9. 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 classic,
zugleich handelnd für die Innungskrankenkassen, die dieser Vereinbarung 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 DAVASO 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 25.05.2018 wird der o.g. Vertrag wie folgt geändert:

1. Rubrum

Das Rubrum erhält die in diesem 9. Nachtrag dargestellte Fassung.

2. Begriffsbestimmungen

Im Abschnitt Begriffsbestimmungen werden folgende Definitionen neu gefasst:
„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“,
„DMP-RL - DMP-Richtlinie in der jeweils gültigen Fassung“,
„DMP-A-RL - DMP-Anforderungen-Richtlinie in der jeweils gültigen Fassung “,
„DMP-AF-RL - DMP-Aufbewahrungsfristen-Richtlinie in der jeweils gültigen Fassung “,
„DS-GVO – Datenschutz-Grundverordnung“,
„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“,

3. Anlagenübersicht

Die Anlage 5 wird wie folgt neu benannt:
„Bestimmungen zum Datenschutz und zur Datensicherheit bei der Datenverarbeitung im Auftrag inklusive der Anhänge A-F“

4. Präambel

Der Text wird wie folgt neu gefasst:
„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 Kranken-kassen in Hamburg und die Kassenärztliche Vereinigung Hamburg mit der Krankenhausgesellschaft 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) und
Asthma bronchiale sowie chronisch obstruktive Lungenerkrankungen (COPD) (Juli 2007).

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), der DMP-Anforderungen-Richtlinie (DMP-A-RL), der DMP-Richtlinie (DMP-RL) und der DMP-Aufbewahrungsfristen-Richtlinie (DMP-AF-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“

5. § 4 Aufgabenbeschreibung

Der Absatz 2 wird wie folgt neu gefasst:

„Die in Anlage 1 beschriebenen Dienstleistungen werden unter Berücksichtigung der Anforderungen der DMP-A-RL, DMP-RL, DMP-AF-RL, RSAV sowie des SGB X und der DS-GVO in ihrer jeweils geltenden Fassung erbracht.“

6. § 6 Statusdatensatz/Workflow-Daten

Im letzten Satz wird das Wort „gültige“ durch das Wort „beauftragte“ ersetzt.

7. § 8 Grundsätze der Leistungserbringung

a) In Absatz 2 werden nach den Wörtern „datenschutzrechtliche Bestimmungen“ die Wörter „gemäß Anlage 5“ eingefügt.
b) Im Absatz 3 Satz 3 werden nach dem Wort „Vertrag“ die Wörter „sowie Anlage 5“ eingefügt.

8. § 9 Absatz 1 Änderung der zu erbringenden Leistungen

Im letzten Satz wird das Wort „gültigen“ durch das Wort „beauftragten“ ersetzt.

9. § 10 Datenschutzmaßnahmen, Subunternehmer

§ 10 wird wie folgt neu gefasst:

(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 fünfzehn Jahre, beginnend mit dem auf das Berichtsjahr folgenden Kalenderjahr. 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.“

10. § 12 Pflichten der Auftraggeber

Absatz 4 wird ersatzlos gestrichen. Der bisherige Absatz 5 wird zu Absatz 4.

11. § 14 Prüfung der Datenstelle und Prüfung der Versichertenzeiten nach § 42 RSAV

Im Absatz 2 werden die Wörter „gemäß Anlage 5“ nach dem Wort „Verpflichtungen“ eingefügt.

12. § 22 Pflichtverletzung, Haftung

In Absatz 2 Satz 2 werden nach dem Wort „Vertrages“ die Wörter „sowie Anlage 5“ eingefügt.

13. Anlage 1 „Aufgabenbeschreibung für die Datenstelle“

Die Anlage „Aufgabenbeschreibung für die Datenstelle“ wird durch die anliegende gleichnamige Anlage ersetzt.

14. Anlage 1 Anhang 3 „eDMP: Kurzbeschreibung DMPonline“

Der Anhang „eDMP: Kurzbeschreibung DMPonline“ wird durch die anliegende gleichnamige Anlage ersetzt.

15. **Anlage 1 Anhang 3a „eDMP: Antragsformular DMPonline“**
    Der Anhang „eDMP: Antragsformular DMPonline“ wird durch die anliegende gleichnamige Anlage ersetzt.

16. **Anlage 2 „Kommunikationsmatrix“**
    Die Anlage „Kommunikationsmatrix“ wird durch die anliegende gleichnamige Anlage ersetzt.

17. **Anlage 3 „Verarbeitung von TE/EWEs gem. Abschnitt 2.4 der Aufgabenbeschreibung“**
    Die Anlage „Verarbeitung von TE/EWEs gem. Abschnitt 2.4 der Aufgabenbeschreibung“ wird durch die anliegende gleichnamige Anlage ersetzt.

18. **Anlage 5 „Regelungen zum Datenschutz inklusive der Anhänge A bis C“**
    Die Anlage „Regelungen zum Datenschutz inklusive der Anhänge A bis C“ wird durch die anliegende Anlage „Bestimmungen zum Datenschutz und zur Datensicherheit bei der Datenverarbeitung im Auftrag inklusive der Anhänge A bis F“ ersetzt.

Hamburg, den 24.05.2018

.....
Kassenärztliche Vereinigung Hamburg*

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

.....
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

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 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 sind nur Formulare gemäß Anlage 3 des Datenstellenvertrages zugelassen.

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 lmages 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 für 15 Jahre, beginnend mit dem dem Berichtsjahr folgenden Kalenderjahr, zu archivieren sind;
- die eingesetzten Archivierungstechnologien den aktuellen Erkenntnissen zur Haltbarkeit/Datensicherheit entsprechen und eine verlustfreie Rekonstruktion der erfassten Daten zulassen;
- nach Ablauf von 15 Jahren, beginnend mit dem dem Berichtsjahr folgenden Kalenderjahr, 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 auf Datenträgern (CD-ROM, Diskette, DVD) oder elektronisch (KV-Portal, DMPonline, KV Connect[1]) an die Datenstelle übersandt. Eine Übermittlung per Datenträger ist nur bis zum 31.12.2018 zulässig. 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 nach dem 31.12.2018 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 auf Datenträgern oder elektronisch übermittelten Dokumentationsdaten in ihr EDV-System. Dabei dokumentiert sie elektronisch den Eingang der einzelnen Dokumentationen.

