftragsverarbeiter ist verpflichtet, den Verantwortlichen bei dessen nach Artikel 35 DSGVO entstehenden Pflichten bei der Erstellung einer Datenschutz-Folgenabschätzung zu unterstützen.
- (10) Sollte das Eigentum des Verantwortlichen beim Auftragsverarbeiter durch Maßnahmen Dritter (z.B. durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren) oder durch sonstige Ereignisse gefährdet werden, hat der Auftragsverarbeiter den Verantwortlichen unverzüglich darüber zu informieren. Der Auftragsverarbeiter ist verpflichtet alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber zu unterrichten, dass es sich um Daten des Verantwortlichen handelt, über die er keinerlei Verfügungs- oder sonstige Bestimmungsgewalt oder Eigentumsrechte hat.

§ 5

Technische und organisatorische Maßnahmen

- (1) Der Auftragsverarbeiter hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen oder Maßnahmen vergleichbarer Art und Güte vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung schriftlich oder in Textform zu dokumentieren und dem Verantwortlichen zur Prüfung zu übergeben (Anhang A). Bei Akzeptanz der Maßnahmen vergleichbarer Art und Güte durch den Verantwortlichen werden die

dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Verantwortlichen einen Anpassungsbedarf ergibt, ist dieser umzusetzen.

- (2) Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Hierzu ist die Umsetzung von individuell geeigneten technischen und organisatorischen Maßnahmen notwendig, die ein angemessenes Schutzniveau in Bezug auf tatsächliche oder mögliche Risiken gewährleisten. Die Risiken und daraus resultierenden Maßnahmen sind mindestens für die folgenden Schutzziele zu bewerten: Vertraulichkeit, Integrität, Verfügbarkeit sowie der Belastbarkeit der Systeme und Dienste. Bei der Bewertung sind insbesondere der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die jeweils unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.
- (3) Die technischen und organisatorischen Maßnahmen unterliegen immer dem technischen Fortschritt und der Weiterentwicklung und sind entsprechend dieser fortlaufend zu gewährleisten, Änderungen sind grundsätzlich 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. auf Anforderung des Verantwortlichen in deutscher Übersetzung in angemessener Zeit zur Verfügung gestellt werden.
- (5) Der Auftragsverarbeiter 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.

§ 6

Sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der vertraglichen Regelungen die Bestimmungen gemäß Artt. 28 bis 33 DSGVO sicherzustellen.

Insofern sind insbesondere folgende Anforderungen zu gewährleisten:

- a. Der Auftragsverarbeiter ist verpflichtet, zur Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2b, 29, 32 Abs. 4 DSGVO für die Erfüllung der vertraglich vereinbarten Leistungen nur Personen einzusetzen, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden sowie regelmäßig informiert und angewiesen werden (Datengeheimnis). Die vorgenannte Verpflichtung hat inhaltlich mindestens dem als Anhang B beigefügten Muster der Verpflichtungserklärung zur Wahrung der Vertraulichkeit zu entsprechen.
- b. Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Einsicht in Daten nehmen kann, darf diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass der Auftragsverarbeiter gesetzlich zur Verarbeitung verpflichtet ist.
- c. Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Dies gilt auch, soweit der Verantwortliche 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 Auftragsverarbeiter ausgesetzt ist.

§ 7

Unterauftragnehmer

- (1) Unterauftragnehmer jeglichen Grades, die für den Auftragsverarbeiter Daten des Verantwortlichen verarbeiten, dürfen vom Auftragsverarbeiter nur mit vorheriger, schriftlicher Zustimmung des Verantwortlichen eingeschaltet werden. Dies gilt auch für Konzerntöchter. In Anhang C sind die Unterauftragnehmer jeglichen Grades anzugeben. Für bereits bei Zuschlag benannte Unterauftragnehmer jeglichen Grades gilt die Zustimmung als erteilt.
- (2) Soweit im Fall der Beauftragung/Zuschlagserteilung ein oder mehrere Unterauftragnehmer jeglichen Grades Daten des Verantwortlichen verarbeiten, müssen sowohl der Auftragsverarbeiter als auch die Unterauftragnehmer jeglichen Grades angeben, welches Aufgabenfeld an welchem Unternehmensstandort ausgeführt werden sollen.
- (3) Die vertraglichen Vereinbarungen nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zwischen Auftragsverarbeiter und Unterauftragnehmer jeglichen Grades sind so zu gestalten, dass sie den Bestimmungen des Vertragsverhältnisses zwischen Verantwortlichem und Auftragsverarbeiter in vollem Umfang entsprechen. Dies gilt auch hinsichtlich der technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit sowie der Prüf- und Kontrollrechte.
- (4) Der Unterauftrag zur Verarbeitung von Daten darf nur erteilt werden, wenn die Verarbeitung im Inland, in einem anderen Mitgliedstaat der Europäischen Union, in einem diesem nach § 35 Absatz 7 des Ersten Buches gleichgestellten Staat, oder, sofern ein Angemessenheitsbeschluss gemäß Artikel 45 der Verordnung (EU) 2016/679 vorliegt, in einem Drittstaat oder in einer internationalen Organisation erfolgt. Der Auftragsverarbeiter stellt sicher, dass – sowohl bei gegenwärtigen Verträgen als auch bei künftigen Verträgen – die tatsächliche Datenverarbeitung nach Maßgabe des § 80 Abs. 2 SGB X erfolgt und es zu keiner Datenverarbeitung außerhalb Deutschlands oder des EU-Raumes kommt, soweit für das Drittland kein Angemessenheitsbeschluss besteht. Dies gilt ausdrücklich auch für alle Unterauftragnehmer jeglichen Grades.
- (5) Sofern wider Erwarten ein Zugriff auf Sozialdaten beim Unterauftragnehmer durch Dritte, wie z. B. Behörden eines Drittstaates ohne Geltung der DSGVO oder eines Angemessenheitsbeschlusses, erfolgt, ist jeder Zugriff dem Auftraggeber unverzüglich mitzuteilen. Der Unterauftragsverarbeiter stellt sicher, dass kein Zugriff auf Sozialdaten durch Dritte, wie z. B. Behörden eines Drittstaates ohne Geltung der DSGVO oder eines Angemessenheitsbeschlusses (Beispiel: Zugriff von US-Behörden), erfolgt und dass die Daten, die Gegenstand der Geschäftsbeziehung zwischen dem Auftragsverarbeiter und dem Unterauftragsverarbeiter sind, nicht an Dritte im vorbezeichneten Sinne herausgegeben werden. Dies wird insbesondere auch sichergestellt, wenn sich die Beteiligungsverhältnisse eines in Deutschland oder Europa ansässigen Unterauftragsverarbeiters in der Weise ändern, dass sich auf der Seite des Unterauftragsverarbeiters die Beteiligungsverhältnisse (unmittelbar oder mittelbar) ändern. Dies gilt ausdrücklich auch für alle Unterauftragnehmer jeglichen Grades.
- (6) Der Auftragsverarbeiter hat sich regelmäßig von der Einhaltung der bei den Unterauftragnehmern jeglichen Grades getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren, mindestens 6 Jahre aufzubewahren und auf Verlangen dem Verantwortlichen vorzulegen.
- (7) Der Auftragsverarbeiter hat im Vertrag mit den Unterauftragnehmern jeglichen Grades den Auftrag, den Arbeitsablauf und die an den jeweiligen Unterauftragnehmer zum Zwecke der auftragsgemäßen Verarbeitung oder Nutzung gelangenden Daten der Art

nach zu bezeichnen sowie die Betriebsstätten/ Geschäftsräume und Standorte in denen die Daten des Verantwortlichen verarbeitet werden, zu benennen.

- (8) Die vom Auftragsverarbeiter mit seinen Unterauftragnehmern geschlossenen Verträgen sowie die von diesen Unterauftragnehmern weitergehend geschlossenen Verträgen mit den Unterauftragnehmern jeglichen Grades bedürfen der Schriftform und sind dem Verantwortlichen auf Verlangen vorzulegen.
- (9) Das Verhalten des Unterauftragnehmers jeglichen Grades ist dem Auftragsverarbeiter wie eigenes Verhalten zuzurechnen. Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter nach Maßgabe des Art. 28 Abs. 4 DSGVO gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Unterauftragnehmers.
- (10) Sollen vom Auftragsverarbeiter während der Vertragslaufzeit andere als in Anhang C benannte Unterauftragnehmer jeglichen Grades beauftragt oder Standorte von Unterauftragnehmern jeglichen Grades verlegt/erweitert werden, sind dem Verantwortlichen rechtzeitig vor der geplanten Veränderung folgende Unterlagen zur Zustimmung vorzulegen:
 - a. Beschreibung der Arbeiten, die der Unterauftragnehmer ausführen soll
 - b. Bericht der letzten Prüfung
 - c. Kopie der geplanten vertraglichen datenschutzrelevanten Regelungen (einschließlich der technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit) mit dem Unterauftragnehmer.
- (11) Wenn andere Stellen die Prüfung oder Wartung von automatisierten Verfahren oder von Datenverarbeitungsanlagen vornehmen und dabei ein Zugriff auf die Daten des Verantwortlichen nicht ausgeschlossen werden kann, gilt der § 80 Abs. 5 SGB X analog. Derartige Beauftragungen sind dem Verantwortlichen rechtzeitig vor Vertragsabschluss mitzuteilen. Sind Störungen im Betriebsablauf zu erwarten oder bereits eingetreten und ist eine kurzfristige Beauftragung eines Unterauftragnehmers unabdingbar, ist der Vertrag unverzüglich nachzuholen. Bereits bei Zuschlag bestehende Vertragsbeziehungen sind in Anhang C aufzuführen.
- (12) Beauftragt der Auftragsverarbeiter für den Datentransport einen Transportunternehmer, so hat er vertraglich sicherzustellen und dem Verantwortlichen auf Verlangen nachzuweisen, dass der Transportunternehmer den Datenschutzbestimmungen Genüge tut. Werden Unterlagen des Verantwortlichen abgeholt, stattet der Auftragsverarbeiter den Transportunternehmer mit einem schriftlichen Berechtigungsausweis für die Entgegennahme der Unterlagen aus.

§ 8

Auskunft, Berichtigung, Einschränkung und Löschung von Daten

- (1) Der Auftragsverarbeiter ist verpflichtet, den Verantwortlichen im Rahmen seiner Pflichten gegenüber Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Information unverzüglich zur Verfügung zu stellen.
- (2) Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Verantwortlichen berichtigen, löschen oder deren Verarbeitung einschränken.
- (3) Wenn von Betroffenen die Rechte gemäß der Artt. 15 – 18 DSGVO i. V. m. §§ 81, 83 und 84 SGB X geltend gemacht werden, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten. Er stellt sicher, dass die Daten von Betroffenen bei Bedarf auf Anweisung des Verantwortlichen berichtigt, gelöscht oder gesperrt werden können.

- (4) Soweit vom Leistungsumfang umfasst sind die Betroffenenrechte nach dokumentierter Weisung des Verantwortlichen unmittelbar durch den Auftragsverarbeiter sicherzustellen. Hierzu gehört die Umsetzung des Löschkonzeptes, Berichtigung und Auskunft.

§ 9

Kontrollrechte des Verantwortlichen

- (1) Der Verantwortliche oder von ihm beauftragte externe Prüfeinrichtungen werden sich vor Beginn der Auftragsverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen überzeugen.
- (2) Der Auftragsverarbeiter gewährt dem Verantwortlichen bzw. den für den Verantwortlichen zuständigen Aufsichtsbehörden oder von ihm beauftragte externe Prüfeinrichtungen in den Betriebsräumen des Auftragsverarbeiters zu jeder geschäftsmäßigen Zeit nach vorheriger schriftlicher oder elektronischer (Textform) Ankündigung ein Prüfrecht. Das Prüfrecht umfasst die Besichtigung von Grundstücken und Geschäftsräumen, Auskünfte zur Vertragsausführung, Einsicht in Papierunterlagen als auch die Einsichtnahme in die beim Auftragsverarbeiter gespeicherten Daten des Verantwortlichen, 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.
- (3) Der Nachweis technischer und organisatorischer Maßnahmen kann erfolgen durch
- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
 - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
 - aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, Informationssicherheitsbeauftragter, Datenschutzauditoren, Qualitätsauditoren);
 - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI Grundschutz).
- (4) Der Auftragsverarbeiter sichert zu, dass er die notwendige personelle und sachliche Unterstützung bei den Prüfungen zur Verfügung stellt.
- (5) Die genannten Rechte des Verantwortlichen können auch durch Mitarbeiter von damit beauftragten Fremdfirmen wahrgenommen werden. Sofern Mitarbeiter von Fremdfirmen mit den genannten Kontrollmaßnahmen beauftragt werden, sind diese vom Verantwortlichen ausdrücklich auf die Geheimhaltung aller in diesem Zusammenhang erlangten Kenntnisse, Daten sowie Betriebs- und Geschäftsgeheimnisse zu verpflichten.
- (6) Die Rechte der für den Auftragsverarbeiter zuständigen Aufsichtsbehörde bleiben davon unberührt.

§ 10

Weisungsbefugnis des Verantwortlichen

Der Verantwortliche ist befugt, erforderlichenfalls schriftliche Weisungen im Rahmen der Artt. 28, 32 DSGVO zur Ergänzung der beim Auftragsverarbeiter vorhandenen technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit zu erteilen.

§ 11

Mitteilungspflichten des Auftragsverarbeiters

- (1) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Artt. 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Verzeichnis von Verarbeitungstätigkeiten, Meldepflichten bei Datenschutzverletzungen, gegebenenfalls erforderlichen 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 personenbezogener Daten - auch durch seine Mitarbeiter oder Unterauftragnehmer - gemäß Art. 33 Abs. 2 und 3 DSGVO unverzüglich an den Verantwortlichen zu melden. In diesem Falle hat der Auftragsverarbeiter sofort alle erforderlichen Maßnahmen zur Sicherung der Daten zu treffen und weitere Anweisungen durch den Verantwortlichen abzuwarten.
- (2) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Meinung ist, dass eine Weisung des Verantwortlichen gegen die DSGVO oder eine andere Datenschutzvorschrift verstößt. Der Auftragsverarbeiter ist in diesem Fall berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

§ 12

Löschung und Rückgabe von personenbezogenen Daten

- (1) Sämtliche Daten und Unterlagen sowie Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem in § 1 dieser Datenschutzbestimmungen genannten Zwecke in die Verfügungsgewalt des Auftragsverarbeiters gelangt sind, hat dieser entsprechend der jeweiligen Vereinbarungen im Einzelfall bzw. nach Abschluss der vertraglichen Arbeiten dem Verantwortlichen auf seine Kosten auszuhändigen bzw. zu übermitteln.
- (2) Auf Verlangen des Verantwortlichen hat der Auftragsverarbeiter in seinem Besitz befindliche Daten bzw. Datenbestände (z.B. physische Datenträger, elektronische Dateien oder Datenbanken in seinen DV-Systemen) nichtreproduzierbar auf seine Kosten zu löschen bzw. physisch zu vernichten. Die Vernichtung hat nach DIN 66399 Teile 1-3 mindestens mit Sicherheitsstufe P-4, F-4, O-4, T-4, H-4 bzw. E-4 zu erfolgen (Schutzklasse 3). Die Datenlöschung hat nach anerkanntem BSI-Standard 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 Verantwortlichen für jede weitere Verarbeitung einzuschränken.
- (3) Die Löschung und Vernichtung hat der Auftragsverarbeiter in geeigneter Weise zu protokollieren und auf Verlangen dem Verantwortlichen vorzulegen. Im Zweifelsfall sind geeignete Maßnahmen mit dem Verantwortlichen abzustimmen.
- (4) Endet das Vertragsverhältnis, hat der Auftragsverarbeiter gegenüber dem Verantwortlichen 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.

§ 13

Haftung

- (1) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen nach Maßgabe der gesetzlichen Bestimmungen für Schäden, die infolge seines oder seiner Unterauftragnehmer (§ 7) Verhaltens gegen Datenschutzbestimmungen und/oder durch die Verletzung dieses Vertrages entstehen. Etwaige vertragliche Haftungsbeschränkungen gelten nicht für Ansprüche, die dem Verantwortlichen gemäß Art. 82 Abs. 5 DSGVO gegen den Auftragsverarbeiter zustehen.
- (2) Der Auftragsverarbeiter bestätigt, sich gegen die Inanspruchnahme wegen Verletzung von Datenschutzvorschriften hinreichend versichert zu haben und diesen Versicherungsschutz für die gesamte Laufzeit des Datenstellenvertrages in vollem Umfang aufrechtzuerhalten. Auf Nachfrage des Verantwortlichen ist dies durch Vorlage geeigneter Dokumente nachzuweisen.

§ 14

Nebenabreden

Änderungen und Nebenabreden zu diesen Datenschutzbestimmungen bedürfen der Schriftform.

§ 15

Laufzeit des Vertrages und Kündigung

- (1) Beginn und Ende des Auftragsverhältnisses sind im Datenstellenvertrag geregelt. Unabhängig davon unterliegen der Auftragsverarbeiter und dessen eingesetzte Mitarbeiter auch nach dem im Datenstellenvertrag genannten Vertragsende hinaus hinsichtlich der im Rahmen des Auftragsverhältnisses übermittelten Daten und bekannt gewordenen Vertraulichkeiten der Geheimhaltungspflicht.
- (2) Die Verletzung von gesetzlichen oder vertraglichen Datenschutzbestimmungen durch den Auftragsverarbeiter ist ein wichtiger Grund für den Verantwortlichen, das im Datenstellenvertrag vorbehaltene Recht zur außerordentlichen Kündigung auszuüben.
- (3) Der Verantwortliche kann den Datenstellenvertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn
 - a. ein schwerwiegender Verstoß des Auftragsverarbeiters gegen Datenschutzvorschriften oder diese Datenschutzbestimmungen vorliegt (ein schwerwiegender Verstoß ist u.a. anzunehmen, wenn gegen die in § 4 Abs. 7, 8 bzw. § 5 Abs. 4, 5 bezeichneten Vorgaben verstoßen wird) oder
 - b. der Auftragsverarbeiter eine Weisung des Verantwortlichen nicht ausführen kann oder will oder
 - c. der Auftragsverarbeiter Kontrollrechte des Verantwortlichen vertragswidrig verweigert oder
 - d. die Grundlage der Vertragserfüllung aufgrund einer Änderung der Rechts- oder Gesetzeslage oder wegen aufsichtsrechtlicher Maßnahmen wesentlich verändert wird oder ganz entfällt.

