Grundlagen zum Datenverarbeitungsauftrag
(Datenschutz für Abrechnungsdienstleistungen)

Zum bereits bestehenden/noch abzuschließenden Abrechnungsvertrag gemäß des schriftlich erteilten Datenverarbeitungsauftrages auf Grundlage von Art. 28 DSG-VO gilt Folgendes:

I. Gegenstand der Auftragsdatenverarbeitung

1. Der Auftragnehmer erhebt, verarbeitet und nutzt personenbezogene Daten im Auftrag des Auftragsgebers.

2. Der Auftrag umfasst Folgendes:

2.1 Gegenstand des Auftrages (Definition der Aufgaben):

Erhebung, Speicherung, Veränderung, Übermittlung, Sperrung, Löschung, Nutzung von GKV-Rezeptdaten zu Abrechnungszwecken gemäß den Bestimmungen der §§ 300 und 302 SGB V und § 105 SGB XI, sowie die Nutzung der Daten zu Forschungszwecken gemäß § 27 Abs. 1 BDSG (neu).

Soweit der Dienst „apokompass“ mit den Programmen apoabgleich, apoprotect etc. beauftragt ist, wird der Auftragnehmer zusätzlich mit dem Entgegennehmen und Prüfen von GKV-Rezeptdaten auf bestimmte Gesetzes- und Vertragskonformität sowie das Rückübertragen der Prüfergebnisse beauftragt. Soweit der Dienst „apokompass“ mit allen Zusatzprogrammen beauftragt ist, wird der Auftragsnehmer zusätzlich mit der Rückübermittlung, Speicherung und Anzeige von GKV-Rezeptdaten im Klartext als sogenannte Rezeptimages sowie sonstige im Zusammenhang mit der Rezeptabrechnung stehende patientenbezogene Dokumente (Genehmigungen, Herstellungsprotokolle etc.) beauftragt.

Erstellung und Übermittlung von datenschutzkonformen Rezeptdatenauswertungen für Apothekenorganisationen (Apothekervereine und -verbände, Apothekerkammern, DAV, BAK, ABDA, DAPI) sowie die datenschutzkonforme Übermittlung von Patientendaten zu wissenschaftlichen Zwecken, soweit der Auftraggeber nachweisen kann, dass entsprechende Patienteneinwilligungen vorliegen.

2.2 Dauer des Auftrages

2.2.1 Der Auftrag gilt für die Laufzeit des Abrechnungsvertrages.

2.2.2 Der Auftraggeber kann den Auftrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen dieser Anlage oder datenschutzgesetzliche Bestimmungen vorliegt, der Auftragnehmer eine den datenschutzgesetzlichen Bestimmungen entsprechende Weisung des Auftraggebers nicht ausführen kann oder will.

2.2.3 Nach Beendigung des Auftrags ist der Auftragnehmer auf schriftliche Weisung des Auftraggebers verpflichtet die für ihn erhobenen und verarbeiteten Daten zu löschen oder an ihn herauszugeben, sofern die Löschung oder Herausgabe der Daten rechtlich möglich sind. Insbesondere die einschlägigen Abrechnungsfristen sind zu beachten. Die dem Auftragnehmer hierbei entstehenden Aufwände hat der Auftraggeber dem Auftragnehmer zu erstatten.

2.3 Kreis der Betroffenen:

Versicherte der GKV, gesetzlichen Unfallkassen und Berufsgenossenschaften, des SGB XII und des AsylBewLG sowie weitere an der GKV-Abrechnung Beteiligte, soweit deren Daten zu Abrechnungszwecken benötigt werden.

II. Rechte und Pflichten des Auftraggebers

1. Für die Beurteilung der Zulässigkeit der Datenerhebung /-verarbeitung /-nutzung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich.

2. Der Auftraggeber hat das Recht, schriftliche Weisungen im Rahmen dieses Datenverarbeitungsauftrages und / oder des Abrechnungsvertrages gegenüber dem Auftragnehmer zu erteilen.

Die Datenverarbeitung erfolgt nur auf Weisung des Auftraggebers, es sei denn, der Auftragnehmer ist durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zur Verarbeitung dieser Daten verpflichtet. Diese Pflicht trifft den Auftragnehmer aus den Abrechnungsvorschriften nach §§ 300, 302 SGB V und § 105 SGB XI. Sollten sich weitere Fälle ergeben, teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

Weisungsberechtigte Person des Auftraggebers ist, soweit nichts anderes vereinbart, allein der Apothekeninhaber.

Weisungsempfänger beim Auftragnehmer sind allein die jeweils vertretungsberechtigten Personen.

3. Der Auftraggeber ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen (s. Nr. IV) nach vorheriger Terminvereinbarung zu überzeugen, soweit sie sich auf seine Daten beziehen.

4. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

5. Die Rechte und Pflichten des Auftraggebers aus Nr. 3 und Nr.4 entfallen, wenn sich der Auftragnehmer selbst von einer anerkannten und zertifizierten Institution und den damit zusammenhängenden technischen und organisatorischen Maßnahmen im Rahmen der Auftragsdatenverarbeitung zertifizieren lässt. Der Auftragnehmer erteilt dem Auftraggeber schriftlich Auskunft über ein solches Zertifikat. Ziffer III. Nr. 6 bleibt von dieser Regelung unberührt.