Sofern Dokumentationen auf Datenträgern (nur bis 31.12.2018 zulässig) übermittelt werden, stellt die Datenstelle sicher, dass die Versandumschläge solange zusammen mit dem Datenträger aufgehoben werden, bis eine Identifikation des absendenden Arztes vorgenommen werden konnte.

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,

[1] In der Übergangsphase bis zur Realisierung der Telematik-Infrastruktur durch die gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH können am DMP teilnehmende Ärzte in Hamburg auch dieses DFÜ-Verfahren nutzen.

informiert die Datenstelle die Hersteller der Arztpraxissoftware, die Geschäftsstelle der Arbeitsgemeinschaft DMP sowie die KVH über die bestehende Problematik.

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 zu übermitteln. Dabei sind dem Arzt insbesondere die Vorteile der elektronischen Dokumentationsübermittlung (KV-Portal, DMPonline, KV-Connect) vorzustellen. 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 für 15 Jahre, beginnend mit dem dem Berichtsjahr folgenden Kalenderjahr, zu archivieren sind;

- 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 von 15 Jahren, beginnend mit dem auf das Berichtsjahr folgenden Kalenderjahr, die archivierten Belege, Images bzw. Datensätze unverzüglich zu vernichten bzw. zu löschen sind; spätestens aber innerhalb eines Zeitraums von 6 Monaten nach Beauftragung;
- 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 bis zum 31.12.2018 übermittelten Datenträger (Diskette, CD-ROM, DVD) werden nach erfolgreicher Datenzuordnung 6 Jahre aufbewahrt und im Anschluss vernichtet;
- die nach dem 31.12.2018 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. Dabei dokumentiert sie insbesondere bekannt gewordene Arztnummernwechsel im zeitlichen Kontext für die bis zum 30.06.2008 gültige Arztnummernsystematik. 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. Zusätzlich stellt die Geschäftsstelle der Arbeitsgemeinschaft DMP der Datenstelle Listen der am DMP-Brustkrebs teilnehmenden Krankenhäuser zur Verfügung.

Bei Dokumentationen, die ab dem 01.07.2008 erstellt werden, 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 Dokumentationszeitraums. 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 unplausiblem 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.

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 Chiffrat (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 § 42 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 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 § 42 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.

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 datenannehmende Stelle übermittelt werden.

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

5.2 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 elektro-

nisch 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.

5.2.1 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 Anzahl der 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 nach o. g. Aufstellung zur Verfügung gestellt.

5.2.2 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.

5.3 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.

5.4 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.

5.5 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. § 42 RSAV

Nachfolgend werden die Aufgaben der Datenstelle zur Vorbereitung der Prüfung nach § 42 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 § 42 RSAV relevanten Unterlagen

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

Die Krankenkassen fordern die zur Durchführung der Prüfung nach § 42 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.);

- bei Erstdokumentationen mit einem Ersterstell- oder Korrekturdatum vor dem 01.01.2012: vom Arzt unterschriebene Versandlisten oder Bestätigungsschreiben als Kopien oder als Images (ohne qualifizierte elektronische Signatur) inklusive Rückseite, sofern dort Angaben vorhanden (Die Schwärzung von gegebenenfalls weiteren in den Listen aufgeführten Versicherten anderer Krankenkassen ist erforderlich.).

Images werden auf einer CD-ROM oder per elektronischer Übermittlung (FTP-Server) 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 § 42 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 Empfangsbekenntnis 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 § 42 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 lückenlose 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, 5 Wochen nach Abschluss des Quartals, elektronisch einen arztbezogenen Nachweis der plausibel, vollständig und fristgerecht eingegangenen Dokumentationen. Die Auswertung ist spätesten 8 Wochen nach Ablauf des Quartals an die KVH zu übermitteln.

Weiterhin erstellt die Datenstelle, getrennt nach DMP, für jedes Quartal unter Angabe der Krankenversichertennummern, frühestens 8 Wochen nach Ablauf des Quartals, elektronisch einen arztbezogenen Nachweis der Dokumentationen, die innerhalb der Frist (vgl. Punkt 3.5) nicht vollständig und plausibel vorlagen.

Die Auswertungen sind spätestens 8 Wochen nach Ablauf des 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 3 zur Anlage 1 zum Datenstellenvertrag i.d.F. des 9. Nachtrags vom 25.05.2018 für die Region Hamburg

Kurzbeschreibung DMPonline

- Voraussetzung: Zur Teilnahme an diesem Verfahren stellt der DMP-Arzt einen formlosen schriftlichen Antrag (auch per Email / Online möglich) bei der Datenstelle. Nach Überprüfung durch die Datenstelle werden der Praxis die Zugangsdaten (Benutzername und Kennwort) schriftlich zugestellt.

- Der koordinierende Arzt meldet sich mit Benutzernamen und Kennwort im geschützten Internetbereich der Datenstelle an (https://dmponline.inter-forum.de) 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)

DAVASO 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 DAVASO 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.

Datum Unterschrift **und** Arztstempel

Anlage 2 zum Datenstellenvertrag i.d.F. des 9. Nachtrags vom 25.05.2018 für die Region Hamburg
Kommunikationsmatrix
Information der koordnierenden Ärzte, KVH und Krankenkassen
Stand: 25.05.2018

Nr.	Information	Details/ Besonderheiten	Frequenz/ Zeitpunkt	Empfänger		
				Arzt	KVH	KKen
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 Übermittlungszeitraumes 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	**Folgedokumentations-reminder:** 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 Krankenkassen mittels Statusdatensatz	wöchentlich		x	x
11	**Irrläufer** unbekannte Krankenkasse	Info an jeweiligen Verband der KK	wöchentlich			x
12	**Lieferung beleghafter TE/EWE im Original**		zweimal wöchentlich			x
13	**Export von Dokumentationsdaten**		wöchentlich			x
14	**KVH-Abrechnung:** Vorliegende Belege, des Vor-quartals, die vollständig und plausibel bzw. vertrags-konform sind	Erstellung unter Berück-sichtigung aller Belege eines Quartals	quartalsweise nach Abschluss Vorquartal (nach 8 Wochen)		x	