§ 16

Salvatorische Klausel

- (1) Sollten einzelne Regelungen dieser Datenschutzbestimmungen ganz oder teilweise unwirksam sein oder werden oder sollten die Datenschutzbestimmungen eine Regelungslücke enthalten, bleibt die Wirksamkeit der übrigen Bestimmungen davon unberührt. Anstelle der unwirksamen oder fehlerhaften Bestimmungen treten die jeweiligen gesetzlichen Regelungen. Unwirksam gewordene Vereinbarungen werden die Vertragspartner durch wirksame Regelungen ersetzen, die dem ursprünglich verfolgten Zweck möglichst nahekommen. Diese sind bei nächster Gelegenheit als Ergänzung in diese Datenschutzbestimmungen aufzunehmen.
- (2) Sollten sich gesetzliche Änderungen während der Vertragslaufzeit ergeben, die zu einer Vertragsanpassung führen müssen, verpflichten sich die Vertragspartner Vertragsverhandlungen mit dem Ziel der Einigung aufzunehmen.

§ 17

Inkrafttreten

- (1) Diese Datenschutzbestimmungen treten mit Inkrafttreten des 19. Nachtrags zum Datenstellenvertrag in Kraft.
- (2) Es gilt die Gerichtsstandsvereinbarung des Datenstellenvertrages.

Anhänge:

Anhang A	Technische und organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit
Anhang B	Muster der Verpflichtungserklärung zur Wahrung der Vertraulichkeit
Anhang C	Sicherheitshandbuch incl. Unterauftragnehmer und Wartungsfirmen
Anhang D	Sozialdaten

Anhang A

Übersicht über die technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit

Dieser Anhang beschreibt die Anforderungen an die technischen und organisatorischen Maßnahmen, welche nach Art. 32 DSGVO für die Auftragsverarbeitung zu erfüllen sind.

Nachstehend sind die an den Auftragsverarbeiter gestellten Dokumentationspflichten aufgeführt, die entsprechend den Vergabeunterlagen, spätestens jedoch auf Nachforderung der Auftraggeberin einzureichen sind:

- Allgemeine Beschreibung der Maßnahmen zu den Gewährleistungszielen (siehe C1)
- Datenschutzkonzept*
- Informationssicherheitskonzept*
- Risikomanagementkonzept**
- Verarbeitungsverzeichnisse nach Art. 30 Abs.2 DSGVO
- Zertifizierung* (siehe C2)
- sonstige Nachweise zur Umsetzung nach Art. 32 DSGVO (siehe C3)
- Nachweis bei Nutzung/ Erbringung von Cloud-Dienstleistungen (siehe C4)

*nach BSI-Grundschutzkatalog oder ISO27001

**nach BSI-Standard 200-3 oder ISO27005/31000

Anhang A

C.1 Angaben zur allgemeinen Beschreibung der Maßnahmen zu den Datenschutzgewährleistungszielen

Es ist eine detaillierte und prüffähige Beschreibung der technischen und organisatorischen Maßnahmen gefordert, die auf die folgenden Punkte eingeht:

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)

- Zutrittskontrolle
kein unbefugter Zutritt zu Datenverarbeitungsanlagen,
z. B. Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pfortner, Alarmanlagen, Videoanlagen
- Zugangskontrolle
keine unbefugte Systembenutzung,
z. B. (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern
- Zugriffskontrolle
kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems,
z. B. Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen
- Trennungskontrolle
getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden,
z. B. Mandantenfähigkeit, Sandboxing
- Pseudonymisierung (Art. 32 Abs. 1 lit. a EU-DSGVO; Art. 25 Abs. 1 EU-DSGVO) Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

2. Integrität (Art. 32 Abs. 1 lit. b EU-DSGVO)

- Weitergabekontrolle
kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport,
z. B. Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur
- Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind,
z. B. Protokollierung, Dokumentenmanagement

Anhang A

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)

- Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust,
z. B. Backup-Strategie
- (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV),
Virenschutz, Firewall, Meldewege und Notfallpläne
- rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c EU-DSGVO).

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d EU-DSGVO; Art. 25 Abs. 1 EU-DSGVO)

- Datenschutz-Management
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 EU-DSGVO)
- Auftragskontrolle

Die Maßnahmen sind schriftlich in einem Sicherheitshandbuch oder einer
Sicherheitsrichtlinie

☒ festgelegt

☐ nicht schriftlich festgelegt

Bezeichnung: Sicherheitshandbuch

Stand: 07.09.2026

Anhang A**C.2 Angaben zur Zertifizierung im Kontext Informationssicherheit und Datenschutz**

Zertifizierungsstandard und -gegenstand:
ISO/IEC 27001:2022

Unternehmenseinheit/Standort	Geltungsbereich
IQVIA Health System Services GmbH Otto-Schmidt-Straße 22 04425 Taucha Deutschland	Genehmigungs-, Abrechnungs- und Daten- management im Gesundheitswesen Papiermanagement und Archivlogistik
IQVIA Health System Services GmbH Eythraer Weg 22 04249 Leipzig Deutschland	Papiermanagement und Archivlogistik
IQVIA Health System Services GmbH Sommerfelder Straße 120 04316 Leipzig Deutschland	Genehmigungs-, Abrechnungs- und Daten- management im Gesundheitswesen, Papier- management und Archivlogistik Zentral- und Servicefunktionen

Erteilung Erstzertifikat: 05.02.2018

Gültigkeit des aktuellen Zertifikats: 13.08.2024 bis 04.02.2027

Sind alle Standorte aus dem Sicherheitshandbuch - Geschäftsstandorte zertifiziert?

☐ ja

☒ nein - Welche nicht? Dortmund

Wird zum Datenschutz-Audit Einsicht in den Zertifizierungsbericht gewährt?

☒ ja

☐ nein

C.3 Angaben zu sonstigen Nachweisen nach Art. 32 EU-DSGVO

Dokumente/Zertifikate/DIN	Beschreibung
DIN EN ISO 22301:2020	Business Continuity Managementsystem
ISO 11799	Betrieb von Archiven für die Aufbewahrung von Dokumenten
ISO 9001	Qualitätsmanagementsystem

Anhang A

C.4 Bei Nutzung/Erbringung von Cloud-Dienstleistungen

Erfolgt die Datenverarbeitung im Inland, in einem Staat des EWR oder in einem Staat mit Angemessenheitsbeschluss gemäß Artikel 45 DSGVO und verfügt die datenverarbeitende Stelle über eine Niederlassung im Inland?

- ☐ ja, im Inland
- ☐ ja, innerhalb des EWR (mit Niederlassung im Inland)
- ☐ ja, Drittland mit Angemessenheitsbeschluss (mit Niederlassung im Inland)
- ☒ nein

Wird der Branchenspezifische Sicherheitsstandard für gesetzliche Kranken- und Pflegeversicherer (B3S-GKV/PV) erfüllt?

- ☒ ja
- ☐ nein

Liegt ein aktuelles C5--Testat oder ein gleichwertiger Nachweis vor und sind die im Prüfbericht enthaltenen, korrespondierenden Kriterien umgesetzt?

- ☐ ja, C5 Typ1-Testat (Gültigkeit bis 01.07.2025)
- ☐ ja, C5 Typ2-Testat
- ☐ ja, folgender Nachweis: [Klicken oder tippen Sie hier, um Text einzugeben.](#)
- ☒ nein

Wird Einsicht in den Zertifizierungs-/Prüfbericht gewährt?

- ☐ ja, vor Vertragsunterzeichnung
- ☐ ja, nach Vertragsunterzeichnung
- ☒ nein

Leipzig,
Ort, Datum

IQVIA Health System Services GmbH

Anhang B

Muster Verpflichtung zur Vertraulichkeit

Sehr geehrte Frau «Vorname» «Name»,

es ist sicher nicht in Ihrem Sinne, wenn Daten über Ihre Person und über Ihre persönlichen Verhältnisse Unbefugten zur Kenntnis gelangen. Deshalb genießen personenbezogene Daten besonderen gesetzlichen Schutz. Personenbezogene Daten sind nicht nur die Daten, die sich konkret einer bestimmten Person zuordnen lassen (wie z.B. Name, Kontaktdaten, Aufgabe im Unternehmen etc.), sondern auch die Daten, bei denen die Person erst über zusätzliche Informationen bestimmbar gemacht werden kann.

Wir gehen in unserem Unternehmen im Zweifel davon aus, dass ein Personenbezug einer Information vorliegt. Für personenbezogene Daten gelten dann die jeweils einschlägigen gesetzlichen Vorschriften zum Datenschutz wie z.B. die Datenschutz-Grundverordnung (DS-GVO) der Europäischen Union.

Nach der DS-GVO dürfen personenbezogene Daten nur dann verarbeitet werden, wenn es hierzu eine Rechtsgrundlage gibt oder der Betroffene eingewilligt hat. Die Daten dürfen grundsätzlich nur zu den vorgesehenen Zwecken verwendet werden. Bei der Verarbeitung der Daten ist insbesondere sicherzustellen, dass die Rechte der betroffenen Person auf Vertraulichkeit, Integrität und Verfügbarkeit ihrer personenbezogenen Daten gewährleistet werden.

Daher ist es Ihnen auch nur gestattet, personenbezogene Daten im Rahmen unserer internen Vorgaben zu verwenden und in dem Umfang und in der Weise zu verarbeiten, wie es zur Erfüllung der Ihnen übertragenen Aufgaben erforderlich ist. Die Daten sind Dritten gegenüber vertraulich zu behandeln.

Nach den geltenden Vorschriften ist es untersagt, personenbezogene Daten unbefugt oder unrechtmäßig zu verarbeiten oder absichtlich oder unabsichtlich die Sicherheit der Verarbeitung in einer Weise zu verletzen, die zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung oder unbefugtem Zugang führt.

Darüber hinaus sind aber auch Betriebs- und Geschäftsgeheimnisse in unserem Unternehmen schutzbedürftige Daten, die ebenfalls vertraulich zu behandeln sind. Eine Offenlegung von Betriebs- und Geschäftsgeheimnissen soll grundsätzlich nur dann erfolgen, wenn der jeweilige Vertrags- oder Geschäftspartner zuvor auf die Vertraulichkeit verpflichtet worden ist.

Verstöße gegen die Datenschutzvorschriften können ggf. mit Geldbuße, Geldstrafe oder Freiheitsstrafe geahndet werden. Entsteht der betroffenen Person durch die unzulässige Verarbeitung ihrer personenbezogenen Daten ein materieller oder immaterieller Schaden, kann ein Schadenersatzanspruch entstehen.

Ein Verstoß gegen die Vertraulichkeits- und Datenschutzvorschriften stellt einen Verstoß gegen arbeitsvertragliche Pflichten dar, der entsprechend geahndet werden kann.

Unser Unternehmen verarbeitet als Dienstleister Daten für verschiedene Träger der sozialen Sicherungssysteme (z.B. Krankenkassen) in deren Auftrag. Daher berührt Ihre Tätigkeit auch das Sozialgeheimnis. Sofern Daten verarbeitet werden, die dem Sozialgeheimnis unterliegen, haben Sie diese im gleichen Umfang geheim zu halten, wie die ursprünglich übermittelnde Stelle.

Bei Fragen oder in Zweifelsfällen können Sie sich jederzeit an Ihre Führungskraft oder den betrieblichen Datenschutzbeauftragten wenden.

Diese **Verpflichtung zur Vertraulichkeit** besteht auch nach der Beendigung des Beschäftigungsverhältnisses fort.

Etwaige andere Vertraulichkeitsvereinbarungen zwischen Ihnen und dem Unternehmen bleiben unberührt. Diese Vertraulichkeitsverpflichtung ersetzt jedoch eine ggf. erfolgte Verpflichtung zum Datengeheimnis nach dem BDSG a.F. mit Wirkung zum 25.05.2018.

Frau «Vorname» «Name», beschäftigt als «Bezeichnung»

erklärt, in Bezug auf die Vertraulichkeit und Integrität personenbezogener Daten die Vorgaben der geltenden gesetzlichen und internen Datenschutzvorschriften einzuhalten.

Mit Ihrer Unterschrift bestätigen Sie zugleich den Empfang einer Kopie dieser Niederschrift nebst Anlage.

Leipzig-Mölkau, den «Datum_Vertragerstellung» _____
Verpflichtete(r)

Verpflichtungserklärung für die Benutzung von Personal Computern

Frau «Vorname» «Name» wurde heute auf die Einhaltung der folgenden Datensicherheitsmaßnahmen bei der Benutzung eines Personal Computers verpflichtet und über mögliche Sanktionen bei Verstößen gegen diese Verpflichtung aufgrund interner oder gesetzlicher Vorschriften belehrt.

Der Mitarbeiter verpflichtet sich dazu,

- ausschließlich die vor- und freigegebene Hard- und Software einzusetzen (der Einsatz von privater Hard- und Software, unlizenzierter und nicht autorisiert selbsterstellter Programme ist verboten),
- unbefugten Personen den Zugang zum PC und den Zugriff auf Programme und Daten durch Einhaltung der vorgegebenen Sicherheitsmaßnahmen zu verwehren,
- den PC und die darauf gespeicherten Programme und Daten nur zur Erfüllung der vorgegebenen Aufgaben - und nicht missbräuchlich – zu verwenden,
- Programme und Daten nicht ohne Erlaubnis an Dritte weiterzugeben,
- nicht mehr benötigte Datenträger so zu vernichten, dass eine missbräuchliche Verwendung der Daten unmöglich ist,

Der Mitarbeiter wurde außerdem in Bezug auf die Vertraulichkeit und Integrität personenbezogener auf die Einhaltung der gesetzlichen und internen Datenschutzvorschriften verpflichtet, wonach es ihm untersagt ist, geschützte Sozialdaten und andere personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen.

Der Mitarbeiter wurde darauf hingewiesen, dass alle Mängel und Unregelmäßigkeiten hinsichtlich Datenschutz und Datensicherheit sowie der Ordnungsmäßigkeit entweder der zuständigen Führungskraft, der zentralen Kontaktstelle für die Meldung sicherheitsrelevanter Ereignisse oder dem Datenschutzbeauftragten unverzüglich mitzuteilen sind.

Verstöße gegen diese Verpflichtungserklärung können gegebenenfalls arbeits- und strafrechtlich verfolgt und geahndet werden. Sie können auch Anlass einer außerordentlichen Kündigung sein.

Diese Verpflichtung besteht über das Ende der Tätigkeit in unserem Unternehmen hinaus.

Leipzig-Mölkau, den «Datum_Vertragerstellung»

(Unterschrift Verpflichtete(r))

Die Europäische Datenschutz-Grundverordnung (DS-GVO) als unmittelbar geltendes Recht und das Bundesdatenschutzgesetz (BDSG) sind im Intranet zur Einsichtnahme veröffentlicht. Interne Vorschriften sind ebenfalls im Intranet veröffentlicht.

Anlage zur Verpflichtung auf die Vertraulichkeit (Stand: 14.01.2019)

Die vorliegende Auswahl gesetzlicher und interner Vorschriften soll Ihnen einen Überblick über das datenschutzrechtliche Regelwerk verschaffen. Die Darstellung erfolgt exemplarisch und ist keineswegs vollständig. Weitere Informationen zu datenschutzrechtlichen Fragestellungen erhalten Sie beim betrieblichen Datenschutzbeauftragten.

Begrifflichkeiten

Art. 4 Nr. 1 DS-GVO: „**Personenbezogene Daten**“ [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Art. 4 Nr. 2 DS-GVO: „**Verarbeitung**“ [meint] jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Grundsätze der Verarbeitung

Art. 5 Abs. 1 lit. a DS-GVO: Personenbezogene Daten müssen [...] auf **rechtmäßige Weise**, nach Treu und Glauben und in einer für die betroffene Person **nachvollziehbaren Weise** verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“).

Art. 5 Abs. 1 lit. f DS-GVO: Personenbezogene Daten müssen [...] in einer Weise verarbeitet werden, die eine angemessene **Sicherheit** der personenbezogenen Daten gewährleistet, einschließlich Schutz vor **unbefugter oder unrechtmäßiger Verarbeitung** und vor unbeabsichtigtem **Verlust**, unbeabsichtigter **Zerstörung** oder unbeabsichtigter **Schädigung** durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Art. 29 DS-GVO: Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten **ausschließlich auf Weisung** des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten zur Verarbeitung verpflichtet sind.

Art. 32 Abs. 2 DS-GVO: Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch **Vernichtung, Verlust** oder **Veränderung**, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte **Offenlegung** von beziehungsweise unbefugten **Zugang** zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

Art. 33 Abs. 1 Satz 1 DS-GVO: Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die **Verletzung** bekannt wurde, diese der [...] zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Haftung

Art. 82 Abs. 1 DS-GVO: Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf **Schadenersatz** gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Art. 83 Abs. 1 DS-GVO: Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von **Geldbußen** gemäß diesem Artikel für Verstöße gegen diese Verordnung [...] in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

§ 42 BDSG Strafvorschriften

- (1) Mit **Freiheitsstrafe** bis zu drei Jahren oder mit **Geldstrafe** wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,
1. einem Dritten übermittelt oder
 2. auf andere Art und Weise zugänglich macht und hierbei gewerbsmäßig handelt.
- (2) Mit **Freiheitsstrafe** bis zu zwei Jahren oder mit **Geldstrafe** wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,
1. ohne hierzu berechtigt zu sein, verarbeitet oder
 2. durch unrichtige Angaben erschleicht
- und hierbei gegen Entgelt oder in Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

§ 202a Abs. 1 StGB: Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit **Freiheitsstrafe** bis zu drei Jahren oder mit **Geldstrafe** bestraft.