Nr.	Information	Details/ Besonderheiten	Frequenz/ Zeitpunkt	Empfänger		
				Arzt	KVH	KKen
15	**KVH-Abrechnung:** Verfristeter Eingang einer Dokumentation		quartalsweise nach Abschluss Vorquartal (nach 8 Wochen)		x	
16	**KVH-Abrechnung:** Außerhalb des Dokumentationszeitraums erstellte Folgedokumentationen		quartalsweise nach Abschluss Vorquartal (nach 8 Wochen)		x	
17	**Online-Retrieval-System:** Belegeingangsstatistik		wöchentlich		x	x

Verarbeitung von TE/EWEs gem. Abschnitt 2.4 der Aufgabenbeschreibung

Gem. Punkt 2.4 der Aufgabenbeschreibung des Datenstellenvertrages sind nachfolgend aufgeführte TE/EWEs von der Datenstelle zu verarbeiten:

- TE/EWE Diabetes (Formularschüssel 010F)
- TE/EWE Brustkrebs (Formularschüssel 020E)
- TE/EWE KHK (Formularschüssel 030D)
- TE/EWE Asthma (Formularschlüssel 050C)
- TE/EWE COPD (Formularschlüssel 060D)
- TE/EWE indikationsübergreifend (Formularschlüssel 070C)

Werden Teilnahmeerklärungen mit Hilfe einer Praxissoftware erstellt und entsprechen diese inhaltlich den oben benannten Formularen, sind diese ebenso anzunehmen und zu verarbeiten. Fehlt lediglich der Formularschlüssel, sind die Formulare ebenso zu verarbeiten.

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

Inhalt

Präambel

Diese Datenschutzbestimmungen legen die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus dem Datenstellenvertrag zur Durchführung der Disease-Management-Programme in Hamburg (im Folgenden Hauptvertrag genannt) beschriebenen Auftragsverarbeitung ergeben fest. Sämtliche in diesen Datenschutzbestimmungen beschriebenen Verpflichtungen finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiterinnen und Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen bzw. kommen können.
Diese Datenschutzbestimmungen regeln den Schutz der Daten bei der Datenverarbeitung im Auftrag unter besonderer Berücksichtigung des Art. 28 DS-GVO und des § 80 SGB X.

§ 1 Grundsätze

(1) Geschäftsgrundlage des Rechtsverhältnisses zwischen Auftragnehmer und Auftraggeber ist, dass der Datenschutz beim Auftragnehmer nach der Art der zu verarbeitenden Daten den Anforderungen genügt, die für den Auftraggeber gelten.

(2) Der Auftraggeber, 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 Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen, vgl. § 10 (Kontrollrechte des Auftraggebers).

§ 2 Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten werden im Hauptvertrag (siehe Anlage 1 des Hauptvertrages) konkret beschrieben.

(2) Gegenstand der Datenverarbeitung sind folgende Datenarten:

- Stammdaten (z.B. Name, Vorname, Geburtsdatum)
- Adressdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Leistungs-/Gesundheitsdaten (medizinische Daten gemäß jeweils aktueller DMP-A-RL)

(3) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Versicherte
- Leistungserbringer (z.B. koordinierender Arzt)
- Beschäftigte

§ 3 Verantwortlichkeit

(1) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Ziff. 7 DS-GVO).

(2) Die Inhalte dieser Datenschutzbestimmungen gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

(3) Auftraggeber sowie Auftragnehmer müssen gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Dazu müssen alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, auf das Datengeheimnis verpflichtet und über ihre Datenschutzpflichten belehrt werden. Dabei ist jede Partei für die Verpflichtung des eigenen Personals zuständig. Ferner müssen die eingesetzten Personen darauf hingewiesen werden, dass das Datengeheimnis auch nach Beendigung der Tätigkeit fortbesteht.

(4) Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

§ 4 Allgemeine Pflichten des Auftragnehmers

(1) Dem Auftragnehmer ist die Verarbeitung von Daten nur zum Zwecke der Erfüllung des Hauptvertrages sowie im Rahmen der schriftlichen Weisungen des Auftraggebers und nach den datenschutzrechtlichen Vorschriften unter Beachtung der technischen und organisatorischen Maßnahmen gem. § 5 dieser Bestimmungen gestattet. Der Auftragnehmer verwendet die Daten und die daraus erzielten Verarbeitungsergebnisse ausschließlich für die Erfüllung des Hauptvertrages. 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 Auftragnehmer verpflichtet sich, dass die Daten des jeweiligen Auftraggebers von Daten anderer Auftraggeber streng getrennt werden. Er verpflichtet sich, keine Kopien oder Duplikate der Datenbestände bzw. Datenbanken ohne Wissen des Auftraggebers 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 Auftragnehmer bestellte Datenschutzbeauftragte (vgl. Art. 37 DS-GVO) bzw. die Person in der Geschäftsleitung, die für die Überwachung der Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich ist, ist in **Anhang A** mit Anschrift und telefonischer und elektronischer Erreichbarkeit benannt. Soweit der Auftragnehmer nach den für ihn maßgeblichen nationalen Datenschutzgesetzen keinen Datenschutzbeauftragten zu bestellen hat, benennt er dem Auftraggeber darüber hinaus die für die Überwachung der Einhaltung der datenschutzrechtlichen Bestimmungen maßgebliche nationale Kontrollbehörde.

(4) Der Auftragnehmer hat den für die Verarbeitung der Sozialdaten des Auftraggebers im Rahmen des Auftragsverhältnisses vorgesehenen Standort/Standorte seiner Geschäftsräume dem Auftraggeber vor Vertragsschluss in **Anhang B** schriftlich zu benennen. Eine Veränderung der Standorte oder Räumlichkeiten, in denen Daten des Auftraggebers verarbeitet werden, oder ein Verlagern der Auftragsdurchführung an eine andere Örtlichkeit als die mit dem Auftraggeber vereinbarte, bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers.