§ 202b StGB: Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten [...] aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit **Freiheitsstrafe** bis zu zwei Jahren oder mit **Geldstrafe** bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202c Abs. 1 StGB: Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten [...] ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit **Freiheitsstrafe** bis zu einem Jahr oder mit **Geldstrafe** bestraft.

§ 303a Abs. 1 StGB: Wer rechtswidrig Daten [...] löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit **Freiheitsstrafe** bis zu zwei Jahren oder mit **Geldstrafe** bestraft.

Sozialgeheimnis

§ 78 Abs. 1 Satz 2 & 3 SGB X: [...] Eine Übermittlung von Sozialdaten an eine nicht-öffentliche Stelle ist nur zulässig, wenn diese sich verpflichtet hat, die Daten nur zu dem Zweck zu verarbeiten, zu dem sie ihr übermittelt werden. Die Dritten haben die Daten **in demselben Umfang geheim zu halten** wie die in § 35 [SGB I] genannten Stellen.

Berufsgeheimnis

§ 203 StGB Verletzung von Privatgeheimnissen

- (1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis offenbart, das ihm als
1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehöriger eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,
 2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,

3. Rechtsanwalt, Kammerrechtsbeistand, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,
4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,
5. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§3 und 8 des Schwangerschaftskonfliktgesetzes,
6. Staatlich anerkannten Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder
7. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. [...]

(4) Mit **Freiheitsstrafe** bis zu einem Jahr oder mit **Geldstrafe** wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als **mitwirkende Person** oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Beauftragter für den Datenschutz bekannt geworden ist. [...]

Verstöße gegen arbeitsvertragliche Pflichten

Verstöße gegen arbeitsvertragliche Pflichten können, je nach Schwere des Verstoßes, gemäß Organisationsanweisung 168 (Vorgehen bei Verstößen gegen bestehende Vorgaben) mit Ermahnung, Abmahnung, Kündigung des Arbeitsverhältnisses und/oder der Einleitung eines Strafverfahrens sanktioniert werden.

Sicherheitshandbuch

Angaben zu den getroffenen technischen und organisatorischen Maßnahmen
gemäß Art. 32 Abs. 1 DS-GVO

Stand: 07.09.2026

Vertraulichkeitsstufe: intern

Inhalt

1	Einleitung	3
1.1	Angaben zum Unternehmen.....	3
1.1.1	Allgemeine Angaben	3
1.1.2	Vertretungsberechtigte Personen	3
1.1.3	Angaben zum Datenschutzbeauftragten.....	3
1.1.4	Angaben zum Datenschutzmanager	3
1.1.5	Angaben zum Informationssicherheitsbeauftragten	4
1.2	Standorte der Datenverarbeitung	4
1.2.1	Leipzig-Mölkau	4
1.2.2	Taucha	4
1.2.3	Leipzig-Knautnaundorf	4
1.2.4	Dortmund	4
2	Gewährleistung der Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO).....	5
2.1	Zutrittskontrolle.....	5
2.2	Zugangskontrolle.....	6
2.3	Zugriffskontrolle.....	7
2.4	Trennungskontrolle/Zweckbindung.....	8
2.5	Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO).....	8
2.6	Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO).....	8
2.7	Personelle Sicherheit	9
2.7.1	Vor der Beschäftigung.....	9
2.7.2	Während der Beschäftigung	9
2.7.3	Beendigung oder Änderung der Anstellung	9
3	Integrität (Art. 32 Abs. 1 lit. b DS-GVO)	10
3.1	Eingabekontrolle	10
3.2	Weitergabekontrolle	10
3.3	Sicherung und Überprüfung der Authentizität	11
4	Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)	12
4.1	Risikomanagement und Cyber-Resilienz.....	12
4.2	Maßnahmen zur Sicherung der Stabilität des Anwendungssystems.....	12
4.3	Maßnahmen zur Ausfallsicherheit gegen Feuer und Wasser.....	14
4.4	Maßnahmen zur Ausfallsicherheit in Bezug auf Außenwirkungen	15
4.5	Maßnahmen gegen Vandalismus	16
4.6	Maßnahmen zum Schutz gegen Schadsoftware	16
4.7	Sicherung der Datenbestände.....	17
4.8	Vertretungsregelungen für abwesende Beschäftigte	17
4.9	Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem Zwischenfall (Art. 32 Abs. 1 lit. c DS-GVO)	17
5	Maßnahmen bei Einsatz von Videokonferenzsystemen	17
6	Telearbeit (IQVIA HSS@Home)	18
7	Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen Maßnahmen (Art. 32 Abs. 1 lit. d DS-GVO)	18
8	Anlagen.....	19

1 Einleitung

Dieses Sicherheitshandbuch enthält als Datensicherheitskonzept die bei IQVIA Health System Services, kurz IQVIA HSS, getroffenen technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO, die für alle Arten von Verarbeitungen personenbezogener Daten und an den einzelnen Standorten eingehalten werden.

Sollten aufgrund eines hohen Risikos für die Rechte und Freiheiten der betroffenen natürlichen Personen zusätzliche Maßnahmen für einzelne Verarbeitungstätigkeiten erforderlich werden, die sich aus wirtschaftlichen, technischen oder sonstigen Gründen nicht für alle Verarbeitungstätigkeiten umsetzen lassen oder für diese nicht erforderlich sind, so erfolgt die Dokumentation dieser besonderen Maßnahmen jeweils als Ergänzung im Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DS-GVO als Verantwortlicher oder aber in Abstimmung mit dem für die Verarbeitungstätigkeit Verantwortlichen im Verzeichnis nach Art. 30 Abs. 2 DS-GVO als Auftragsverarbeiter.

1.1 Angaben zum Unternehmen

1.1.1 Allgemeine Angaben

IQVIA Health System Services GmbH
Sommerfelder Straße 120
04316 Leipzig

Telefon: (+49) 341 25920-0
Fax: (+49) 341 25920-20
Website: <https://www.iqvيا.com/hss-germany>
Registergericht: Amtsgericht Leipzig
Registernummer: HRB 32082
USt-IdNr.: DE141624398

1.1.2 Vertretungsberechtigte Personen

Dr. Frank Wartenberg, Fabian Marx, Dr. Matthias Staritz

1.1.3 Angaben zum Datenschutzbeauftragten

Ronny Neid (ext. DSB)
DGI Deutsche Gesellschaft für Informationssicherheit AG
E-Mail: datenschutz@iqvia-hss.de

1.1.4 Angaben zum Datenschutzmanager

Tom Heuser
Tel.: (+49) 341 25920-7180
Fax: (+49) 341 25920-20
E-Mail: datenschutz@iqvia-hss.de

1.1.5 Angaben zum Informationssicherheitsbeauftragten

Tom Heuser

Tel.: (+49) 341 25920-7180

Fax: (+49) 341 25920-20

E-Mail: Informationssicherheit@iqvia-hss.de

1.2 Standorte der Datenverarbeitung

1.2.1 Leipzig-Mölkau

Anschrift:

Sommerfelder Straße 120, 04316 Leipzig

Funktion/Beschreibung:

- Zentrale Verwaltung
- Zentrale IT
- Postbearbeitung für die Auftragsverarbeitung
- Erfassung und Prüfung von Abrechnungen und Belegen im Rahmen der Auftragsverarbeitung
- Digitalisierung von Belegen und Abrechnungen im Rahmen der Auftragsverarbeitung
- Betrieb einer DMP-Datenstelle im Auftrag verschiedener DMP-Arbeitsgemeinschaften

1.2.2 Taucha

Anschrift:

Otto-Schmidt-Straße 22, 04425 Taucha

Funktion/Beschreibung:

- Postbearbeitung für die Auftragsverarbeitung
- Digitalisierung von Belegen und Abrechnungen im Rahmen der Auftragsverarbeitung
- Kurz- und Langzeitarchivierung von Belegen, Abrechnungen und Datenträgern im Rahmen der Auftragsverarbeitung
- Archivierung eigener Geschäftsunterlagen
- Prüfung von Abrechnungen und Belegen im Rahmen der Auftragsverarbeitung

1.2.3 Leipzig-Knautnaundorf

Anschrift:

Eythraer Weg 22, 04249 Leipzig

Funktion/Beschreibung:

- Langzeitarchivierung von Belegen in Papierform

1.2.4 Dortmund

Anschrift:

Hauert 8, 44227 Dortmund

Funktion/Beschreibung:

- Administration und Überwachung von Produktivsystemen per Fernzugriff

2 Gewährleistung der Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

2.1 Zutrittskontrolle

- Es sind vier Sicherheitszonen entsprechend den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) definiert und entsprechend den örtlichen Gegebenheiten eingerichtet (0-Außenbereich, 1-Kontrollierter Innenbereich, 2-Interner Bereich, 3-Hochsicherheitsbereich).
- Für alle Zutrittsstellen, die von einem großen Personenkreis genutzt werden müssen oder die zu einem Hochsicherheitsbereich gehören, ist ein DV-gestütztes Zutrittskontrollsystem zur Gewährleistung einer effektiven Zutrittskontrolle mit Protokollierung aller Zutritte und Zutrittsversuche im Einsatz.
- Zur Vereinfachung der Vergabe von Zutrittsberechtigungen erfolgt eine Zusammenfassung der erforderlichen Zutrittsrechte bestimmter Beschäftigtengruppen zu Zutrittsprofilen. Davon ausgenommen sind Berechtigungen für die Sicherheitszone 3 (Hochsicherheitsbereich).
- Der Zutritt zur Sicherheitszone 3 wird nur in begründeten Fällen mit Zustimmung des für den jeweiligen Sicherheitsbereich Verantwortlichen durch die Einzelzuweisung der Berechtigung gewährt.
- Die Zutrittsrechte sind auf das erforderliche Minimum nach dem Grundsatz „so viel wie nötig, so wenig wie möglich“ beschränkt.
- Wenig frequentierte Zutrittsstellen und Einzelbüros bis zur Sicherheitszone 2 werden durch mechanische Einzelschließungen (Sicherheitsschließzylinder) gesichert.
- Es wird ein Schlüsselverzeichnis mit geregelter Aus- und Rückgabe der Schlüssel gegen Quittung geführt.
- Nicht ausgegebene Schlüssel werden gesichert in einem Tresor aufbewahrt.
- Alle Beschäftigten sind zum sichtbaren Tragen der Zutritts-/Mitarbeiterkarte bereits ab Sicherheitszone 1 (kontrollierter Innenbereich) verpflichtet.
- Die Zutritts-/Mitarbeiterkarten sind zur optischen Kontrolle mit einem Passfoto und der Personalnummer ausgestattet. Sie enthalten keinerlei Hinweise zum Unternehmen, um die Möglichkeit einer missbräuchlichen Verwendung bei Verlust einzuschränken.
- Die Beschäftigten sind verpflichtet, den Verlust ihrer Zutritts-/Mitarbeiterkarte unverzüglich anzuzeigen. Die Karten werden dann sofort gesperrt.
- Fremdpersonen (Besucher, Gäste etc.) dürfen erst nach Anmeldung, Legitimation und Registrierung im Besucherbuch und nur in Begleitung und mit Besucherkarte die Räumlichkeiten betreten.
- An den Standorten Leipzig-Mölkau und Taucha übernimmt der Wachschutz auch den Empfangs- und Pfortnerdienst. Der Pfortner kontrolliert bzw. beobachtet die Personenbewegungen an der Pforte. Unbekannte Personen haben sich beim Pfortner auszuweisen. Der Pfortner nimmt Besucher sowie Post- und Lieferdienste in Empfang und informiert die Besuchten. Er erfasst Besucher in einem Besucherbuch und stellt Besucherkarten aus.

- Die Eingangsbereiche und Fluchttüren der Gebäude und Mietbereiche sowie zu den Sicherheits-Serverräumen werden vom Wachschutz be- bzw. überwacht. Diese Bereiche sind darüber hinaus auch videoüberwacht.
- Zur Sicherung aller Gebäude bzw. Mietbereiche sind Einbruchmeldeanlagen mit Aufschaltung beim Wachschutz bzw. einer Notrufzentrale installiert.
- Bei Gebäudeteilen, die zur Sicherheitszone 3 (Hochsicherheitsbereich) gehören, sowie bei Archivstandorten werden keine Hinweise auf die Nutzung der betreffenden Räumlichkeiten angebracht, um Unbefugten keine Anhaltspunkte für ein gezieltes Eindringen zu geben.
- Gefährdete Verglasungen im Erdgeschossbereich und beim Vorhandensein von Aufstiegshilfen (z. B. Rank-Gerüste, Fallrohre) sind durch das Aufbringen einer einbruchhemmenden Folie geschützt.
- Außerhalb der Arbeitszeit sowie an Wochenenden und Feiertagen werden durch den Wachschutz die Vorgaben zum Verschließen der Hauseingangs- und Etagentüren überprüft und bei Bedarf umgesetzt.

2.2 Zugangskontrolle

- IT-Systeme und aktive Netzkomponenten werden grundsätzlich nur in gesicherten Räumen aufgestellt, zu denen nur Berechtigte Zutritt haben.
- Zum Schutz vor unbefugten Zugriffen über Mobilgeräte gibt es zum Unternehmensnetzwerk keine Zugangsmöglichkeit über das Gäste-WLAN.
- Der Zugriff für Mitarbeiter über WLAN auf das Unternehmensnetzwerk erfordert eine besondere Berechtigung und ist nur für registrierte Mobilgeräte möglich.
- Sämtliche Kommunikation über WLAN wird nach dem Stand der Technik verschlüsselt. Die WLANs werden regelmäßig Sicherheitschecks unterzogen.
- Ungesicherte Netzzugänge werden durch die Abschottung des internen Netzes gegenüber dem öffentlichen Netz mittels mehrstufiger Firewall mit DMZ verhindert.
- Außenstandorte sind ausschließlich über VPN-Tunnel angebunden.
- Der Zugang zu IT-Systemen ist in einer Zugangssteuerungsrichtlinie geregelt.
- Es werden ausschließlich „Named-User“-Benutzerkonten verwendet.
- Benutzer müssen sich gegenüber dem IT-System durch User-ID und Passwort legitimieren.
- Die Erstellung und Nutzung sicherer Passwörter sind in einer Organisationsanweisung geregelt. Dort sind auch die Anforderungen an Passwörter und die Sicherheitseinstellungen zur Passwortsicherheit in den Kontorichtlinien festgelegt.
- Nach 3 fehlerhaften Passwordeingaben erfolgt eine automatische Sperrung der Benutzerkennung. Die Sperre wird durch den Administrator nach Beauftragung durch die verantwortliche Führungskraft oder automatisch nach acht Stunden aufgehoben.

2.3 Zugriffskontrolle

- Es wurden Regelungen zur Klassifizierung und Handhabung von Informationen hinsichtlich ihrer Vertraulichkeit in einer Organisationsanweisung herausgegeben.
- Zugriffsrechte auf klassifizierte Daten werden für jeden Beschäftigten in Abhängigkeit von der Arbeitsaufgabe restriktiv nach dem Prinzip „so viele Rechte wie nötig, so wenige wie möglich“ vergeben.
- Zur Vereinfachung werden Berechtigungen zu Rechteprofilen zusammengefasst und die Benutzer diesen Profilen zugeordnet.
- Die Rechteprofile und die Zuordnung der Benutzer zu diesen Profilen werden dokumentiert.
- Es ist ein restriktiver Datenzugriff über die Anwendungssoftware sichergestellt. Es werden nur Funktionalitäten und Daten zur Verfügung gestellt, die für die Erfüllung der jeweiligen Arbeitsaufgabe erforderlich sind.
- Alle Beschäftigten sind angehalten, ihren Bildschirm bei Verlassen des Arbeitsplatzes mit einem passwortgeschützten Bildschirmschoner zu verdunkeln. Nach fünf Minuten der Nichtbenutzung werden Bildschirme automatisch verdunkelt.
- Es gibt Vorgaben für die Beschäftigten zum aufgeräumten Arbeitsplatz, nach denen Dokumente und Datenträger bei Verlassen des Arbeitsplatzes unter Verschluss genommen oder beaufsichtigt werden müssen.
- Das sichere, rückstandsfreie Löschen der Daten bzw. Vernichten von Datenträgern nach Ablauf der Aufbewahrungsfristen lt. Löschkonzept bzw. entsprechend der Weisung des Auftraggebers bei Verarbeitung im Auftrag eines Verantwortlichen i. S. v. Art. 28 DS-GVO mit Lösch- bzw. Vernichtungsprotokoll wird gewährleistet.
- Die einzusetzenden Lösch- und Vernichtungsverfahren sind in einem Löschkonzept festgelegt.
- Bei Auftragsverarbeitung werden Daten bzw. Datenträger nur nach Weisung und vertraglichen Vorgaben des Auftraggebers als Verantwortlichem gelöscht bzw. vernichtet.
- Es gibt Festlegungen zur Auswahl und Beauftragung externer Dienstleister mit der Vernichtung von Datenträgern, insbesondere unter Beachtung der Vorschriften von Art. 28 DS-GVO.
- Die Vernichtung von Datenträgern und Akten erfolgt in Abhängigkeit vom Schutzbedarf der gespeicherten Daten bzw. bei Verarbeitung im Auftrag eines Verantwortlichen im Sinne von Art. 28 DS-GVO nach den Weisungen bzw. vertraglichen Vorgaben des für die Verarbeitungstätigkeit Verantwortlichen nach DIN 66399 Teil 1 und 2 sowie DIN SPEC 66399-3 durch einen beauftragten Unterauftragnehmer (siehe auch Anlage 1). *Dabei ist festzuhalten, dass die genannten Normen zurückgezogen wurden und ihre Inhalte in der international gültigen Normenreihe ISO/IEC 21964 fortgeführt werden. Die dort definierten Schutzklassen und Sicherheitsstufen bilden weiterhin die Grundlage für die Auswahl geeigneter Vernichtungsverfahren.*
- Das zur Vernichtung anstehende Material wird in verschlossenen Sicherheitsbehältern bzw. bei Archivmaterial in verschlossenen Sicherheits-Press-Containern gesammelt und zur Abholung bereitgestellt.

2.4 Trennungskontrolle/Zweckbindung

- Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden getrennt verarbeitet. Die Trennung wird durch mandantenfähige IT-Systeme, logische oder physikalische Trennung der IT-Systeme und Datenbestände gewährleistet.
- Bei Verarbeitung im Auftrag eines Verantwortlichen entscheidet grundsätzlich der Auftraggeber als Verantwortlicher, in welcher Form die Trennung der Daten zu erfolgen hat.
- Es erfolgt stets eine strikte Trennung zwischen Entwicklung, Test und Produktion bei Anwendungsprogrammen und Daten.

2.5 Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO)

- Es wird ein ausschließlich verschlüsselter Versand vertraulicher Daten auf mobilen Datenträgern oder über öffentliche Netze auf der Grundlage eines Kryptokonzeptes gewährleistet.
- Das Kryptokonzept sowie die verwendeten kryptographischen Verfahren und Schlüssel werden regelmäßig in Abstimmung mit dem für die jeweilige Verarbeitungstätigkeit Verantwortlichen an den Stand der Technik angepasst.
- Sichere Verbindungen werden durch die Einrichtung eines VPN-Tunnels oder die Nutzung der TLS-Verschlüsselung hergestellt, bei der Verarbeitung im Auftrag eines Verantwortlichen nach den vertraglichen Vorgaben und Weisungen des Auftraggebers als Verantwortlichem.
- Zur Verschlüsselung werden zufällig erzeugte Schlüssel verwendet.

2.6 Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO)

- Für den Fall, dass für die Verarbeitung die Identität der betroffenen Personen nicht mehr erforderlich ist, stehen geeignete Verfahren zur Pseudonymisierung zur Verfügung.
- Über den Einsatz der Pseudonymisierung entscheidet jeweils der für die Verarbeitung Verantwortliche im Rahmen seines Weisungsrechts bzw. durch vertragliche Vereinbarung.
- Bei der Pseudonymisierung wird die strikte Trennung der pseudonymisierten Daten von den identifizierenden Angaben gewährleistet.

2.7 Personelle Sicherheit

2.7.1 Vor der Beschäftigung

- Bewerber werden einem mehrstufigen Auswahlverfahren unterzogen, bei dem sowohl fachliche als auch persönliche Kriterien bewertet werden. Neue Beschäftigte müssen neben der fachlichen Eignung auch erkennen lassen, dass sie sich der Verantwortung zum Schutz personenbezogener Daten bewusst sind und dieser Verantwortung gerecht werden können.
- Jeder neue Beschäftigte hat sich bei Aufnahme seiner Tätigkeit durch Vorlage des Personalausweises oder eines vergleichbaren Dokuments (z. B. Reisepass) auszuweisen.
- Alle Beschäftigten werden vor Beginn ihrer Tätigkeit zu Vertraulichkeit und Einhaltung gesetzlicher und betrieblicher Vorschriften unter Aushändigung eines Merkblatts durch die Personalabteilung verpflichtet.

2.7.2 Während der Beschäftigung

- Es erfolgt eine geregelte Einarbeitung nach einem Einarbeitungsplan und unter Zuordnung eines erfahrenen Beschäftigten als Mentor.
- Arbeitsaufgaben und Befugnisse sind für jeden Beschäftigten in Funktions- und Tätigkeitsbeschreibungen festgelegt.
- Die Beschäftigten werden zeitnah nach Arbeitsaufnahme und dann regelmäßig zu Datenschutz und Informationssicherheit geschult.
- Es erfolgt eine regelmäßige und anlassbezogene Sensibilisierung der Beschäftigten hinsichtlich ihrer Verantwortung und ihrer Pflichten zur Wahrung von Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten sowie zu Betriebs- und Geschäftsgeheimnissen durch die Führungskräfte sowie das Datenschutz- und Informationssicherheitsmanagement.
- Beschäftigte, die gegen bestehende Regelungen verstoßen, werden nach einem geordneten Maßregelungsprozess sanktioniert.

2.7.3 Beendigung oder Änderung der Anstellung

- Es existiert ein geregelter Aussteuerungsprozess für ausscheidende Beschäftigte mit sofortigem Entzug sämtlicher Zutritts-, Zugangs- und Zugriffsrechte sowie der Rückgabe von zur Verfügung gestellten Arbeits- und Zugangsmitteln (Schlüssel, Chipkarte etc.).
- Es existiert ein geregelter Prozess bei Umsetzung innerhalb des Unternehmens mit Entzug der bisherigen und der Zuweisung neuer Berechtigungen, ggf. einschließlich ausgegebener Arbeits- und Zugangsmittel.

3 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

3.1 Eingabekontrolle

- Der Zugriff auf personenbezogene Daten erfolgt ausschließlich über „Named-User“-Benutzerkonten.
- Alle Eingaben personenbezogener Daten in IT-Systeme werden automatisch mit Zeitpunkt, User-ID und den betroffenen Dateien bzw. Datensätzen oder Datenfeldern mit ihren Inhalten protokolliert.
- Es erfolgt eine Synchronisationskontrolle durch das Sperren von Datenobjekten (Locking) zur Verhinderung von Inkonsistenzen bei möglichen parallelen Zugriffen auf den Datenbestand.
- Es erfolgt eine Integritätskontrolle zur Vermeidung semantischer Fehler bzw. semantisch unsinniger Zustände der Datenbanken durch Überwachung und Erzwingung der geforderten Integritätsbedingungen.
- Protokolldaten werden durch die verantwortliche Führungskraft bzw. einem von dieser Beauftragten stichprobenartig und anlassbezogen kontrolliert.

3.2 Weitergabekontrolle

- Die Weitergabe von personenbezogenen Daten erfolgt nur auf der Grundlage eindeutiger vertraglicher Regelungen bzw. Weisungen des für die Verarbeitungstätigkeit Verantwortlichen an berechnigte Empfänger.
- Für Versand und Empfang von Daten und Datenträgern werden stets Verantwortliche bzw. Berechnigte benannt. Die Berechnigten müssen sich legitimieren können.
- Für jede Weitergabe werden Kommunikationspartner, Wege und Verfahren des Transports bzw. der Übermittlung eindeutig festgelegt. Bei der Verarbeitung im Auftrag eines Verantwortlichen erfolgt die Weitergabe nach dessen vertraglichen Vorgaben und Weisungen.
- Die Verpflichtung aller am Verfahren beteiligten Beschäftigten zur Vertraulichkeit wird gewährleistet.
- Ein standortinterner Transport von Datenträgern zwischen unterschiedlichen Sicherheitszonen erfolgt nur in geschlossenen Behältern.
- Der Transport von Datenträgern zwischen den unterschiedlichen Standorten erfolgt in Fahrzeugen mit geschlossenem Aufbau.
- Für den Versand von Datenträgern werden nur sichere Verpackungen mit genutztem Schreibechutz eingesetzt. Die Verpackung wird so gestaltet, dass Manipulationen an den Datenträgern durch Veränderung an der Verpackung erkennbar sind.
- Die Ausgabe von Datenträgern erfolgt nur an autorisierte Personen mit Begleitpapieren und Auftragsquittung. Autorisierte Personen müssen sich ausweisen können.
- Datenträger werden für den Empfänger ausreichend beschriftet bzw. gekennzeichnet, ohne dass die Kennzeichnung für Unbefugte Rückschluss auf die Art und den Inhalt der gespeicherten Information zulässt.

- Die Lagerung aufbewahrungspflichtiger Datenträger erfolgt stets in einem Sicherheitsbereich.
- Die kontrollierte, datenschutzgerechte Vernichtung zu vernichtender Datenträger erfolgt auf der Grundlage eines Löschkonzeptes entsprechend den Weisungen des für die Verarbeitung Verantwortlichen nach DIN 66399 in der von diesem festgelegten Sicherheitsstufe und Schutzklasse mit Protokollierung. *Dabei ist festzuhalten, dass die genannte Norm zurückgezogen wurde und ihre Inhalte in der international gültigen Normenreihe ISO/IEC 21964 fortgeführt wird. Die dort definierten Schutzklassen und Sicherheitsstufen bilden weiterhin die Grundlage für die Auswahl geeigneter Vernichtungsverfahren.*
- Die elektronische Übertragung von vertraulichen Daten und auch deren Weitergabe auf mobilen Datenträgern erfolgt nur unter Verwendung von geeigneten kryptographischen Sicherheitsmechanismen (Verschlüsselung, Signatur) nach dem Stand der Technik entsprechend den Vorgaben des für die Verarbeitung Verantwortlichen.
- Die Anbindung externer Standorte und von Auftraggebern sowie weiterer berechtigter Stellen an das IT-Netz erfolgt ausschließlich über nach dem Stand der Technik verschlüsselte Verbindungen (VPN-Tunnel, TLS).

3.3 Sicherung und Überprüfung der Authentizität

- Verfahrensabhängig sind Maßnahmen eingerichtet, die die Veränderung gespeicherter oder übertragener Daten nachträglich feststellbar machen (Signaturverfahren, Hashverfahren). Über die Anwendung der Verfahren entscheidet der jeweils für die Verarbeitungstätigkeit Verantwortliche im Rahmen seines Weisungsrechts bzw. vertraglicher Vereinbarungen.

4 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

4.1 Risikomanagement und Cyber-Resilienz

Cyber-Resilienz beschreibt die Widerstandsfähigkeit des Unternehmens gegenüber Angriffen auf die Sicherheit seiner Informations- und Kommunikationstechnologie.

Praktisch ist Cyber-Resilienz bei IQVIA HSS als Kreislauf eines kontinuierlichen Verbesserungsprozesses (KVP) aufgesetzt. Dieser Prozess besteht aus fünf wesentlichen Schritten:

1. Die Identifikation und Analyse von Cyberrisiken, Schwachstellen und der allgemeinen Bedrohungslage.
2. Die Planung, Durchführung und Überwachung von Präventivmaßnahmen, damit Sicherheitsvorfälle erst gar nicht eintreten.
3. Die Entdeckung, Erkennung und zügige Meldung bzw. Eskalation von Abweichungen und Sicherheitsereignissen.
4. Die schnelle, angemessene und zielführende Reaktion auf Ereignisse und Vorfälle (insbesondere Notfälle) unter Wahrung der Betriebskontinuität.
5. Die Wiederherstellung des Normalbetriebs der Prozesse, sowie die Nachbereitung von Vorfällen und Abweichungen.

Diese Schritte stellen zusammen eine stetige Verbesserung bei der Cyberresilienz sicher. Dies betrifft nicht nur Sicherheitsereignisse und -vorfälle. Auch wenn in der regelmäßigen Überwachung eine Sollabweichung erkannt wird (dies kann ein Blocker sein), werden wirksame Maßnahmen ergriffen, um diese zu beheben.

Einzelheiten dazu sind in einem separaten Konzept „Risikomanagement und Cyberresilienz“ beschrieben.

4.2 Maßnahmen zur Sicherung der Stabilität des Anwendungssystems

Zur Sicherung der Systemstabilität werden alle IT-Systeme durch ein System-Monitoring überwacht. Diese Lösung schafft Transparenz bezüglich Zustand und Auslastung von Netzwerk und einzelnen IT-Komponenten.

Der Zustand des Netzes und seiner Komponenten wird visuell dargestellt. Bei Warnungen und kritischen Zuständen erfolgt eine zentrale Alarmierung. Performance- und Auslastungsdaten werden aufgezeichnet und stehen für Auswertungen und Systemoptimierungen zur Verfügung.

Weiterhin wurden folgende Maßnahmen zur Sicherung der Systemstabilität getroffen:

Maßnahmen gegen den Ausfall interner Versorgungsnetze

- Einschlägige DIN-Normen und VDE-Vorschriften werden beim Einbau technischer Gebäudeausrüstungen und bei Beschaffung und Betrieb von Geräten eingehalten.
- Ein geregelter Zutritt/Zugang zu Verteilern für Befugte wird gewährleistet.
- Es wird eine angepasste Aufteilung der Stromkreise sichergestellt, ggf. auch durch Prüfung und bedarfsgerechte Anpassung der Elektroinstallation.

Maßnahmen gegen den Ausfall vorhandener Sicherheitseinrichtungen

- Türschlösser werden regelmäßig durch die Haustechnik auf Zustand und Funktion geprüft und bei Beschädigung unverzüglich ausgetauscht.
- Die vorhandenen Feuerlöscher und Brandmeldeeinrichtungen werden regelmäßig geprüft und gewartet.
- Alle Brandmelder werden in einem sauberen Zustand gehalten und regelmäßig durch einen Fachbetrieb überprüft.
- Durch regelmäßige Kontrollen und Sensibilisierungsmaßnahmen wird sichergestellt, dass Brand- und Rauchschutztüren nicht z. B. durch Keile offengehalten werden.

Maßnahmen gegen Datenverlust oder Systemcrash durch defekte Datenträger

- Es werden ausschließlich redundante Plattensysteme, sogenannte RAID-Sets für System- und Anwendungsdaten eingesetzt.
- Es erfolgen eine softwaretechnische Überwachung der redundanten Plattensysteme sowie ein unverzüglicher Austausch von defekten Platten.

Maßnahmen gegen den Verlust gespeicherter Daten

- Die Einhaltung von erforderlichen Umgebungsbedingungen wird durch Klimatisierung der Serverräume bei redundanter Auslegung der Klimageräte erreicht.
- Zum Schutz vor Zerstörung durch Feuer sind die Sicherheitsserverräume jeweils mit Brandfrühsterkennungs- und Brandmeldesystem sowie einer Stickstoff-Löschanlage ausgerüstet.
- Zum Schutz vor Zerstörung durch Wasser werden wasserführende Leitungen in den Serverräumen vermieden.
- Der Schutz vor der Zerstörung durch Magnetfelder wird durch das Dämpfungsverhalten der Lampertz-Sicherheitsserverräume bei einer Dämpfung zwischen 13 dB und 65 dB im Frequenzband von 10 kHz bis 1 GHz erreicht.
- Den Schutz vor unbeabsichtigtem Löschen oder Überschreiben der Daten auf den IT-Systemen sichert die Anwendungssoftware, die ein Löschen von Datensätzen durch Benutzer nicht zulässt.
- Der Einsatz redundanter Plattensysteme (RAID-Sets) schützt vor Datenverlust durch technisches Versagen (z. B. Headcrash) sowie durch fehlerhafte Datenträger.

Maßnahmen gegen Ausfall einer Datenbank

- Gegen den Ausfall durch unbefugte Zugriffe schützen die eingerichteten Zugangs- und Zugriffskontrollmaßnahmen.
- Redundante Festplattensysteme (RAID-Sets) für Datenbank- und Log-Dateien schützen vor Ausfall der Datenbank durch defekte Datenträger.
- Das tägliche Backup der Datenbankdateien sowie die täglich mehrmalige Sicherung der Datenbank-Logs gewährleisten bei Ausfall eine Wiederherstellung mit geringem Datenverlust.

Maßnahmen gegen Ausfall oder Störung von zentralen Netzkomponenten

- Die redundante Auslegung der Core-Switches in den Sicherheits-Serverräumen („Hot Standby“) gewährleistet die Verfügbarkeit des Netzes auch bei Ausfall eines Gerätes durch Störung oder Wartung.
- Die redundante Auslegung der Firewall-Komponenten Paketfilter und Application Level Gateway („Hot Standby“) gewährleistet die sichere Anbindung an das öffentliche Netz auch bei Ausfall einer Firewall-Komponente durch Störung oder Wartung.
- Die redundante Auslegung der VPN-Appliances („Hot Standby“) sichert den Betrieb der VPN-Verbindungen auch bei Ausfall einer Appliance durch Störung oder Wartung.

4.3 Maßnahmen zur Ausfallsicherheit gegen Feuer und Wasser**Maßnahmen gegen Feuer**

- Zentrale IT-Systeme und Netzkomponenten sind zum Schutz gegen Feuer in Sicherheitsserverräumen der Feuerwiderstandsklasse F90 nach DIN 4102 untergebracht, die die Grenzwerte nach EN 1047-2 über 30 Minuten einhalten.
- Die Ausstattung der Sicherheitsserverräume mit Brandfrühgesternkennungs- und Brandmeldesystem einschließlich dessen Integration in die bestehende Brandmeldeanlage gewährleistet eine frühzeitige Erkennung von Brandgefahren und ermöglicht ein Eingreifen vor dem Ausbruch eines Feuers.
- Die Ausstattung der Sicherheitsserverräume mit automatischen Stickstoff-Löschanlagen einschließlich Überdruckableitung und Rauchgasentsorgung verhindert Feuerschäden an den IT-Systemen bei Ausbruch eines Brandes.
- Die Rauchgasdichtigkeit der Sicherheitsserverräume (Türsystem nach EN 18095) schützt die IT-Systeme gegen korrosive Gase aus der Umgebung der Serverräume. Dabei liegt die Luftaustauschrate für das gesamte Raumvolumen des Sicherheitsraumes unter 0,8.
- Die Gebäude an allen Standorten sind mit Brandmeldeanlagen ausgerüstet, die situativ direkt bei der Feuerwehr oder dem Sicherheitsdienst aufgeschaltet sind.
- Alle Bürogebäude und Archive sind mit Feuerlöschern in ausreichender Menge ausgerüstet.
- Es sind Maßnahmen des vorbeugenden Brandschutzes getroffen, wie
 - ein generelles Rauchverbot in allen Räumlichkeiten,
 - das Verbot des Hantierens mit Feuer und offenem Licht in allen Räumlichkeiten,
 - die Vermeidung unnötiger Brandlasten,
 - die Gewährleistung der Funktion der Brandschutz- und Rauchschutztüren,
 - regelmäßige Begehungen durch den Brandschutzbeauftragten.