(5) Der Auftragnehmer stellt sicher, dass ein Zugriff auf die Daten des Auftraggebers von Betriebsstätten/ Geschäftsräumen und anderen Orten außerhalb der in **Anhang B** angegebenen Standorte des Auftragnehmers grundsätzlich ausgeschlossen ist.

(6) Eine Verarbeitung von Sozialdaten des Auftraggebers unter Nutzung mobiler Arbeitsplätze/ Heim- oder Telearbeitsplätze findet nicht statt.

(7) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in Deutschland statt. Jede Verlagerung in ein Drittland bedarf der

vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

(8) Der Auftragnehmer ist verpflichtet, den Auftraggeber zu informieren, wenn Aufsichtsbehörden nach § 40 BDSG tätig werden oder eine zuständige Behörde beim Auftragnehmer oder seinen Unterauftragnehmern ermittelt. Die unverzügliche Information des Auftraggebers 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 personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(9) Der Auftragnehmer ist verpflichtet, den Auftraggeber bei dessen nach Artikel 35 DS-GVO entstehenden Pflichten in Zusammenhang mit Datenschutz-Folgenabschätzung zu unterstützen.

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

§ 5 Technische und organisatorische Maßnahmen

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

(2) Der Auftraggeber verarbeitet in der Regel nur Daten, die einem hohen bis sehr hohem Schutzbedarf nach den Klassifikationen der IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) unterliegen. Der Auftragnehmer trägt daher die Gewähr dafür, dass die hierzu erforderlichen technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit getroffen sind und eingehalten werden. Die in **Anhang C** beschriebenen Maßnahmen sind dabei der Mindeststandard.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Abweichungen oder Veränderungen sind nur zur Verbesserung des Datenschutzes und der Datensicherheit zulässig. Insoweit darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(4) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe geforderten technischen und organisatorischen Maßnahmen hinsichtlich der konkreten Auftragsdurchführung bestätigt.

(5) Der Auftragnehmer stellt dem Auftraggeber auf Anforderung vorhandene Datenschutz- und Sicherheitskonzepte für das Auftragsverhältnis zur Verfügung. In den Konzepten sind insbesondere die Verarbeitungsschritte der Erhebung, Verarbeitung und Nutzung der Daten des Auftraggebers näher zu beschreiben.

(6) Der Auftragnehmer hat die ergriffenen technischen und organisatorischen Maßnahmen zu dokumentieren und dem Auftraggeber auf Verlangen zur Prüfung zu übergeben.

(7) Soweit die Prüfung des Auftraggebers Feststellungen ergibt, dass die Anforderungen der technischen und organisatorischen Maßnahmen einer sicheren Datenverarbeitung für diesen Vertrag nicht entspricht und sich daher ein Anpassungsbedarf ergibt, so ist diese Anforderung umzusetzen.

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

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

§ 6 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der vertraglichen Regelungen die Bestimmungen gemäß Art. 28 bis 33 DS-GVO sicherzustellen.

Insofern sind insbesondere folgende Anforderungen zu gewährleisten:

(1) Ein Wechsel des Datenschutzbeauftragten/der verantwortlichen Person wird dem Auftraggeber unverzüglich mitgeteilt.

(2) Der Auftragnehmer ist verpflichtet, zur Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2b, 29, 32 Abs. 4 DS-GVO 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 D** beigefügten Muster der Verpflichtungserklärung zur Vertraulichkeit zu entsprechen.

(3) Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu Sozialdaten hat, darf diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass der Auftragnehmer gesetzlich zur Verarbeitung verpflichtet ist.

(4) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Dies gilt auch, soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist.

§ 7 Unterauftragnehmer

(1) Unterauftragnehmer, die für den Auftragnehmer Daten des Auftraggebers verarbeiten, dürfen vom Auftragnehmer nur mit vorheriger, schriftlicher Einwilligung des Auftraggebers eingeschaltet werden. Dies gilt auch für Konzerntöchter. In **Anhang E** sind die Unterauftragnehmer anzugeben. Für bereits bei Zuschlag benannte Unterauftragnehmer gilt die Zustimmung als erteilt.

(2) Soweit im Fall der Beauftragung ein oder mehrere Unterauftragnehmer Daten des Auftraggebers verarbeiten, müssen sowohl der Auftragnehmer als auch der Unterauftragnehmer angeben, welches Aufgabenfeld an welchem Unternehmensstandort ausgeführt werden solle.

(3) Die vertraglichen Vereinbarungen nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zwischen Auftragnehmer und Unterauftragnehmer sind so zu gestalten, dass sie den Bestimmungen des Vertragsverhältnisses zwischen Auftraggeber und Auftragnehmer 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 Auftragnehmer darf nur Unterauftragnehmer einschalten, die die Erbringung der vertraglich vereinbarten Datenverarbeitung ausschließlich in Deutschland betreiben.

(5) Der Auftragnehmer hat sich regelmäßig von der Einhaltung der beim Unterauftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren, mindestens 6 Jahre aufzubewahren und auf Verlangen dem Auftraggeber vorzulegen.

(6) Der Auftragnehmer hat im Vertrag mit dem Unterauftragnehmer den Auftrag, den Arbeitsablauf und die an den 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 Auftraggebers erhoben, verarbeitet oder genutzt werden, zu benennen.

(7) Die vom Auftragnehmer mit dem Unterauftragnehmer geschlossenen Verträge bedürfen der Schriftform und sind dem Auftraggeber auf Verlangen vorzulegen.

(8) Das Verhalten seiner Unterauftragnehmer ist dem Auftragnehmer wie eigenes Verhalten zuzurechnen. Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer nach Maßgabe des Art. 28 Abs. 4 DS-GVO gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes anderen Unterauftragnehmers.

(9) Sollen vom Auftragnehmer während der Vertragslaufzeit andere als in **Anhang E** benannte Unterauftragnehmer beauftragt oder Standorte von Unterauftragnehmern verlegt/erweitert werden, sind dem Auftraggeber

rechtzeitig vor der geplanten Veränderung folgende Unterlagen zur Zustimmung vorzulegen:

a) Beschreibung der Arbeiten, die der Unterauftragnehmer ausführen soll
b) Bericht der letzten Prüfung (nicht älter als 6 Monate)
c) Kopie der geplanten vertraglichen datenschutzrelevanten Regelungen (einschließlich der technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit) mit dem Unterauftragnehmer.

(10) Wenn andere Stellen die Prüfung oder Wartung von automatisierten Verfahren oder von Datenverarbeitungsanlagen vornehmen und dabei ein Zugriff auf die Daten des Auftraggebers nicht ausgeschlossen werden kann, gilt der § 80 Abs. 3 SGB X analog. Derartige Beauftragungen sind dem Auftraggeber 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 F** aufzuführen.

(11) Beauftragt der Auftragnehmer für den Datentransport einen Transportunternehmer, so hat er vertraglich sicherzustellen und dem Auftraggeber auf Verlangen nachzuweisen, dass der Transportunternehmer den Datenschutzbestimmungen Genüge tut. Werden Unterlagen des Auftraggebers abgeholt, stattet der Auftragnehmer den Transportunternehmer mit einem schriftlichen Berechtigungsausweis für die Entgegennahme der Unterlagen aus.

§ 8 Auskunft, Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer ist verpflichtet, den Auftraggeber im Rahmen seiner Pflichten gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Information unverzüglich zur Verfügung zu stellen.

(2) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken.

(3) Wenn von Betroffenen die Rechte gemäß der Art. 15 – 18 DS-GVO i. V. m. §§ 81, 83 und 84 SGB X geltend gemacht werden, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Er stellt sicher, dass die Daten von Betroffenen bei Bedarf auf Anweisung des Auftraggebers berichtigt, gelöscht oder gesperrt werden können.

(4) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

§ 9 Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftraggeber wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z. B. durch Einholung von

Einwilligungserklärungen für die Verarbeitung der Daten) geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen rechtsverletzungsfrei erbringen kann.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Der Auftraggeber ist hinsichtlich der vom Auftragnehmer eingesetzten und vom Auftraggeber genehmigten Verfahren zur automatisierten Verarbeitung personenbezogener Daten datenschutzrechtlich verantwortlich und hat – neben der eigenen Verpflichtung des Auftragnehmers – ebenfalls die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten.

(4) Dem Auftraggeber obliegen die aus Art. 33, 34 DS-GVO resultierenden Informationspflichten gegenüber der Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen.

(5) Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.

(6) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

(7) Der Auftraggeber stellt sicher, dass die aus Art. 32 DS-GVO resultierenden Anforderungen bzgl. der Sicherheit der Verarbeitung seinerseits eingehalten werden. Insbesondere gilt dies für Fernzugriffe des Auftragnehmers auf die Datenbestände des Auftraggebers.

(9) Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten vom Auftraggeber zu tragen. Sofern der vereinbarte Leistungsumfang überschritten wird, ist hierzu vorab eine gesonderte schriftliche Vereinbarung zu treffen.

§ 10 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber oder von ihr beauftragte externe Prüfeinrichtungen werden sich vor Beginn der Auftragsverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen.

(2) Der Auftragnehmer gewährt dem Auftraggeber bzw. den für den Auftraggeber zuständigen Aufsichtsbehörden oder von ihm beauftragte externe Prüfeinrichtungen in den Betriebsräumen des Auftragnehmers zu jeder geschäftsmäßigen Zeit nach vorheriger schriftlicher Ankündigung (ggf. per Telefax / E-Mail) ein Prüfrecht. Das Prüfrecht umfasst die Besichtigung von Grundstücken und Geschäftsräumen, Auskünfte zur Vertragsausführung, Einsicht in Papierunterlagen als auch die Einsichtnahme in die beim Auftragnehmer gespeicherten Sozialdaten des Auftraggebers, soweit dies im Rahmen des Auftrags zur Überwachung von Datenschutz und Datensicherheit erforderlich ist. Dies gilt insbesondere für den Nachweis der Umsetzung der technischen und organisatorischen Maßnahmen.

(3) Der Nachweis technischer und organisatorischer Maßnahmen kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI Grundschutz).

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

(5) Die genannten Rechte des Auftraggebers können auch durch Mitarbeiter von damit beauftragten Fremdfirmen wahrgenommen werden. Sofern Mitarbeiter von Fremdfirmen mit den genannten Kontrollmaßnahmen beauftragt werden, sind diese vom Auftraggeber ausdrücklich auf die Geheimhaltung aller in diesem Zusammenhang erlangten Kenntnisse, Daten sowie Betriebs- und Geschäftsgeheimnisse zu verpflichten.

(6) Die Rechte der für den Auftragnehmer zuständigen Aufsichtsbehörde bleiben davon unberührt.

§ 11 Weisungsbefugnis des Auftraggebers

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers. Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragnehmer eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird. Der Auftragnehmer unterrichtet soweit ihm möglich in derartigen Situationen den Auftraggeber vor Beginn der Verarbeitung über die entsprechenden rechtlichen Anforderungen. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann.

(2) Die Weisungen des Auftraggebers werden vom Auftragnehmer dokumentiert und dem Auftraggeber unmittelbar nach erfolgter Dokumentation als unterschriebene Kopie zur Verfügung gestellt.

(3) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind von der Weisungsbefugnis des Auftraggebers gedeckt und entsprechend zu dokumentieren. Bei einer wesentlichen Änderung des Auftrags steht dem Auftragnehmer ein Widerspruchsrecht zu. Besteht der Auftraggeber trotz des Widerspruchs des Auftragnehmers auf der Änderung, steht dem Auftragnehmer ein ordentliches Kündigungsrecht bezüglich des von der Weisung betroffenen AV-Vertrages sowie der von der AV-Vereinbarung betroffenen Bestandteile des entsprechenden Hauptvertrages zu. Verweigert der Auftragnehmer, die Änderung durchzuführen, steht auch dem Auftraggeber ein ordentliches Kündigungsrecht zu. Erfolgt eine Kündigung, so ist für die restliche Vertragslaufzeit weiterhin die vertraglich vereinbarte Leistung durch den Auftragnehmer zu erbringen.

(4) Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer notiert sich Datum, Uhrzeit

und Person, welche die mündliche Weisung erteilte sowie den Grund, warum keine schriftliche Beauftragung erfolgen konnte.