Maßnahmen gegen Wasser

- Bei der Standortauswahl wird stets darauf geachtet, dass sich die Standorte nicht in Überschwemmungsgebieten befinden. Grundlage dafür bildet das Zonierungssystem für Überschwemmungsrisiko und Einschätzung von Umweltrisiken (ZÜRS) des Gesamtverbandes der Deutschen Versicherungswirtschaft.
- Die zentralen IT-Systeme sind durch die Aufstellung in Sicherheitsserverräumen nachhaltig gegen stehendes Wasser (z. B. Löschwasser) geschützt. Die Leckage-Rate der Räume ist nach Herstellerangaben kleiner als 1 Liter in 72 Stunden bei einer Wassersäule von 40 cm im Außenbereich des Raumes.
- Die Serverräume selbst beinhalten keine wasserführenden Leitungen.

4.4 Maßnahmen zur Ausfallsicherheit in Bezug auf Außenwirkungen

Stromausfall/Netzausfall

- Die Mittelspannungsversorgung der Standorte erfolgt über eine Ringleitung, die eine kurzfristige Wiederherstellung der Versorgung bei einer Störung ermöglicht. Die Wiederherstellung erfolgt lt. Netzbetreiber i. d. R. innerhalb von 2 Stunden, eine Wiederherstellung durch Freischaltung des gestörten Abschnitts in max. 4 Stunden wird bei Netzausfall garantiert.
- Ausfälle der Stromversorgung bis zu 6 Stunden können für Serverräume, Netzkomponenten und einzelne ausgewählte Arbeitsplätze durch ein Bleibatterie-USV-System überbrückt werden. Danach steht die Energieversorgung für diese Systeme noch bis zu 2 Stunden für einen geordneten Shutdown zur Verfügung.
- Die Server werden nach Ablauf der Autonomiezeit automatisch in einer festgelegten Reihenfolge heruntergefahren. Testsysteme werden zur Verlängerung der Autonomiezeit für die Produktivsysteme unverzüglich heruntergefahren.

Funktionsausfall oder Wartung der Hauptstromversorgung

- Bei Ausfall oder Wartung der Hauptstromversorgung können die zentralen IT-Systeme sowie die externe Anbindung am Hauptstandort in Leipzig-Mölkau durch einen Hilfsbetrieb über die Niederspannungs-Hauptstromversorgung des Vermieters umgeschaltet werden, sofern nicht gleichzeitig ein Netzausfall des Versorgers vorliegt.

Spannungsschwankungen/Überspannung/Unterspannung

- Schutz vor Überspannungen und Spannungsschwankungen besteht für zentrale IT-Systeme und Datenspeicher durch Netzfilter in den unterbrechungsfreien Stromversorgungen.
- Bei Unterspannungen greifen die gleichen Mechanismen wie bei Stromausfall.

Ausfall der Internetanbindung

- Bei Ausfall eines Anschlusses für externe Zugriffe steht eine Backup-Leitung zur Verfügung.
- Die für die externe Kommunikation erforderlichen Netzkomponenten sind durch die o. g. Maßnahmen gegen Stromausfall, Spannungsschwankungen, Über- und Unterspannung geschützt.

4.5 Maßnahmen gegen Vandalismus

- Sämtliche IT-Systeme, Archivsysteme und aktive Netzkomponenten sind in entsprechend gesicherten Räumen aufgestellt.
- Die sichere Verwahrung von Datenträgern und Dokumenten in entsprechenden Sicherheitszonen wird gewährleistet.
- Es wird auf geschlossene Fenster bei unbesetzten Räumen und verschlossene Außentüren geachtet.
- Alle Standorte werden rund um die Uhr durch einen Sicherheitsdienst be- bzw. überwacht.
- Es erfolgt eine Bestreifung der Objekte durch den Sicherheitsdienst während der Betriebsruhezeiten nach festen, vorgeschriebenen Plänen.
- Zusätzlich werden alle Objekte durch Einbruchmeldeanlagen mit Aufschaltung beim Sicherheitsdienst bzw. einer Notrufzentrale überwacht.
- Glasflächen an Fenstern und sonstigen Verglasungen in Erdgeschossbereichen und beim Vorhandensein von Aufstiegshilfen (z. B. Rank-Gerüste, Fallrohre) sind mit einer einbruchhemmenden Folie ausgerüstet.
- An allen Standorten erfolgt eine Videoüberwachung der Eingangsbereiche und Fluchttüren.
- In unübersichtlichen Bereichen wie z. B. im Archiv sind Fluchttüren auch während der Betriebszeit mit einer Alarmierung ausgerüstet.
- Die Sicherheits-Serverräume sind mit Türsystemen der Widerstandsklasse RC 4 (alt WK 4) nach EN 1627:2011 ausgestattet. Das komplette Raumsystem erfüllt RC 3 (alt WK 3) nach EN 1627:2011.

4.6 Maßnahmen zum Schutz gegen Schadsoftware

- Bekannte Schwachstellen in Betriebssystemen und Anwendungssoftware werden durch ein Patch-Management regelmäßig beseitigt.
- Alle IT-Systeme werden mit sicheren BIOS-Einstellungen mit Passwortschutz betrieben.
- Die Nutzung von mobilen Datenträgern ist nur an bestimmten, dafür vorgesehenen IT-Systemen möglich. An allen anderen IT-Systemen wird die Nutzung von mobilen Datenträgern mit technischen Mitteln unterbunden.
- Es ist ein durchgängiger, mehrstufiger Virenschutz mit folgenden Komponenten umgesetzt:
 1. Zentraler Virenschutz des ein- und ausgehenden Datenverkehrs einschließlich E-Mails im Bereich der Firewall,
 2. zentral verwalteter Virenschutz auf allen Client-Systemen und Fileservern.
- Die tägliche automatische Aktualisierung des Virenschutzes wird zentral gewährleistet.

- Bei der Internetnutzung werden aktive Inhalte – soweit möglich – geblockt.
- Dateien und Programme dürfen nur von dafür Befugten aus vertrauenswürdigen Quellen heruntergeladen werden.
- Es erfolgt keine Unterdrückung von Dateiendungen an Arbeitsstationen und Servern, um Dateiarten unterscheiden und so ggf. versteckte Schadsoftware erkennen zu können.
- Es erfolgt eine angemessene Schulung und Sensibilisierung der Anwender zu Bedrohungen und Schutzmaßnahmen, insbesondere auch zum Umgang mit verdächtigen E-Mails bzw. E-Mail-Anhängen. Auf aktuelle Ereignisse und Bedrohungen wird auch im Intranet hingewiesen.

4.7 Sicherung der Datenbestände

- Es erfolgt eine regelmäßige Sicherung der Datenbestände nach einem Backup-Konzept.
- Die Datensicherungen werden getrennt von den Produktionsdaten in anderen Brandabschnitten und/oder Gebäuden aufbewahrt.

4.8 Vertretungsregelungen für abwesende Beschäftigte

- Für Funktionen und Tätigkeiten sind Vertretungsregelungen eingerichtet.

4.9 Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem Zwischenfall (Art. 32 Abs. 1 lit. c DS-GVO)

- Für den Umgang mit bestimmten Notfallsituationen wurde ein Notfallhandbuch erarbeitet, das neben wichtigen Regelungen zum Umgang mit Notsituationen, zu Meldewegen und Verantwortlichkeiten auch Wiederanlaufpläne zur Wiederherstellung der Verfügbarkeit nach einem Zwischenfall enthält.
- Die Wiederherstellbarkeit von IT-Systemen sowie Wiederanlaufszszenarien werden regelmäßig durch Recovery-Tests bzw. Notfallübungen geprüft.
- Identifizierung neuer Risiken und Schwachstellen sowie Neubewertung erkannter Risiken und deren Behandlung im Rahmen der Nachbereitung von Notfallsituationen.

5 Maßnahmen bei Einsatz von Videokonferenzsystemen

- Für die Kommunikation mit Auftraggebern werden ausschließlich durch IQVIA HSS freigegebene Videokonferenzsysteme eingesetzt. Die Nutzung erfolgt unter Beachtung der jeweils geltenden datenschutzrechtlichen, vertraglichen und informationssicherheitsrelevanten Vorgaben. Die dabei verarbeiteten Daten unterliegen den in diesem Sicherheitshandbuch beschriebenen technischen und organisatorischen Maßnahmen.
- Zur Gewährleistung von Vertraulichkeit, Verfügbarkeit und Integrität der dabei verarbeiteten personenbezogenen Daten greifen die in diesem Sicherheitshandbuch beschriebenen Maßnahmen.
- Die inhaltliche Aufzeichnung von Online-Meetings ist grundsätzlich technisch gesperrt.
- Die Nutzer werden darüber unterrichtet, dass das Mitschneiden von Video- und/oder Audiodaten, das Speichern und das Verbreiten solcher Aufnahmen strafbar sein kann.

- Sollen im Ausnahmefall Online-Meetings aufgezeichnet werden, so wird zuvor von allen Teilnehmern eine Einwilligung gemäß Art. 7 DS-GVO eingeholt. Die Aufzeichnung muss zudem intern gesondert beantragt und genehmigt werden.
- Zulässig sind Aufzeichnungen nur bei Meetings mit Informationscharakter, wie z.B. Informations-Sessions, Präsentationen oder Trainings.
- Sobald der Verwendungszweck gemäß Einwilligung entfällt, ist die Aufzeichnung zu löschen.
- Der sog. beständige Chat ist zentral deaktiviert. Sobald ein Chatfenster geschlossen wird, wird auch der Inhalt gelöscht. Es wird lediglich der Chatverlauf gespeichert und nach einem Monat gelöscht.
- Mit der Einladung zum Online-Meeting wird auch ein Link zu den Datenschutzhinweisen zur Erfüllung der Informationspflichten gemäß Art. 13 DS-GVO versendet.

6 Telearbeit (IQVIA HSS@Home)

- Die Erbringung von Arbeitsleistungen mittels Telearbeit an einem häuslichen Arbeitsplatz ist nur mit ausdrücklicher Genehmigung des Auftraggebers zulässig.
- Sofern der Auftraggeber Telearbeit beim Auftragnehmer genehmigt hat, erfolgt die Arbeit an häuslichen Arbeitsplätzen, die den gesetzlichen Anforderungen an Arbeitsstätten (ArbStättV) entsprechen müssen.
- Die Einrichtung der Telearbeitsplätze sowie die Gewährleistung von Datenschutz und Datensicherheit bei der Telearbeit erfolgt auf der Grundlage der „Konzeption zur Telearbeit IQVIA HSS@Home“, die dem Auftraggeber bei der Beantragung von Telearbeit unaufgefordert zur Verfügung gestellt wird.
- Die Maßnahmen zu Datenschutz und Datensicherheit berücksichtigen insbesondere auch die Hinweise aus dem Datenschutz-Wegweiser „Telearbeit und mobiles Arbeiten“, der vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit herausgegeben wurde.

7 Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen Maßnahmen (Art. 32 Abs. 1 lit. d DS-GVO)

- Die Gesamtverantwortung für Datenschutz und Informationssicherheit und die damit verbundenen Maßnahmen hat die Geschäftsführung in einer für alle Beschäftigten transparenten Form durch eine Datenschutzrichtlinie und eine Informationssicherheitspolitik übernommen.
- Die Beschäftigten werden bei Arbeitsaufnahme und danach regelmäßig zu Datenschutz und Informationssicherheit geschult und der Wissensstand durch einen Wissenstest überprüft.
- Die Verpflichtung der Beschäftigten zum vertraulichen Umgang mit personenbezogenen Daten sowie Betriebs- und Geschäftsgeheimnissen erfolgt bei Einstellung durch die Personalabteilung.
- Im Unternehmen wurden ein Datenschutzbeauftragter und ein Informationssicherheitsbeauftragter benannt. Der Datenschutzbeauftragte ist weisungsfrei bei der Erfüllung seiner Aufgaben und berichtet direkt an die Geschäftsführung.
- Es sind ein Internes Kontrollsystem (IKS) und eine Innenrevision zur Prüfung der Rechts- und Auftragskonformität der Geschäftsprozesse eingerichtet.

- Es ist ein Informationssicherheitsmanagementsystem (ISMS) nach DIN EN ISO/IEC 27001 (aktuellste Version) in Verbindung mit einem Datenschutzmanagementsystem (DSMS) eingerichtet. In Verbindung damit ist auch ein Risikomanagement etabliert.
- Die Wirksamkeit der aus der Risikobewertung und den Audits resultierenden Maßnahmen wird regelmäßig durch interne Kontrollen und Audits überprüft. Bei Bedarf werden die Maßnahmen angepasst bzw. durch andere, geeignete Maßnahmen ersetzt oder ergänzt.
- Es ist ein Verfahren zur fristgemäßen Behandlung von Anfragen Betroffener eingerichtet.
- Es ist ein Verfahren zur Meldung und Behandlung von Datenschutzverletzungen und Informationssicherheitsvorfällen eingerichtet.

8 Anlagen

- Anlage 1 – Übersicht der Unterauftragnehmer
- Anlage 2 – Übersicht der Wartungsunternehmen

 Health System Services Partner des deutschen Gesundheitswesens	Übersicht Unterauftragnehmer	
--	-------------------------------------	---

Übersicht der für die IQVIA Health System Services GmbH tätigen Unterauftragnehmer, die unmittelbar Daten des Auftraggebers erheben oder verarbeiten, sowie jene Unterauftragnehmer, die die eingesetzten automatisierten Verfahren oder Datenverarbeitungsanlagen im Auftrag prüfen bzw. warten und bei denen im Zusammenhang mit diesen Tätigkeiten ein Zugriff auf Sozialdaten nicht ausgeschlossen werden kann (vgl. § 80 Abs. 5 SGB X)

Name des Unterauftragnehmers	Anschrift	Aufgabenfeld
REISSWOLF Akten- und Datenvernichtung GmbH Sachsen	Fischweg 14a 09114 Chemnitz	Akten- und Datenträgervernichtung
Konica Minolta Business Solutions Deutschland GmbH	Europaallee 17 30855 Langenhagen	Wartung von Kopierern, Multifunktionsgeräten und Großdruckern
Pitney Bowes Deutschland GmbH	Poststraße 4-6 64293 Darmstadt	Wartung von Kuvertiermaschinen
IBYKUS AG	Hermann-Hollerith-Straße 1 99099 Erfurt	Wartung der Kodak-Scanner (Hardware und Software)
Telekom Deutschland GmbH	Landgrabenweg 151 53838 Bonn	Erkennung von Bedrohungen und Sicherheitsvorfällen durch den Magenta Security Shield Advanced Managed SOC Service Magenta Security Red Team Services für realistische Bewertung des Schutzniveaus durch Simulation eines Cyberangriffs sowie Incident Response Prozesse
Imaging Business Machines GmbH	Line-Eid-Straße 3 78467 Konstanz	Wartung der IBML-Scanner (Hardware und Software)
HeptaSphere GmbH	Drosselweg 19 14656 Brieselang	Wartung des Belegauslesesystems (OCR)
recosys Recognition Systems GmbH	Turmstr. 14 78467 Konstanz	Wartung von Zusatzsoftware – IBML Scanner
Druckerfachmann.de GmbH & Co. KG	Wegedornstraße 36 12524 Berlin	Wartung aller Bürodruker

Übersicht über weitere für die IQVIA Health System Services GmbH tätige Unternehmen, die jedoch keine Daten des Auftraggebers erheben, verarbeiten und/oder nutzen:

Name des Unterauftragnehmers	Anschrift	Aufgabenfeld
Noack & Neumann GmbH	Maximilianallee 4 04129 Leipzig	Objektbewachung, Stellung von Wach- und Empfangspersonal
Deutsche Post InHaus Services GmbH	Euskirchener Straße 52 53121 Bonn	Abholung, Frankierung und Sortierung verschlossener Briefsendungen (Verwendung von Adressdaten nach § 41 Abs. 2 Postgesetz (PostG))

Stand: 07.09.2026

 Health System Services Partner des deutschen Gesundheitswesens	Übersicht Wartungsfirmen	
--	---------------------------------	---

Übersicht über die für die IQVIA Health System Services GmbH tätigen Wartungsfirmen, die die eingesetzten automatisierten Verfahren oder die eingesetzten Datenverarbeitungsanlagen im Auftrag prüfen oder warten und bei denen im Zusammenhang mit den genannten Tätigkeiten ein Zugriff auf Sozialdaten nicht ausgeschlossen werden kann, vgl. § 80 Abs. 5 SGB X.

Name der Wartungsfirma	Anschrift	Aufgabenfeld
Konica Minolta Business Solutions Deutschland GmbH	Europaallee 17 30855 Langenhagen	Wartung von Kopierern, Multifunktionsgeräten und Großdruckern
Pitney Bowes Deutschland GmbH	Poststraße 4-6 64293 Darmstadt	Wartung von Kuvertiermaschinen
MTG-Kommunikations-Technik GmbH	Portitzer Allee 8 04329 Leipzig	Wartung von Telefon- und Alarmanlage
BE-terna GmbH	Bornaer Straße 19 04288 Leipzig	Wartung der Software Microsoft Dynamics Navision
SecCommerce Informationssysteme GmbH	Obenhauptstraße 5 22335 Hamburg	Wartung der Signaturanwendungskomponenten
IBYKUS AG (ehem. e-das GmbH)	Hermann-Hollerith-Straße 1 99099 Erfurt	Wartung der Kodak-Scanner (Hardware und Software)
Kodak Alaris Germany GmbH	Augsburger Straße 712 70329 Stuttgart	Hardware-Wartung Kodak-Scanner
MGID Mitteldeutsche Gesellschaft für Informationssicherheit und Datenschutz mbH	Mozartstraße 10 04107 Leipzig	Sicherheitstechnische Überprüfung der IT-Infrastruktur mittels Penetrationstests
Telekom Deutschland GmbH	Landgrabenweg 151 53838 Bonn	Erkennung von Bedrohungen und Sicherheitsvorfällen durch den Magenta Security Shield Advanced Managed SOC Service Magenta Security Red Team Services für realistische Bewertung des Schutzniveaus durch Simulation eines Cyberangriffs sowie Incident Response Prozesse
Imaging Business Machines GmbH	Line-Eid-Straße 3 78467 Konstanz	Wartung der IBML-Scanner (Hardware und Software)
HeptaSphere GmbH	Drosselweg 19 14656 Brieselang	Wartung des Belegauslesesystems (OCR)
recosys Recognition Systems GmbH	Turmstr. 14 78467 Konstanz	Wartung von Zusatzsoftware – IBML Scanner

Stand: 07.09.2026

Welche personenbezogenen Daten werden verarbeitet?