§ 12 Mitteilungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Verzeichnis über die Datenverarbeitung, Meldepflichten bei Datenpannen, 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 DS-GVO unverzüglich an den Auftraggeber zu melden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung nachteiliger Folgen für die Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(2) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Meinung ist, dass eine Weisung des Auftraggebers gegen die DS-GVO oder eine andere Datenschutzvorschrift verstößt. Der Auftragnehmer ist in diesem Fall berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§ 13 Löschung und Rückgabe von personenbezogenen Daten

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

(2) Auf Verlangen des Auftraggebers hat der Auftragnehmer in seinem Besitz befindliche Daten bzw. Datenbestände (z.B. physische Datenträger, elektronische Dateien oder Datenbanken in seinen DV-Systemen) nichtreproduzierbar zu löschen bzw. physisch zu vernichten. Die Vernichtung hat nach DIN 66399 Teile 1-3 mindestens mit der Schutzklasse 3 mindestens mit Sicherheitsstufe P-4, F-4, O-4, T-4, H-4 bzw. E-4 zu erfolgen. Die Datenlöschung hat nach anerkanntem BSI-Standard (Bundesamt für Sicherheit in der Informationstechnik) oder anderweitiger adäquater Regelung für vertrauliche Daten in der jeweils aktuellen Fassung zu erfolgen. Dies gilt auch für Test- und Zwischenergebnisse. Ist eine Löschung auf Sicherungskopien wegen der besonderen Art der Speicherung nur

mit einem unverhältnismäßig hohen Aufwand möglich, sind die Daten nach Abstimmung mit dem Auftraggeber für jede weitere Verarbeitung einzuschränken.

(3) Die Löschung und Vernichtung hat der Auftragnehmer in geeigneter Weise zu protokollieren und auf Verlangen dem Auftraggeber vorzulegen. Im Zweifelsfall sind geeignete Maßnahmen mit dem Auftraggeber abzustimmen.

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

§ 14 Haftung

(1) Der Auftragnehmer haftet gegenüber dem Auftraggeber nach Maßgabe der gesetzlichen Bestimmungen für Schäden, die infolge seines oder seiner Unterauftragnehmer (§ 7) schuldhaften Verhaltens gegen gesetzliche Datenschutzregelungen und/oder durch die schuldhafte Verletzung dieser Datenschutzbestimmungen entstehen. Das nähere ist im Hauptvertrag geregelt.

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

§ 15 Nebenabreden

Änderungen und Nebenabreden zu diesen Datenschutzbestimmungen bedürfen der Schriftform und sind von beiden Vertragsparteien zu unterschreiben.

§ 16 Laufzeit des Vertrages und Kündigung

(1) Beginn und Ende des Auftragsverhältnisses sind im Hauptvertrag geregelt.

(2) Unabhängig von Abs. 1 unterliegen der Auftragnehmer und dessen eingesetzte Mitarbeiter auch nach dem im Hauptvertrag genannten Vertragsende hinaus hinsichtlich der im Rahmen des Auftragsverhältnisses übermittelten Daten und bekannt gewordenen Vertraulichkeiten der Geheimhaltungspflicht.

(3) Die Verletzung von gesetzlichen oder vertraglichen Datenschutzbestimmungen durch den Auftragnehmer ist ein wichtiger Grund für den Auftraggeber, das im Hauptvertrag vorbehaltene Recht zur außerordentlichen Kündigung auszuüben.

§ 17 Salvatorische Klausel

(1) Sollten einzelne Bestimmungen dieser Datenschutzbestimmungen einschließlich dieser Regelung ganz oder teilweise unwirksam sein oder werden oder sollten die Datenschutzbestimmungen eine Regelungslücke enthalten,

bleibt die Wirksamkeit der übrigen Bestimmungen oder Teile solcher Bestimmungen 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.

§ 18 Inkrafttreten

(1) Diese Bestimmungen zum Datenschutz und zur Datensicherheit bei der Datenverarbeitung im Auftrag treten zum 25.05.2018 in Kraft und ersetzen die bisher gültigen Regelungen zum Datenschutz vom 23.08.2016.

Anhänge:

Anhang A	Datenschutzbeauftragter, IT-Verantwortlicher und IT-Sicherheitsbeauftragter des Auftragnehmers
Anhang B	Standorte der Geschäftsräume des Auftragnehmers
Anhang C	Technische und organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit einschließlich Maßnahmenkatalog
Anhang D	Muster der Verpflichtungserklärung zur Vertraulichkeit
Anhang E	Übersicht über die Unterauftragnehmer
Anhang F	Übersicht über die Wartungsfirmen

Anhang A zur Anlage 5 – Bestimmungen zum Datenschutz und zur Datensicherheit bei der Datenverarbeitung im Auftrag (§ 80 SGB X i.V.m. Art. 28 DS-GVO)

Datenschutzbeauftragter, IT-Verantwortlicher und IT-Sicherheitsbeauftragter des Auftragnehmers

Der Auftragnehmer hat entsprechend Art. 37 DS-GVO einen Datenschutzbeauftragten bestellt:

Wolfgang Leistner
Name des Datenschutzbeauftragten
0341 25920-180
Telefonnummer
datenschutz@davaso.de
E-Mail-Adresse

IT-Verantwortlicher des Auftragnehmers:

Steffen Dunst
Name des IT-Verantwortlichen
0341 259209-7610
Telefonnummer
steffen.dunst@davaso.de
E-Mail-Adresse

Wenn vorhanden: IT-Sicherheitsbeauftragter des Auftragnehmers:

Michael Weigel
Name des IT-Sicherheitsbeauftragten
0341 259209-7022
Telefonnummer
michael.weigel@davaso.de
E-Mail-Adresse

Ort, Datum	Unterschrift und Firmenstempel des Auftragnehmers

Anhang B zur Anlage 5 – Bestimmungen zum Datenschutz und zur Datensicherheit bei der Datenverarbeitung im Auftrag (§ 80 SGB X i.V.m. Art. 28 DS-GVO)

Standorte der Geschäftsräume des Auftragnehmers

Übersicht über die Standorte der Geschäftsräume des Auftragnehmers, in denen die Verarbeitung der Sozialdaten des Auftraggebers im Rahmen des Auftragsverhältnisses stattfinden werden

	Genaue postalische Anschrift, ggf. ergänzend Gebäudeteil, Etage etc.
1. Standort der Geschäftsräume:	Hauptstandort Leipzig-Mölkau Sommerfelder Straße 120 04316 Leipzig ▪ Datenannahme und –verarbeitung
2. Standort der Geschäftsräume:	Standort Taucha Otto-Schmidt-Straße 22 04425 Taucha ▪ Belegarchivierung
3. Standort der Geschäftsräume:	Standort Leipzig-Mockau Am alten Flughafen 1 04356 Leipzig ▪ Datenannahme und –verarbeitung ▪ Belegarchivierung
4. Standort der Geschäftsräume:	Standort Leipzig-Volkmarsdorf Torgauer Platz 1 – 3 04315 Leipzig ▪ Datenverarbeitung (keine Bearbeitung von DMP-Daten)

5. Standort der Geschäftsräume:	Standort Suhl Fröhliche-Mann-Straße 3b 98528 Suhl ▪ Datenverarbeitung (keine Bearbeitung von DMP-Daten)

Leipzig,

Ort, Datum	DAVASO GmbH

Anhang C zur Anlage 5 – Bestimmungen zum Datenschutz und zur Datensicherheit bei der Datenverarbeitung im Auftrag (§ 80 SGB X i.V.m. Art. 28 DS-GVO)

Technische und Organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit bei DAVASO GmbH um das erforderliche Schutzniveau für die Verarbeitung und Nutzung von Daten zu gewährleisten

Angabe und Beschreibung der technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit, die im Einzelfall getroffen wurden, um

- die Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)
- die Integrität (Art. 32 Abs. 1 lit. b DS-GVO)
- die Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

zu gewährleisten sowie

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

sicherzustellen.

Die Maßnahmen sind schriftlich in einem Sicherheitshandbuch oder einer Sicherheitsrichtlinie

☒ festgelegt ☐ nicht schriftlich festgelegt

Bezeichnung: Sicherheitshandbuch

Stand: 25.05.2018

Leipzig,

_____ _____

Ort, Datum DAVASO GmbH

Sicherheitshandbuch

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

Stand: 25.05.2018

Vertraulichkeitsstufe: intern

DAVASO

Ein Unternehmen mit den Marken
INTER-FORUM | Syntela | DAVASO

Inhalt

1 Einleitung

Dieses Sicherheitshandbuch enthält als Datensicherheitskonzept die bei DAVASO 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

DAVASO GmbH
Sommerfelder Straße 120
04316 Leipzig

Telefon:	(+49) 341 25920-0
Fax:	(+49) 341 25920-20
Website:	http://www.davaso.de
Registergericht:	Amtsgericht Leipzig
Registernummer:	HRB 32082
USt-IdNr.:	DE141624398

1.1.2 Vertretungsberechtigte Personen

Jan Schaller (CEO), Hans Günther Nolte (CTO), Georg Schoder (CFO)

1.1.3 Angaben zum Datenschutzbeauftragten

Wolfgang Leistner

Tel.: (+49) 341 25920-80
Fax: (+49) 341 25920-20
E-Mail: datenschutz@davaso.de

1.1.4 Angaben zum Informationssicherheitsbeauftragten

Michael Weigel

Tel.: (+49) 341 25920-99
Fax: (+49) 341 25920-20

1.2 Standorte der Datenverarbeitung

1.2.1 Leipzig-Mölkau

Anschrift:

Sommerfelder Straße 120
04316 Leipzig

Funktion/Beschreibung:

- Zentrale Verwaltung
- Zentrale IT
- 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:

- 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-Mockau

Anschrift:

Am alten Flughafen 1
04356 Leipzig

Funktion/Beschreibung:

- Digitalisierung von Belegen und Abrechnungen im Rahmen der Auftragsverarbeitung
- Kurz- und Langzeitarchivierung von Belegen und Abrechnungen im Rahmen der Auftragsverarbeitung

1.2.4 Leipzig-Volkmarsdorf

Anschrift:

Torgauer Platz 1-3
04315 Leipzig

Funktion/Beschreibung:

- Außenstelle IT (Softwareentwicklung, Qualitätssicherung, Operating, DB-Administration)
- Prüfung von Abrechnungen und Belegen im Rahmen der Auftragsverarbeitung

1.2.5 Suhl

Anschrift:

Fröhliche-Mann-Straße 3b
98528 Suhl

Funktion/Beschreibung:

- Prüfung von Abrechnungen und Belegen im Rahmen der Auftragsverarbeitung

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 muss 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 Sicherheitsbereichs 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 Pförtnerdienst. Der Pförtner kontrolliert bzw. beobachtet die Personenbewegungen an der Pforte. Unbekannte Personen haben sich beim Pförtner auszuweisen. Der Pförtner 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 WLAN.
- Ungesicherte Netzzugänge und die Abschottung des internen Netzes gegenüber dem öffentlichen Netz werden durch eine mehrstufige 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 5 fehlerhaften Passworteingaben 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 viel Rechte wie nötig, so wenig 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 Arbeitslatzes 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 i. S. v. 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).
- Das zur Vernichtung anstehende Material wird in verschlossenen Sicherheitsbehältern bzw. bei Archivmaterial in verschlossenen Großraumcontainern gesammelt.

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 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.

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 berechtigte Empfänger.
- Für Versand und Empfang von Daten und Datenträgern werden stets Verantwortliche bzw. Berechtigte benannt. Die Berechtigten 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 Schreibschutz 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.
- 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 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 Brandfrühesterkennungs- 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 tägliches 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-Switche 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.

4.2 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 Brandfrühesterkennungs- 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 Leistungen.

4.3 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.
- Kurzzeitige Ausfälle bis 5 Minuten (Autonomiezeit) können durch die unterbrechungsfreien Stromversorgungen in den Serverräumen überbrückt werden, bevor der geordnete Shutdown eingeleitet wird.
- 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 des 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.

4.4 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.