Die Tabelle zeigt Datenkategorien und Personengruppen.

	Versicherte/ Privatkunden	Vertreter von Geschäfts- partnern	Leis- tungser- bringer	Geschäfts- partner
Stammdaten	☒	☒	☒	☒
Identitätsdaten	☐	☒	☒	☐
Finanzidentifikations- daten	☐	☐	☐	☒
Kommunikationsda- ten	☐	☒	☒	☒
Versicherungs- und Beitragsdaten	☐			
Leistungs- und Gesundheitsdaten	☒			
Beschäftigtendaten				
technische Daten	☐	☐	☒	☒
Betriebs- und Geschäftsgeheim- nisse		☐	☐	☐

Übersicht zu den Datenannahmestellen der Krankenkassen *)

Vertragsbereich	Krankenkasse	IK-Kasse	Dokumentationen			Teilnahme- und Einwilligungserklärungen	Statusdatensatz
			plausible b-Daten	nicht plausible b-Daten	Zyklus	Zyklus	
HH	AOK HH	104 212 516	ja	nein	wtl./Di-Sa	wtl./Di-Sa	wtl./Di-Fr
HH	IKK classic (HH)	101 500 154	ja	nein	wtl./Di-Sa	wtl./Fr	wtl./Di-Fr
HH	IKK classic (BW, HS)	108 001 963	ja	nein	wtl./Sa	keine Datenlieferung	wtl./Fr
HH	IKK classic (SA)	107 202 793	ja	nein	wtl./Sa	keine Datenlieferung	wtl./Fr
HH	IKK classic (TH)	105 903 116	ja	nein	wtl./Sa	keine Datenlieferung	wtl./Fr
HH	IKK classic (WL)	103 500 693	ja	nein	wtl./Sa	keine Datenlieferung	wtl./Di-Fr
HH	IKK - Die Innovationskasse (ehem.IKK Nord) (Ost)	100 202 549	ja	nein	wtl./Sa	wtl./Sa	wtl./Fr
HH	IKK - Die Innovationskasse (ehem.IKK Nord) (West)	101 300 129	ja	nein	wtl./Sa	wtl./Sa	wtl./Fr
HH	IKK Südwest	109 303 301	ja	nein	wtl./Sa	wtl./Fr	wtl./Fr
HH	IKK gesund plus	101 202 961	ja	nein	wtl./Sa	wtl./Fr	wtl./Di-Fr
HH	BIG direkt gesund	103 501 080	ja	nein	wtl./Sa	wtl./Fr	nein
HH	IKK Brandenburg und Berlin	100 602 360	ja	nein	wtl./Sa	keine Datenlieferung	nein
HH	SVLFG (LKK Niedersachsen-Bremen)	102 108 731	ja	nein	wtl./Do	keine Datenlieferung	wtl./Fr
HH	SVLFG LKK Mittel- und Ostdeutschland)	100 609 049	ja	nein	wtl./Do	keine Datenlieferung	wtl./Fr
HH	SVLFG (LKK Schleswig-Holstein und Hamburg)	101 308 719	ja	nein	wtl./Do	keine Datenlieferung	wtl./Fr
HH	SVLFG (LKK Baden-Württemberg)	108 008 880	ja	nein	wtl./Do	keine Datenlieferung	wtl./Fr
HH	SVLFG (LKK Hessen, Rheinland-Pfalz und Saarland)	105 508 787	ja	nein	wtl./Do	keine Datenlieferung	wtl./Fr
HH	SVLFG (LKK NRW, Detmold/Münster/Düsseldorf)	103 708 773	ja	nein	wtl./Do	keine Datenlieferung	wtl./Fr
HH	SVLFG (LKK Bayern, Franken/Oberbayern)	108 608 820	ja	nein	wtl./Do	keine Datenlieferung	wtl./Fr
HH	SVLFG (LKK Bayern, Niederbayern/Oberpfalz/Schwaben)	109 008 837	ja	nein	wtl./Do	keine Datenlieferung	wtl./Fr
HH	SVLFG (Krankenkasse für den Gartenbau)	105 508 890	ja	nein	wtl./Do	keine Datenlieferung	wtl./Fr
HH	Knappschaft	109 905 003	ja	nein	wtl./Do	wtl./Di	wtl./Di-Fr
HH	DAK-Gesundheit	105 830 016	ja	nein	wtl./Di-Sa	keine Datenlieferung	wtl./Di-Fr
HH	BARMER	104 940 005	ja	nein	wtl./Di-Sa	wtl./Di-Sa	täglich
HH	Techniker Krankenkasse (TK)	101 575 519	ja	nein	wtl./Di-Sa	wtl./Di-Sa	täglich
HH	Kaufmännische Krankenkasse - KKH	102 171 012	ja	nein	wtl./Di-Sa	wtl./Di-Sa	täglich
HH	HEK - Hanseatische Krankenkasse	101 570 104	ja	nein	wtl./Di-Sa	wtl./Di-Sa	täglich
HH	Handelskrankenkasse (hkk)	103 170 002	ja	nein	wtl./Di-Sa	wtl./Di-Sa	wtl./Di-Fr
HH	BKK ²⁾	diverse HIK	ja	nein	wtl./Fr	keine Datenlieferung	täglich ¹⁾
HH	SBK Siemens-Betriebskrankenkasse	108 433 248	ja	nein	wtl./Di-Sa	keine Datenlieferung	wtl./Di-Fr
HH	Mobil Krankenkasse	101 520 078	ja	nein	wtl./Fr	wtl./Fr	wtl./Di
HH	VIActiv Krankenkasse	104 526 376	ja	nein	wtl./Fr	wtl./Fr	wtl./Di-Fr

*) Nur elektronische Daten. Weitere Informationen, einschließlich zum Versand der Dokumentationsbögen, entnehmen Sie bitte der Leistungsbeschreibung.

*1) Lieferung Statusdatensatz für die BKK'n erfolgt an die Bitmarck Service GmbH (IK 104027544)

*2) außer: Mobil Krankenkasse und VIActiv Krankenkasse sowie SBK Siemens-Betriebskrankenkasse

IQVIA Health System Services GmbH · Sommerfelder Straße 120 · 04316 Leipzig



Dr. Max Mustermann
Dr. Partner1 MustermannP1
Dr. Partner2 MustermannP2
Musterweg 12
01234 Musterhausen

Achtung: DAVASO GmbH ist jetzt IQVIA Health System Services GmbH.

Neue KIM-Adresse ab 01.10.2026

Bitte verwenden Sie ab 01.10.2026

dmp-datenstelle@iqvia-hss.kim.telematik

Die bisherige KIM-Adresse bleibt bis zum 31.12.2026 aktiv

Telefon: 0341 25920-43

Fax: 0341 25920-22

Datum: 15.09.2026

DMP - Verarbeitungsstand Ihrer Daten

Sehr geehrte Damen und Herren,

eine unserer zentralen Aufgaben ist die Erfassung und Plausibilisierung der von den Ärzten angelieferten DMP-Daten. Um Ihnen einen Überblick über die Verarbeitung der von Ihnen gelieferten Teilnahme- und Einwilligungserklärungen (TE) und Dokumentationen zu geben, übersenden wir Ihnen regelmäßig Informationen über den Bearbeitungsstand. **Es sind nur für Sie zutreffende Anlagen diesem Schreiben beigelegt.**

- Für Ihre in der Anlage „**Übersicht: nicht plausible Dokumentationen und TE, die Ihnen bereits zur Korrektur vorliegen**“ genannten Patienten erfolgte bislang keine vollständige Erfassung der notwendigen Dokumentationen oder TE im Rahmen des genannten DMP. Bitte verwenden Sie hierfür die bereits übermittelten Korrekturbelege. Sollten Sie innerhalb der letzten 3 Werktage Korrekturlieferungen an uns gesandt haben, so sind diese in der Information nicht berücksichtigt.
- Ihre in der Anlage „**Übersicht: plausible Dokumentationen und TE der letzten 14 Tage**“ aufgeführten Dokumentationen und TE sind gültig. Bitte prüfen Sie die Auflistung auf Vollständigkeit.
- Für Ihre in der Anlage „**Übersicht: fehlende Erstdokumentationen**“ genannten Patienten fehlen uns die entsprechenden Daten.
- Für Ihre in der Anlage „**Übersicht: zu erstellende Folgedokumentationen**“ genannten Patienten fehlen uns die entsprechenden Daten. **Die befristete Sonderregelung zur fakultativen Erstellung von Folgedokumentationen aufgrund der Corona-Pandemie ist zum 31.12.2021 ausgelaufen. Ab dem 01.01.2022 sind wieder regelmäßige Folgedokumentationen für die Patienten zu erstellen.**
- Ihre in der Anlage „**Übersicht: Folgedokumentationen im falschen zeitlichen Kontext**“ aufgeführten Folgedokumentationen können in der Regel nicht für die DMP-Prozesse berücksichtigt werden. Eine nähere Erklärung entnehmen Sie bitte der Legende der Anlage.
- Ihre in der Anlage „**Übersicht: außerhalb des Übermittlungszeitraumes eingegangene Dokumentationen**“ aufgeführten Dokumentationen können aufgrund der Überschreitung des Übermittlungszeitraumes nicht für die DMP-Prozesse berücksichtigt werden.
- Ihre in der Anlage „**Übersicht: Patienten, deren Krankenkasse nicht am DMP teilnimmt**“ aufgeführten Dokumentationen und TE werden von uns nicht weiter verarbeitet.

- Ihre in der Anlage „**Übersicht: nicht prozesskonforme Dokumentationen und TE**“ aufgeführten Dokumentationen und TE können wegen verfahrensbedingter Fehler nicht für die DMP-Prozesse verwendet werden. Eine nähere Erklärung entnehmen Sie bitte der Legende dieser Anlage.
- Für Ihre in der Anlage „**Übersicht: Fallbeendigungen**“ aufgeführten Patienten wurden die DMP-Fälle beendet. Eine nähere Erklärung entnehmen Sie bitte der Legende dieser Anlage.
- Ihre in der Anlage „**Übersicht: nicht verarbeitbare Datenlieferungen**“ aufgeführten DMP-Daten können nicht für die Weiterverarbeitung im Sinne der DMP-Prozesse berücksichtigt werden. Bitte übermitteln Sie uns die betreffenden DMP-Daten erneut.

Bitte beachten Sie, dass zur Erstellung der Teilnahme- und Einwilligungserklärungen das aktuell gültige Formular mit dem Formularschlüssel 070E (indikationsübergreifend) zu verwenden ist.

Wir bitten Sie, diese Information als Serviceleistung für Ihre Praxis zu betrachten.

Bei Postsendungen verwenden Sie bitte folgende Adresse:

IQVIA Health System Services GmbH
Abteilung DMP-HH
Postfach 50 07 53
04304 Leipzig

Für Rückfragen stehen wir Ihnen telefonisch unter 0341 25920-43 gern zur Verfügung.

Mit freundlichen Grüßen

IQVIA Health System Services GmbH

Übersicht: nicht plausible Dokumentationen und TE, die Ihnen bereits zur Korrektur vorliegen

Patient Name, Vorname	Krankenvers.-nummer	Krankenkasse	DMP-Fall-Nr.	Belegtyp	DMP-Diagnose	Datum Beleg	Datum Versand	Fristablauf
Doppelmuster, Michaela	B175162340	Musterkasse	411139	FD	DM2	18.08.2026	16.09.2026	23.11.2026
Fremdmuster, Martha	F50411442	Musterkasse	252910	FD	DM2	11.09.2026	15.09.2026	23.11.2026
Großmuster, Michaela	G999835226	Musterkasse	628428	FD	DM2	08.07.2026	17.09.2026	23.11.2026
Großmuster, Molly	U608501573	Musterkasse	647975	TE	AB, DM2	14.09.2026	18.09.2026	-
Heimmuster, Marcus	R172109408	Musterkasse	605485	TE	KHK, AB	14.09.2026	17.09.2026	-
Heimmuster, Michael	Z653508592	Musterkasse	656137	ED	DM2	01.09.2026	19.09.2026	23.11.2026
Heimmuster, Molly	P368234118	Musterkasse	536774	FD	DM2	17.08.2026	17.09.2026	23.11.2026
Heimmuster, Moritz	L583989399	Musterkasse	944117	ED	DM2	02.09.2026	17.09.2026	23.11.2026
Heimmuster, Moritz	F544557915	Musterkasse	384903	FD	DM2	14.09.2026	19.09.2026	23.11.2026
Heimmuster, Moritz	R765537466	Musterkasse	879237	FD	DM2	14.08.2026	15.09.2026	23.11.2026
Kleinstmuster, Michaela	B980757012	Musterkasse	374102	TE	AB, DM1	11.09.2026	18.09.2026	-
Kleinstmuster, Michaela	I153864957	Musterkasse	480230	FD	DM2	11.09.2026	17.09.2026	23.11.2026
Musterfrau, Martha	I229151814	Musterkasse	672538	FD	DM2	11.09.2026	19.09.2026	23.11.2026
Mustermann, Markus	U47366895	Musterkasse	605763	ED	DM2	04.09.2026	19.09.2026	23.11.2026
Mustermann, Markus	D872049511	Musterkasse	619096	FD	DM2	11.09.2026	19.09.2026	23.11.2026
Muster, Margoth	E871618095	Musterkasse	795586	ED	DM2	15.09.2026	17.09.2026	23.11.2026
Muster, Margoth	I344059240	Musterkasse	753272	FD	DM2	29.07.2026	17.09.2026	23.11.2026
Muster, Micky	M137356752	Musterkasse	465850	FD	DM2	14.09.2026	16.09.2026	23.11.2026
Musterson, Maria	V728458504	Musterkasse	675977	TE	KHK, AB, DM1	10.09.2026	17.09.2026	-
Musterson, Martin	F394614262	Musterkasse	145313	FD	DM2	11.09.2026	17.09.2026	23.11.2026
Randmuster, Manuela	M995727493	Musterkasse	771907	FD	DM2	26.08.2026	18.09.2026	23.11.2026
Randmuster, Margoth	I940947652	Musterkasse	374318	FD	DM2	10.08.2026	19.09.2026	23.11.2026
Randmuster, Maria	L507142443	Musterkasse	290892	FD	DM2	11.09.2026	16.09.2026	23.11.2026
Randmuster, Max	L907483050	Musterkasse	473615	FD	DM2	11.09.2026	18.09.2026	23.11.2026
Von Muster, Micky	L925055488	Musterkasse	408755	FD	DM2	10.09.2026	17.09.2026	23.11.2026

Datum Beleg = Ausstellungsdatum der Dokumentation oder TE
Datum Versand = Postausgangsdatum der Korrekturaufforderung an die Arztpraxis
Fristablauf = spätestster Termin, an dem die Dokumentation angenommen werden kann

Belegtypen: ED = Erstdokumentation,
FD = Folgedokumentation,
TE = Teilnahmeerklärung

AB = Asthma bronchiale
BK = Brustkrebs
COPD = Chronisch obstruktive Lungenerkrankung
DM1 = Diabetes mellitus Typ1
DM2 = Diabetes mellitus Typ2
OPE = Osteoporose
KHK = Koronare Herzkrankheit

Diese Dokumentationen und TE sollten schnellstmöglich an die Datenstelle übermittelt werden.