4.5 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 Virenscan des ein- und ausgehenden Datenverkehrs 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.

4.6 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.

4.7 Vertretungsregelungen für abwesende Beschäftigte

- Für Funktionen und Tätigkeiten sind Vertretungsregelungen eingerichtet.

4.8 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 Wiederanlaufszenarien werden regelmäßig durch Recovery-Tests bzw. Notfallübungen geprüft.

5 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 Regelung zur Datenschutzorganisation 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 bestellt. 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 ISO/IEC 27001:2013 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.

6 Anlagen

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

Übersicht Unterauftragnehmer

Übersicht über die für die DAVASO GmbH tätigen Unterauftragnehmer, die unmittelbar Daten des Auftraggebers erheben, verarbeiten und/oder nutzen:

Name des Unterauftragnehmers	Anschrift	Aufgabenfeld
REISSWOLF Akten- und Datenvernichtung GmbH Sachsen	Fischweg 14a 09114 Chemnitz	Akten- und Datenträgervernichtung

Übersicht über weitere für die DAVASO 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: 25.05.2018

Übersicht Wartungsfirmen

Übersicht über die für die DAVASO 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. 7 SGB X.

Name der Wartungsfirma	Anschrift	Aufgabenfeld
Konica Minolta Business Solutions Deutschland GmbH	Europaallee 17 30855 Langenhagen	Wartung der Kopierer
Pitney Bowes Deutschland GmbH	Poststraße 4 64293 Darmstadt	Wartung der Kuvertiermaschinen
MTG-Kommunikations-Technik GmbH	Portitzer Allee 8 04329 Leipzig	Wartung der Telefonanlage und Alarmanlage
BE-terna GmbH	Bornaer Straße 19 04288 Leipzig	Wartung der Software Microsoft Dynamics Navision
exela Technologies GmbH	Monzastraße 4c 63225 Langen	Wartung der Scanner
Bechtle GmbH IT-Systemhaus Leipzig	Westringstraße 59 04435 Schkeuditz	Wartung der Storage- und Archivsysteme
Fa. SecCommerce	Obenhauptstraße 5 22335 Hamburg	Wartung der Signaturanwendungskomponenten

Stand: 25.05.2018

Anhang D zur Anlage 5 – Bestimmungen zum Datenschutz und zur Datensicherheit bei der Datenverarbeitung im Auftrag (§ 80 SGB X i.V.m. Art. 28 DS-GVO)

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/Herr <Vorname> <Name>, beschäftigt als <Abteilung/Tätigkeit>,

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.

_____, _____ _____

Ort, Datum Verpflichtete(r)

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

Anlage zur Verpflichtung auf die Vertraulichkeit (Stand: 17.01.2018)

Die vorliegende Auswahl gesetzlicher 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 identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

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.

Anhang E zur Anlage 5 – Bestimmungen zum Datenschutz und zur Datensicherheit bei der Datenverarbeitung im Auftrag (§ 80 SGB X i.V.m. Art. 28 DS-GVO)

Übersicht über die für DAVASO GmbH im Rahmen der Aufgaben nach § 1 Abs. 1 der Datenschutzbestimmungen tätigen Unterauftragnehmer, die unmittelbar die Daten des Auftraggebers erheben, verarbeiten und/oder nutzen (z. B. Datenträgervernichter, Letter-Shop)

Unterauftragnehmer:	REISSWOLF Akten- und Datenträgervernichtung GmbH Sachsen
Anschrift:	Fischweg 14a 09114 Chemnitz
Aufgabenfeld:	Akten- und Datenträgervernichtung
Betriebsstätten/Standorte, an denen sich die Daten des Auftraggebers befinden - inkl. der Standorte der ggf. beauftragten Unterunterauftragnehmer:	Chemnitz
Datum Vertragsabschluss:	25.11./01.12.2015
Datum der letzten Prüfung gemäß § 7 Abs. 4 der Datenschutzbestimmungen:	27.10.2016/11.01.2017
Prüfung wurde durchgeführt durch:	Datenschutzbeauftragten
Prüfbericht vorhanden ja/nein:	ja

Übersicht gültig ab:	**25.05.2018**
Stand der Aktualisierung:	

Leipzig,

_____ _____

Ort, Datum DAVASO GmbH

Anhang F zur Anlage 5 – Bestimmungen zum Datenschutz und zur Datensicherheit bei der Datenverarbeitung im Auftrag (§ 80 SGB X i.V.m. Art. 28 DS-GVO)

Übersicht über die für die DAVASO GmbH tätigen Prüf- und (Fern-)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:	Konica Minolta Business Solutions Deutschland GmbH
Anschrift:	Europaallee 17 30855 Langenhagen
Aufgabenfeld:	Wartung der Kopierer

Name der Wartungsfirma:	Pitney Bowes Deutschland GmbH
Anschrift:	Poststraße 4 64293 Darmstadt
Aufgabenfeld:	Wartung der Kuvertiermaschinen

Name der Wartungsfirma:	MTG-Kommunikations-Technik GmbH
Anschrift:	Portitzer Allee 8 04329 Leipzig
Aufgabenfeld:	Wartung der Telefonanlage und Alarmanlage

Name der Wartungsfirma:	BE-terna GmbH
Anschrift:	Bornaer Straße 19 04288 Leipzig
Aufgabenfeld:	Wartung der Software Microsoft Dynamics Navision

Name der Wartungsfirma:	exela Technologies GmbH
Anschrift:	Monzastraße 4c 63225 Langen
Aufgabenfeld:	Wartung der Scanner

Name der Wartungsfirma:	Bechtle GmbH IT-Systemhaus Leipzig
Anschrift:	Westringstraße 59 04435 Schkeuditz
Aufgabenfeld:	Wartung der Storage- und Archivsysteme

Name der Wartungsfirma:	Fa. SecCommerce
Anschrift:	Obenhauptstraße 5 22335 Hamburg
Aufgabenfeld:	Wartung der Signaturanwendungskomponenten

Bei Bedarf bitte die Liste nach dem vorgegebenen Muster erweitern.

Übersicht gültig ab:	25.05.2018
Stand der Aktualisierung:	

Leipzig,

Ort, Datum	DAVASO GmbH