Übersicht: plausible Dokumentationen und TE der letzten 14 Tage

Patient Name, Vorname	Krankenvers.-nummer	Krankenkasse	DMP-Fall-Nr.	Belegtyp	DMP-Diagnose	Datum Beleg	Datum Prüfung
Doppelmuster, Martina	R261189129	Musterkasse	292821	TE	BK, RKN	07.09.2026	11.09.2026
Fremdmuster, Manuela	P974272824	Musterkasse	639649	TE	BK	02.09.2026	11.09.2026
Fremdmuster, Michael	X198467201	Musterkasse	404546	FD	DM2	28.08.2026	15.09.2026
Fremdmuster, Micky	R362451027	Musterkasse	952950	TE	BK	08.09.2026	11.09.2026
Großmuster, Martha	Z619673120	Musterkasse	849412	TE	AB, DM2	15.09.2026	15.09.2026
Kleinmuster, Maria	J49336050	Musterkasse	408395	FD	DM2	04.09.2026	15.09.2026
Kleinmuster, Maria	L227250112	Musterkasse	588108	FD	DM2	09.09.2026	15.09.2026
Kleinmuster, Martina	K223889751	Musterkasse	62781	FD	BK	11.09.2026	11.09.2026
Kleinmuster, Moritz	Z310756460	Musterkasse	109723	FD	DM2	27.08.2026	15.09.2026
Musterberg, Manuela	T680232605	Musterkasse	785330	FD	DM2	14.09.2026	15.09.2026
Musterfrau, Marcus	R49611561	Musterkasse	552725	FD	DM2	03.09.2026	15.09.2026
Musterfrau, Max	S577385431	Musterkasse	538897	FD	BK	14.09.2026	14.09.2026
Musterfrau, Michael	T791499651	Musterkasse	77726	FD	DM2	09.09.2026	15.09.2026
Mustermann, Manuela	Y956928947	Musterkasse	92387	FD	BK	10.09.2026	10.09.2026
Musterson, Martin	V454166578	Musterkasse	665929	FD	DM2	14.09.2026	15.09.2026
Musterson, Max	Y50537093	Musterkasse	438779	TE	KHK, AB, DM1	27.08.2026	15.09.2026
Musterson, Maximilian	R9471041	Musterkasse	543891	FD	DM2	28.08.2026	15.09.2026
Musterson, Molly	X930383992	Musterkasse	861086	FD	DM2	31.08.2026	15.09.2026
Randmuster, Martha	Q216329588	Musterkasse	655102	TE	BK	10.09.2026	11.09.2026
Randmuster, Michaela	J306681944	Musterkasse	114211	FD	DM2	04.09.2026	15.09.2026
Randmuster, Michelle	G223126177	Musterkasse	355836	TE	KHK, AB	08.09.2026	15.09.2026
Randmuster, Molly	P590299384	Musterkasse	975314	TE	AB, DM1	21.08.2026	15.09.2026
Randmuster, Molly	P206905470	Musterkasse	395789	FD	BK	14.09.2026	14.09.2026
Randmuster, Moritz	N554544240	Musterkasse	231703	FD	DM2	09.09.2026	15.09.2026
Von Muster, Marcus	X512756184	Musterkasse	128280	FD	DM2	03.09.2026	15.09.2026

Datum Beleg = Ausstellungsdatum der Dokumentation oder TE

Datum Prüfung = Datum der Plausibilitätsprüfung

Belegtypen: ED = Erstdokumentation,
FD = Folgedokumentation,
TE = Teilnahmeerklärung**Diese Dokumentationen und TE sind gültig. Bitte prüfen Sie die Auflistung auf Vollständigkeit.**

AB	= Asthma bronchiale
BK	= Brustkrebs
COPD	= Chronisch obstruktive Lungenerkrankungen
DM1	= Diabetes mellitus Typ1
DM2	= Diabetes mellitus Typ2
OPE	= Osteoporose
KHK	= Koronare Herzkrankheit

Übersicht: fehlende Erstdokumentationen

Patient Name, Vorname	Krankenvers.- nummer	Krankenkasse	DMP- Fall-Nr.	DMP- Diagnose	Fehlender Beleg
Doppelmuster, Martha	A366472077	Musterkasse	134112	BK	ED
Fremdmuster, Marcus	H197126016	Musterkasse	151370	KHK	ED
Fremdmuster, Michelle	F661831589	Musterkasse	268756	KHK	ED
Großmuster, Manuela	Q682740658	Musterkasse	942171	BK	ED
Großmuster, Marcus	U138571864	Musterkasse	810353	KHK	ED
Großmuster, Marcus	X640334442	Musterkasse	862085	KHK	ED
Heimmuster, Maria	O615528287	Musterkasse	155107	KHK	ED
Heimmuster, Michael	P562360063	Musterkasse	338404	KHK	ED
Heimmuster, Michelle	E247808629	Musterkasse	372058	KHK	ED
Heimmuster, Molly	B280098772	Musterkasse	493254	KHK	ED
Kleinstmuster, Marcus	Y253353024	Musterkasse	404103	KHK	ED
Kleinstmuster, Max	N335233610	Musterkasse	887290	BK	ED
Kleinstmuster, Maximilian	O874260055	Musterkasse	915532	BK	ED
Musterberg, Michelle	T317434796	Musterkasse	63515	KHK	ED
Mustermann, Michaela	D273687001	Musterkasse	664921	KHK	ED
Mustermann, Micky	S181871261	Musterkasse	426755	KHK	ED
Muster, Martina	M44211738	Musterkasse	594867	KHK	ED
Musterson, Marcus	J386359985	Musterkasse	112545	BK	ED
Randmuster, Martha	I42854561	Musterkasse	327758	KHK	ED
Randmuster, Martin	B880933411	Musterkasse	458287	BK	ED
Randmuster, Max	V739857000	Musterkasse	236550	KHK	ED
Randmuster, Maxi	I362731444	Musterkasse	133517	BK	ED
Von Muster, Margoth	C840913584	Musterkasse	291595	BK	ED
Von Muster, Max	J14453573	Musterkasse	699785	KHK	ED
Von Muster, Michael	D408615052	Musterkasse	951156	BK	ED

Fehlender Beleg = Dokumentation, welche für die Wirksamkeit der Einschreibung fehlt
Belegtypen: ED = Erstdokumentation

Für die aufgeführten Patienten fehlt eine aktuelle Erstdokumentation. Bitte reichen Sie diese umgehend ein. Ursache für eine fehlende Erstdokumentation kann eine zwischenzeitliche Fallbeendigung für einen Patienten sein. Gegebenenfalls könnte auch eine Teilnahmeerklärung fehlen. Ein Abgleich in diesem Zusammenhang erfolgte nicht.

AB = Asthma bronchiale
BK = Brustkrebs
COPD = Chronisch obstruktive
Lungenerkrankungen
DM1 = Diabetes mellitus Typ1
DM2 = Diabetes mellitus Typ2
OPE = Osteoporose
KHK = Koronare Herzkrankheit

Übersicht: zu erstellende Folgedokumentationen im laufenden Quartal (Reminder)

Patient Name, Vorname	Krankenvers.-nummer	Krankenkasse	DMP-Fall-Nr.	Belegtyp	DMP-Diagnose	Datum Beleg	Dokumentationsintervall
Doppelmuster, Martina	N875663107	Musterkasse	474531	FD	KHK	14.06.2026	3 Monate
Doppelmuster, Max	N45708896	Musterkasse	450088	FD	KHK	14.06.2026	3 Monate
Doppelmuster, Maximilian	K32257238	Musterkasse	401679	FD	KHK	03.06.2026	3 Monate
Doppelmuster, Michelle	D33878752	Musterkasse	893175	FD	KHK	14.12.2025	6 Monate
Fremdmuster, Molly	M248016566	Musterkasse	663980	FD	KHK	09.12.2025	6 Monate
Großmuster, Margda	Y375582850	Musterkasse	649338	FD	KHK	10.12.2025	6 Monate
Großmuster, Margoth	O321554605	Musterkasse	8703	FD	KHK	08.06.2026	3 Monate
Großmuster, Margoth	Y277736012	Musterkasse	42261	FD	KHK	14.12.2025	6 Monate
Großmuster, Maximilian	Z51362287	Musterkasse	613405	FD	KHK	10.06.2026	3 Monate
Heimmuster, Maximilian	D830474788	Musterkasse	420580	FD	KHK	09.06.2026	3 Monate
Heimmuster, Micky	P58459296	Musterkasse	540276	FD	KHK	03.06.2026	3 Monate
Heimmuster, Molly	K618049952	Musterkasse	149689	FD	KHK	14.12.2025	6 Monate
Kleinstmuster, Maxi	O991173594	Musterkasse	859788	FD	KHK	01.06.2026	3 Monate
Kleinstmuster, Michelle	A401949659	Musterkasse	536382	FD	KHK	14.06.2026	3 Monate
Muster, Margoth	D164292841	Musterkasse	424762	FD	KHK	10.12.2025	6 Monate
Muster, Maria	D807032876	Musterkasse	570079	FD	KHK	10.06.2026	3 Monate
Muster, Martina	R371980401	Musterkasse	374331	FD	KHK	07.06.2026	3 Monate
Muster, Micky	N594995299	Musterkasse	733913	FD	KHK	10.06.2026	3 Monate
Musterberg, Marcus	E328414997	Musterkasse	417943	FD	KHK	27.05.2026	3 Monate
Mustermann, Michelle	Y948568402	Musterkasse	905513	FD	KHK	11.06.2026	3 Monate
Musterson, Marcus	O494637009	Musterkasse	952579	FD	KHK	11.06.2026	3 Monate
Randmuster, Martina	L542145179	Musterkasse	784449	FD	KHK	09.06.2026	3 Monate
Randmuster, Max	Z845286539	Musterkasse	748121	FD	KHK	10.12.2025	6 Monate
Von Muster, Maxi	Y402082029	Musterkasse	864657	FD	KHK	28.05.2026	3 Monate
Von Muster, Moritz	I41766156	Musterkasse	535203	FD	KHK	10.06.2026	3 Monate

Datum und Intervall beziehen sich auf die letzte Dokumentation zu diesem DMP-Fall.
 3 Monate = jedes Quartal 6 Monate = jedes 2. Quartal 12 Monate = Jährlich

Datum Beleg = Ausstellungsdatum der Dokumentation

Belegtypen:

ED = Erstdokumentation,
 FD = Folgedokumentation

AB = Asthma bronchiale
 BK = Brustkrebs
 COPD = Chronisch obstruktive Lungenerkrankungen
 DM1 = Diabetes mellitus Typ1
 DM2 = Diabetes mellitus Typ2
 OPE = Osteoporose
 KHK = Koronare Herzkrankheit

Nach dem Ende der Corona-Sonderregelung sind seit dem 01.01.2022 wieder regelmäßig Folgedokumentationen für die Patienten zu erstellen.

Im DMP Brustkrebs beachten Sie dabei bitte die abweichenden Regelungen zum Dokumentationsintervall und prüfen Sie, ob gemäß Anlage 3 Nr. 1.5 DMP-A-RL eine Folgedokumentation zu erstellen ist.

Übersicht: Folgedokumentationen im falschen zeitlichen Kontext

Patient Name, Vorname	Krankenvers.-nummer	Krankenkasse	DMP-Fall-Nr.	Belegtyp	DMP-Diagnose	Datum Beleg	Datum letzter Beleg	Dokuintervall
Doppelmuster, Martina	O333994836	Musterkasse	455992	FD	AB	25.08.2026	29.07.2026	6 Monate
Doppelmuster, Michaela	K444103524	Musterkasse	589001	FD	DM1	31.08.2026	31.07.2026	3 Monate
Doppelmuster, Michelle	M994710487	Musterkasse	923314	FD	DM1	02.09.2026	16.07.2026	3 Monate
Doppelmuster, Micky	O737417347	Musterkasse	521815	FD	DM1	02.09.2026	22.07.2026	3 Monate
Doppelmuster, Molly	M971674583	Musterkasse	213311	FD	DM1	07.09.2026	17.07.2026	3 Monate
Fremdmuster, Martha	D317510105	Musterkasse	552370	FD	AB	26.08.2026	07.07.2026	6 Monate
Fremdmuster, Molly	U460001866	Musterkasse	658541	FD	DM1	03.09.2026	05.07.2026	3 Monate
Großmuster, Max	U479426479	Musterkasse	237220	FD	AB	03.09.2026	08.08.2026	3 Monate
Kleinstmuster, Margda	T665037608	Musterkasse	626682	FD	AB	14.09.2026	11.08.2026	6 Monate
Kleinstmuster, Micky	R325439016	Musterkasse	554182	FD	DM1	29.08.2026	12.07.2026	3 Monate
Kleinstmuster, Molly	Y460416655	Musterkasse	381871	FD	AB	15.07.2026	13.07.2026	6 Monate
Musterberg, Molly	H638381973	Musterkasse	251811	FD	AB	16.07.2026	02.07.2026	6 Monate
Musterfrau, Marcus	T768811019	Musterkasse	163998	FD	DM1	31.08.2026	01.08.2026	3 Monate
Musterfrau, Martin	P738135961	Musterkasse	305021	FD	DM1	31.08.2026	15.07.2026	3 Monate
Musterfrau, Maximilian	B366214138	Musterkasse	563643	FD	DM1	02.09.2026	26.07.2026	3 Monate
Musterfrau, Molly	S887716094	Musterkasse	811242	FD	DM1	31.08.2026	23.08.2026	3 Monate
Musterfrau, Moritz	T659577471	Musterkasse	752228	FD	DM1	02.09.2026	19.07.2026	3 Monate
Mustermann, Margoth	H815433311	Musterkasse	229552	FD	DM1	04.09.2026	08.08.2026	3 Monate
Mustermann, Margoth	H884669958	Musterkasse	108132	FD	DM1	07.09.2026	16.07.2026	3 Monate
Muster, Martha	J831812364	Musterkasse	272479	FD	DM1	02.09.2026	31.07.2026	3 Monate
Muster, Martina	W929247196	Musterkasse	776966	FD	DM1	02.09.2026	20.08.2026	3 Monate
Musterson, Marcus	X926461234	Musterkasse	896942	FD	DM1	31.08.2026	08.07.2026	3 Monate
Randmuster, Markus	M276138559	Musterkasse	174149	FD	AB	11.09.2026	26.08.2026	6 Monate
Randmuster, Maximilian	O64618179	Musterkasse	419824	FD	DM1	31.08.2026	16.07.2026	3 Monate
Von Muster, Manuela	P211733979	Musterkasse	870197	FD	DM1	03.09.2026	11.07.2026	3 Monate

Datum Beleg = Ausstellungsdatum der Dokumentation
Belegtyp: FD = Folgedokumentation

Datum letzter Beleg = Ausstellungsdatum der zuvor vorliegenden Dokumentation
Dokuintervall = 3 Monate (jedes Quartal), 6 Monate (jedes 2. Quartal)

AB = Asthma bronchiale
BK = Brustkrebs
COPD = Chronisch obstruktive Lungenerkrankungen
DM1 = Diabetes mellitus Typ1
DM2 = Diabetes mellitus Typ2
OPE = Osteoporose
KKH = Koronare Herzkrankheit

Ursachen für den falschen zeitlichen Kontext können der Eingang von Erstdokumentation und Folgedokumentation im gleichen Dokumentationszeitraum oder der Eingang von zwei Folgedokumentationen von verschiedenen Ärzten im gleichen Dokumentationszeitraum sein.

Übersicht: außerhalb des Übermittlungszeitraumes eingegangene Dokumentationen

Patient Name, Vorname	Krankenvers.-nummer	Krankenkasse	DMP-Fall-Nr.	BS	B.-typ	DMP-Diagnose	Datum Beleg	Datum Eingang	Fristablauf
Doppelmuster, Margoth	F452920525	Musterkasse	884808	P	FD	DM1	13.06.2026	09.09.2026	21.08.2026
Doppelmuster, Martin	F903609984	Musterkasse	287078	P	ED	DM1	05.06.2026	13.09.2026	21.08.2026
Doppelmuster, Maxi	Q52820955	Musterkasse	399194	P	FD	DM1	30.04.2026	31.08.2026	21.08.2026
Fremdmuster, Margda	A599693913	Musterkasse	840361	P	ED	DM1	24.04.2026	29.08.2026	21.08.2026
Fremdmuster, Michael	L426034146	Musterkasse	289362	P	FD	DM1	26.04.2026	29.08.2026	21.08.2026
Fremdmuster, Michael	Z593400084	Musterkasse	53642	P	FD	DM1	31.05.2026	05.09.2026	21.08.2026
Großmuster, Margda	W675109788	Musterkasse	231919	P	ED	DM1	16.06.2026	22.08.2026	21.08.2026
Großmuster, Margoth	W994111634	Musterkasse	379894	P	ED	DM1	06.06.2026	10.09.2026	21.08.2026
Großmuster, Martin	T729477429	Musterkasse	110429	P	FD	DM1	12.04.2026	25.08.2026	21.08.2026
Großmuster, Max	X154327699	Musterkasse	1696	P	ED	DM1	05.04.2026	29.08.2026	21.08.2026
Großmuster, Michael	B927008029	Musterkasse	820796	P	FD	DM1	07.05.2026	27.08.2026	21.08.2026
Großmuster, Michaela	B800276749	Musterkasse	414044	P	FD	DM1	30.04.2026	28.08.2026	21.08.2026
Großmuster, Micky	M709104743	Musterkasse	207677	P	FD	KHK	22.06.2026	29.08.2026	21.08.2026
Heimmuster, Markus	W750444267	Musterkasse	740669	P	ED	DM1	03.04.2026	29.08.2026	21.08.2026
Heimmuster, Martin	E744405629	Musterkasse	833243	P	ED	DM1	28.06.2026	22.08.2026	21.08.2026
Heimmuster, Maxi	J236748483	Musterkasse	497995	P	FD	DM1	26.05.2026	03.09.2026	21.08.2026
Musterberg, Max	X694070704	Musterkasse	321992	P	FD	DM1	30.05.2026	26.08.2026	21.08.2026
Musterfrau, Margda	O320343719	Musterkasse	43254	P	ED	DM1	22.04.2026	05.09.2026	21.08.2026
Musterfrau, Maxi	Z142767034	Musterkasse	144405	P	FD	DM1	23.04.2026	01.09.2026	21.08.2026
Mustermann, Michelle	A361448679	Musterkasse	479731	P	ED	DM1	10.06.2026	03.09.2026	21.08.2026
Muster, Martha	T168409045	Musterkasse	696314	P	ED	DM1	21.06.2026	30.08.2026	21.08.2026
Muster, Martha	H40015491	Musterkasse	838499	P	ED	DM1	07.05.2026	27.08.2026	21.08.2026
Randmuster, Maria	I935177635	Musterkasse	884732	P	FD	DM1	11.04.2026	07.09.2026	21.08.2026
Von Muster, Markus	W722637283	Musterkasse	473358	P	FD	DM1	13.05.2026	03.09.2026	21.08.2026
Von Muster, Martina	L162361637	Musterkasse	89256	P	FD	DM1	29.04.2026	11.09.2026	21.08.2026

Datum Beleg = Ausstellungsdatum der Dokumentation

Datum Eingang = Posteingangsdatum der Dokumentation oder der Korrekturrücksendung (nach Fristende, sodass die Dokumentation nicht gewertet werden kann)

Fristablauf = spätestster Termin, an dem die Dokumentation angenommen werden kann

BS = Belegstatus: P (Beleg plausibel), NP (Beleg nicht plausibel)

B.-typ = Belegtyp: ED = Erstdokumentation, FD = Folgedokumentation

AB = Asthma bronchiale
BK = Brustkrebs
COPD = Chronisch obstruktive Lungenerkrankungen
DM1 = Diabetes mellitus Typ1
DM2 = Diabetes mellitus Typ2
OPE = Osteoporose
KHK = Koronare Herzkrankheit

Diese Dokumentationen können aufgrund der Überschreitung des Übermittlungszeitraumes nicht für die DMP-Prozesse berücksichtigt werden.

Übersicht: Patienten, deren Krankenkasse nicht am DMP teilnimmt

Patient Name, Vorname	Krankenvers.- nummer	Krankenkasse	DMP- Fall-Nr.	Beleg- typ	DMP- Diagnose	Datum Beleg	Datum Prüfung
Doppelmuster, Maximilian	C100242976	Musterkasse	277727	ED	AB	14.09.2026	14.09.2026
Doppelmuster, Micky	Y391234940	Musterkasse	673040	ED	AB	14.09.2026	14.09.2026
Fremdmuster, Maria	P983038716	Musterkasse	102985	TE	AB, DM1	27.08.2026	15.09.2026
Großmuster, Margoth	H478143433	Musterkasse	43519	FD	AB	14.09.2026	15.09.2026
Großmuster, Maria	D593202175	Musterkasse	572186	TE	KHK, AB, DM1	09.09.2026	15.09.2026
Großmuster, Martin	X920170152	Musterkasse	231679	FD	AB	11.09.2026	15.09.2026
Großmuster, Michael	T49608634	Musterkasse	144393	FD	AB	14.09.2026	15.09.2026
Heimmuster, Marcus	J572484190	Musterkasse	321309	FD	AB	15.09.2026	15.09.2026
Heimmuster, Maria	D786851224	Musterkasse	213101	ED	AB	07.09.2026	14.09.2026
Kleinstmuster, Maxi	E179519114	Musterkasse	889591	ED	AB	14.09.2026	14.09.2026
Kleinstmuster, Moritz	W72394435	Musterkasse	23629	FD	AB	14.09.2026	15.09.2026
Musterberg, Margoth	I480554398	Musterkasse	457212	TE	AB, DM2	08.09.2026	15.09.2026
Musterberg, Michelle	Q695339203	Musterkasse	949325	ED	AB	04.02.2026	14.09.2026
Mustermann, Michaela	O129621885	Musterkasse	367586	ED	AB	09.09.2026	14.09.2026
Mustermann, Molly	K843740565	Musterkasse	62573	ED	AB	24.08.2026	14.09.2026
Muster, Martin	S594043951	Musterkasse	809271	FD	AB	10.09.2026	15.09.2026
Muster, Michael	M529037781	Musterkasse	224470	FD	AB	10.09.2026	15.09.2026
Musterson, Maximilian	H992816346	Musterkasse	321181	TE	KHK, AB	27.08.2026	15.09.2026
Randmuster, Martin	H597499223	Musterkasse	785644	ED	AB	20.07.2026	14.09.2026
Randmuster, Maxi	Q553124117	Musterkasse	136907	ED	AB	30.07.2026	14.09.2026
Randmuster, Maximilian	H927786424	Musterkasse	651377	ED	AB	14.09.2026	14.09.2026
Von Muster, Manuela	M641046413	Musterkasse	79712	FD	AB	15.09.2026	15.09.2026
Von Muster, Manuela	G323967552	Musterkasse	977422	ED	AB	14.09.2026	14.09.2026
Von Muster, Martina	V576593238	Musterkasse	481267	FD	AB	14.09.2026	15.09.2026
Von Muster, Moritz	R288232901	Musterkasse	567797	ED	AB	14.09.2026	14.09.2026

Datum Beleg = Ausstellungsdatum der Dokumentation oder TE
Datum Prüfung = Datum der Plausibilitätsprüfung
Belegtypen: ED = Erstdokumentation,
FD = Folgedokumentation,
TE = Teilnahmeerklärung

Diese Dokumentationen und TE werden nicht weiter verarbeitet.

AB = Asthma bronchiale
BK = Brustkrebs
COPD = Chronisch obstruktive
Lungenerkrankungen
DM1 = Diabetes mellitus Typ1
DM2 = Diabetes mellitus Typ2
OPE = Osteoporose
KHK = Koronare Herzkrankheit

Übersicht: nicht prozesskonforme Dokumentationen und TE

Patient Name, Vorname	Krankenvers.-nummer	Krankenkasse	DMP-Fall-Nr.	Belegtyp	DMP-Diagnose	Datum Beleg	Datum Eingang	Grund der Stornierung
Doppelmuster, Martha	K14596386	Musterkasse	62801	ED	COPD	14.09.2026	14.09.2026	39
Doppelmuster, Maximilian	B888019881	Musterkasse	416469	FD	COPD	09.09.2026	15.09.2026	28
Fremdmuster, Margoth	L607455218	Musterkasse	12373	ED	COPD	07.07.2026	14.09.2026	12
Fremdmuster, Maria	B444570070	Musterkasse	337616	ED	AB	14.09.2026	14.09.2026	38
Großmuster, Martina	J348410646	Musterkasse	373849	ED	AB	14.09.2026	14.09.2026	29
Großmuster, Max	H817811567	Musterkasse	664024	ED	AB	14.09.2026	14.09.2026	36
Großmuster, Michael	U302473233	Musterkasse	102919	ED	AB	14.09.2026	14.09.2026	37
Heimmuster, Marcus	B118019747	Musterkasse	754682	TE	COPD	15.03.2025	15.09.2026	40
Kleinmuster, Maximilian	A566829738	Musterkasse	571931	ED	COPD	14.09.2026	15.09.2026	33
Kleinmuster, Moritz	I837954858	Musterkasse	327061	FD	COPD	28.08.2026	15.09.2026	36
Musterberg, Margoth	O698554488	Musterkasse	240717	ED	COPD	07.08.2026	14.09.2026	33
Musterberg, Markus	L141807736	Musterkasse	627617	ED	COPD	28.08.2026	14.09.2026	35
Musterberg, Moritz	R358284738	Musterkasse	249344	ED	AB	10.09.2026	14.09.2026	35
Musterfrau, Margoth	Y594761191	Musterkasse	14268	ED	COPD	10.08.2026	14.09.2026	39
Musterfrau, Martin	E221584228	Musterkasse	54309	ED	COPD	02.09.2026	15.09.2026	38
Musterfrau, Martin	S872572818	Musterkasse	841978	FD	COPD	11.09.2026	15.09.2026	39
Musterfrau, Michael	O714156853	Musterkasse	299944	ED	COPD	14.09.2026	14.09.2026	38
Mustermann, Maximilian	F392914311	Musterkasse	317949	ED	AB	14.09.2026	14.09.2026	39
Muster, Michael	S110358855	Musterkasse	416518	TE	COPD	15.03.2025	15.09.2026	40
Randmuster, Marcus	J885250410	Musterkasse	977369	ED	AB	14.09.2026	14.09.2026	28
Randmuster, Martha	Z896449070	Musterkasse	719959	ED	AB	14.09.2026	14.09.2026	39
Randmuster, Michelle	N968762745	Musterkasse	220942	ED	AB	28.08.2026	14.09.2026	29
Von Muster, Margoth	G756424351	Musterkasse	601033	FD	COPD	03.09.2026	15.09.2026	37
Von Muster, Maria	X50213623	Musterkasse	397674	ED	AB	14.09.2026	14.09.2026	28
Von Muster, Moritz	O849228582	Musterkasse	533087	FD	COPD	10.09.2026	15.09.2026	29

Datum Beleg = Ausstellungsdatum der Dokumentation

Belegtypen: ED = Erstdokumentation,

FD = Folgedokumentation

TE = Teilnahmeerklärung

Stornogründe: 12 - doppelt eingereichte Dokumentationen

17 - Folgedokumentation vor der Erstdokumentation eingegangen

28 - ungültiges Format nach Versionsumstellung

29 - ungültiges Format vor Versionsumstellung

33 - Erstdokumentation im laufenden DMP-Fall (keine Vergütung)

35 - keine Zuordnung zu einem Versicherten bei der Krankenkasse möglich

36 - Löschung im Bestand der Krankenkasse

37 - Dokumentation ohne gültige Teilnahmeerklärung - nicht heilbar

38 - Dokumentation ohne gültige Teilnahmeerklärung - Nachreichung fehlender Teilnahmeerklärung erforderlich

39 - Widerruf der Teilnahmeerklärung durch den Patienten

40 - Verfristung einer nicht gültigen Teilnahmeerklärung nach 18 Monaten

AB = Asthma bronchiale

BK = Brustkrebs

COPD = Chronisch obstruktive Lungenerkrankungen

DM1 = Diabetes mellitus Typ1

DM2 = Diabetes mellitus Typ2

OPE = Osteoporose

KHK = Koronare Herzkrankheit

Diese Dokumentationen und Teilnahmeerklärungen können aus oben genannten Gründen nicht für die DMP-Prozesse berücksichtigt werden. Bitte prüfen Sie bei Stornogrund 33 unter Berücksichtigung unseres Reminders, ob noch eine Folgedokumentation für das laufende Quartal zu erstellen ist.

Übersicht: Fallbeendigungen

Patient Name, Vorname	Krankenvers.- nummer	Krankenkasse	DMP- Fall-Nr.	DMP- Diagnose	Grund der Beendigung	Fallende
Doppelmuster, Maria	W768610080	Musterkasse	389005	OPE	16	15.09.2026
Doppelmuster, Martina	Q387414784	Musterkasse	798979	OPE	15	15.09.2026
Doppelmuster, Michelle	L97040707	Musterkasse	756286	OPE	18	15.09.2026
Doppelmuster, Molly	H609590256	Musterkasse	286229	OPE	03	15.09.2026
Fremdmuster, Markus	S636738701	Musterkasse	19576	OPE	01	15.09.2026
Großmuster, Michael	R922487383	Musterkasse	342255	OPE	02	15.09.2026
Heimmuster, Marcus	Q792082629	Musterkasse	180864	OPE	02	15.09.2026
Kleinmuster, Martina	X461062518	Musterkasse	883501	OPE	20	15.09.2026
Kleinmuster, Michelle	G362824406	Musterkasse	679753	OPE	15	15.09.2026
Kleinmuster, Molly	U17923468	Musterkasse	194550	OPE	03	15.09.2026
Musterberg, Molly	X488761398	Musterkasse	153621	OPE	03	15.09.2026
Musterfrau, Martin	Z512980320	Musterkasse	64988	OPE	05	15.09.2026
Musterfrau, Martin	H643622513	Musterkasse	393515	OPE	18	15.09.2026
Musterfrau, Michael	I831632372	Musterkasse	225462	OPE	18	15.09.2026
Mustermann, Maria	B102765281	Musterkasse	373992	COPD	03	15.09.2026
Muster, Manuela	S665707390	Musterkasse	657004	OPE	16	15.09.2026
Muster, Martha	P780938283	Musterkasse	515628	OPE	18	15.09.2026
Muster, Maxi	I217182713	Musterkasse	268688	OPE	18	15.09.2026
Muster, Maximilian	U950863908	Musterkasse	983953	OPE	03	15.09.2026
Muster, Michael	R913261333	Musterkasse	867289	OPE	03	15.09.2026
Muster, Moritz	F874097575	Musterkasse	135477	COPD	15	15.09.2026
Muster, Moritz	Q115144602	Musterkasse	847034	OPE	03	15.09.2026
Musterson, Margda	Y530466277	Musterkasse	330915	OPE	01	15.09.2026
Musterson, Margoth	Q509030035	Musterkasse	27448	OPE	18	15.09.2026
Von Muster, Maria	D593219439	Musterkasse	626050	OPE	18	15.09.2026

Gründe der Fallbeendigungen:

- 01 - Patient verstorben
- 02 - Patient ausgetreten
- 03 - Patient nicht einschreibefähig
- 05 - Kassenwechsel
- 15 - Arztwechsel
- 16 - verfahrensbedingt durch Krankenkasse
- 18 - zwei fehlende Folgedokumentationen
- 20 - zwei unbegründet abgelehnte Schulungen
- 23 - Rezidivfreiheit älter 10 Jahre

- AB = Asthma bronchiale
- BK = Brustkrebs
- COPD = Chronisch obstruktive Lungenerkrankungen
- DM1 = Diabetes mellitus Typ1
- DM2 = Diabetes mellitus Typ2
- OPE = Osteoporose
- KHK = Koronare Herzkrankheit

Für die aufgeführten Patienten wurden die DMP-Fälle aus oben genannten Gründen beendet.

Übersicht: nicht verarbeitbare Datenlieferungen

Datenlieferung		Hinweise zum Fehler
Eingang	Typ	
18.01.2010	KV-Portal	Datei konnte nicht entschlüsselt werden
Medium / Dateiname		ID: 10891153 0118203351_2_028926882_20100116_1_khk.zip.xkm
18.10.2019	KV-Portal	Datei ist keine DMP-Datei
Medium / Dateiname		ID: 14565321 316642_021974244_20191001114608_1_eHKS.zip.XKM
02.10.2019	KV-Portal	Datei ist keine DMP-Datei
Medium / Dateiname		ID: 14551890 311663_023090998_20191002161748_1_eHKS.zip.XKM
24.09.2019	KV-Portal	Datei ist keine DMP-Datei
Medium / Dateiname		ID: 14531584 307744_028313817_20190923175206_1_eHKS.zip.XKM
05.07.2019	KV-Portal	Datei ist keine DMP-Datei
Medium / Dateiname		ID: 14456310 300930_022292598_20190705125944_1_eHKS.zip.XKM
02.07.2019	KV-Portal	Datei ist keine DMP-Datei
Medium / Dateiname		ID: 14452026 299132_023030298_20190402171203_1_eHKS.zip.XKM
01.07.2019	KV-Portal	Datei ist keine DMP-Datei
Medium / Dateiname		ID: 14449765 297913_028021405_20190630165252_1_eHKS.zip.XKM
18.04.2019	KV-Portal	Datei ist keine DMP-Datei
Medium / Dateiname		ID: 14367151 291697_021450398_20190329111032_1_eHKS.zip.XKM
15.04.2019	KV-Portal	Datei ist keine DMP-Datei
Medium / Dateiname		ID: 14364008 291157_029023787_20190415150738_1_eHKS.zip.XKM 291156_029023787_20190415150738_1_eHKS.zip.XKM
01.04.2019	KV-Portal	Datei ist keine DMP-Datei
Medium / Dateiname		ID: 14349029 284734_023030298_20190102122000_1_eHKS.zip.XKM

Ihre in dieser Anlage aufgeführten DMP-Datenlieferungen können nicht für die Weiterverarbeitung im Sinne der DMP-Prozesse berücksichtigt werden.

Zur Gewährleistung einer lückenlosen Führung Ihrer DMP-Fälle übermitteln Sie uns bitte die betreffenden DMP-Daten erneut.

Plausibilitätsprüfrichtlinie TE/EWE (Stand: 01.10.2026)

Feldname	Prüfung
Name	Der Name des Versicherten muss angegeben sein.
Vorname	Der Vorname des Versicherten muss angegeben sein.
Geburtsdatum	Das Geburtsdatum des Versicherten muss angegeben sein.
Geburtsdatum	Das Geburtsdatum des Versicherten muss zeitlich vor dem Versichertenunterschriftsdatum liegen.
Kostenträgerkennung	Das Institutionskennzeichen der Krankenkasse muss angegeben sein.
Kostenträgerkennung	Die angegebene Krankenkasse muss in dieser Diagnose gemeldet sein. Sofern keine Diagnose ausgewählt wurde, muss die angegebene Krankenkasse in einer Diagnose gemeldet sein.
Versicherten-Nr.	Die Versicherten-Nr. muss angegeben sein.
Versicherten-Nr.	Die Versicherten-Nr. muss 10 Stellen aufweisen.
Versicherten-Nr.	Die Versicherten-Nr. muss mit einem Großbuchstaben beginnen.
Versicherten-Nr.	Die Versicherten-Nr. muss eine korrekte Prüfziffer aufweisen.
Betriebsstätten-Nr.	Die Betriebsstätten-Nr. muss angegeben sein, sofern das Krankenhaus-IK nicht ausgefüllt ist.
Arzt-Nr.	Die Lebenslange Arztnummer muss angegeben sein, sofern das Krankenhaus-IK nicht ausgefüllt ist.
Arzt-Nr.	Die Lebenslange Arztnummer muss in Verbindung mit der Betriebsstätten-Nr. in dieser Diagnose gemeldet sein. Sofern keine Diagnose ausgewählt wurde, muss die Lebenslange Arztnummer in Verbindung mit der Betriebsstätten-Nr. in einer Diagnose gemeldet sein.
Krankenhaus-IK	Das Krankenhaus-IK muss angegeben sein, sofern die die Lebenslange Arztnummer bzw. die Betriebsstätten-Nr. nicht ausgefüllt ist.
Krankenhaus-IK	Das Krankenhaus-IK muss in dieser Diagnose gemeldet sein. Sofern keine Diagnose ausgewählt wurde, muss das Krankenhaus-IK in einer Diagnose gemeldet sein.
Auswahl Diagnose	Es muss mindestens eine Diagnose angegeben sein.
Auswahl Diagnose	Die Auswahlfelder "Diabetes mellitus Typ 1" und "Diabetes mellitus Typ 2" bzw. "Asthma" und "COPD" bzw. "Koronare Herzkrankheit" und "Herzinsuffizienz" bzw. „Adipositas Erwachsene“ und „Adipositas Kinder u. Jugendliche“ dürfen nicht gleichzeitig angekreuzt sein.
Formularschlüssel	Ein Formularschlüssel muss angegeben sein.
Formularschlüssel	Der Schlüssel des verwendeten Formulars muss gültig sein.
Versichertenunterschriftsdatum	Das Versichertenunterschriftsdatum muss angegeben sein. Bei Nichtvorhandensein ist ersatzweise das Datum des Posteingangs beim Auftragnehmer zu erfassen.
Versichertenunterschriftsdatum	Das Versichertenunterschriftsdatum darf nicht in der Zukunft (nach Posteingang in der Datenstelle) oder vor Beginn des DMP liegen.
Versichertenunterschrift	Die Unterschrift des Versicherten muss vorliegen. Namenszusätze wie i. A. oder i. V. sind nicht zu beachten.
Arztunterschriftsdatum	Das Arztunterschriftsdatum muss angegeben sein. Bei Nichtvorhandensein ist ersatzweise das Datum des Posteingangs beim Auftragnehmer zu erfassen.
Arztunterschriftsdatum	Das Arztunterschriftsdatum darf nicht in der Zukunft (nach Eingang in der Datenstelle) oder vor Beginn des DMP liegen.
Arztunterschrift	Die Unterschrift des Arztes muss vorliegen.
Plausibilisierungsdatum (bei Korrekturen)	Das Plausibilisierungsdatum (jüngstes Arztunterschriftsdatum) muss zeitlich nach dem Arztunterschriftsdatum des Originals liegen.
Plausibilisierungsdatum (bei Korrekturen)	Das Plausibilisierungsdatum (Arztunterschriftsdatum der Korrektur) darf nicht nach dem Datum des Posteingangs der Korrektur bei der Datenstelle liegen.