6. Der Auftraggeber ist verpflichtet, alle im Rahmen des Auftragsdatenverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

Grundlagen zum Datenverarbeitungsauftrag
(Datenschutz für Abrechnungsdienstleistungen)

III. Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen, nach Weisungen des Auftraggebers sowie den gesetzlichen und liefervertraglichen Bestimmungen. Er hat personenbezogene Daten zu berücksichtigen, zu löschen und zu sperren, wenn der Auftraggeber dies in der getroffenen Vereinbarung oder einer Weisung verlangt oder vertraglich / gesetzlich vorgesehen ist und sonstige gesetzliche Bestimmungen dem entgegen stehen.

2. Dem Auftraggeber sind insbesondere Kontrollen nach den gesetzlichen Bestimmungen des Art. 32 DSGVO zu ermöglichen.

3. Soweit ein Verzeichnis für Verarbeitungstätigkeiten erstellt wird, hat der Auftragnehmer hieran mitzuwirken. Er hat die erforderlichen Angaben dem Auftraggeber zuzuleiten.

4. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden - automatisierten - Verwaltung. Eingang und Ausgang werden dokumentiert.

5. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird. Im Zweifel kann der Auftragnehmer die Zulässigkeit der Weisungsaufgabe vom Landesdatenschutzbeauftragten überprüften lassen.

6. Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber jederzeit - unter Einhaltung einer angemessenen Ankündigungsfrist - dazu berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarung, insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen, im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort, soweit es sich auf Daten des Auftraggebers bezieht. Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen mitwirkt. Die in diesem Fall beim Auftragnehmer anfallenden Kosten übernimmt der Auftraggeber. Ohne gesonderte Kostenberechnung ist der Auftragnehmer verpflichtet, den Nachweis für die Umsetzung der technischen und organisatorischen Maßnahmen, die nicht nur den konkreten Auftrag betreffen, durch Vorlage eines ausgefüllten Fragebogens (Anhang) zu erbringen.

7. Die auf Weisung des Auftraggebers vom Auftragnehmer verarbeiteten Daten werden im Rahmen der gesetzlichen und vertraglichen vereinbarten Aufbewahrungspflichten gespeichert. Nach Ablauf der Aufbewahrungspflichten werden sie vom Auftragnehmer gelöscht.

8. Soweit mit der Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers Unterauftragnehmer einbezogen werden, wird dies grundsätzlich nur unter folgenden Voraussetzungen genehmigt:

- Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem Unterauftragnehmer so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.

- Auf Anfrage teilt der Auftragnehmer den Namen und Anschrift der Unterauftragnehmer dem Auftraggeber mit.

- Der Auftragnehmer beauftragt ständig die GfI Gesellschaft für Informations- und Datenverarbeitung mbH (GfI), Bauerland 3, 28259 Bremen als Datenverarbeitungsunterauftragnehmer. Der Auftragnehmer hat mit der GfI die gleichen vertraglichen Regelungen getroffen, wie sie mit dem Auftraggeber vereinbart sind. Dieses Auftragsdatenverarbeitungsverhältnis unterliegt der Kontrolle und dem Zertifikat nach Ziffer II., Nr. 5. Auf Anfrage teilt der Auftragnehmer den Namen und die Anschrift anderer Unterauftragnehmer dem Auftraggeber mit, soweit es solche gibt.

Soweit Dienstleister beauftragt werden, die keine Wartungsarbeiten durchführen und entsprechend auch keinen Zugriff auf personenbezogene Daten haben, werden diese nicht als Unterauftragnehmer im Sinne dieser Regelung tätig. Dazu zählen z. B. der Betrieb der Telekommunikationsanlagen und Reinigungsarbeiten. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers, auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen. Das Gleiche gilt für vom Auftragnehmer zur Erbringung der vertraglichen Leistungen eingesetzte freie Mitarbeiter als Erfüllungsgehilfen, wenn mit diesen die notwenigen Sorgfalts- und Geheimhaltungspflichten vertraglich ver- einbart sind.

9. Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 45-49 DSGVO erfüllt sind.

Grundlagen zum Datenverarbeitungsauftrag
(Datenschutz für Abrechnungsdienstleistungen)

10. Vom Auftragnehmer ist gemäß § 38 BDSG (neu) ein Beauftragter für den Datenschutz bestellt. Auf Anfrage wird dem Auftraggeber der Name des Datenschutzbeauftrag- ten mitgeteilt.

11. Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers, das Datengeheimnis zu wahren.

12. Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften des BDSG (neu) und der DSGVO bekannt sind. Der Auftragnehmer bestätigt, dass ihm auch sozial-datenschutzrechtliche Vorschriften, hierbei insbesondere die mit der Apothekertätigkeit und Rezeptabrechnung verbundenen datenschutzrechtlichen Vorschriften, bekannt sind.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und sie auf das Datengeheimnis schriftlich verpflichtet. Der Auftragnehmer überwacht die Einhaltung der hier angegebenen datenschutzrechtlichen Vorschriften.

13. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen. Ausgenommen hiervon sind Auskünfte an Gerichte, Ermittlungs- oder sonstige Behörden, soweit die gesetzliche Pflicht zur Auskunft besteht und erforderliche amtliche Beschlüsse vorliegen.

14. Der Auftragnehmer unterstützt den Auftraggeber gemäß Art. 28 Abs. 3 lit. e DSGVO nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen, damit dieser seine bestehenden Pflichten gegenüber der betroffenen Person nach Kapitel 3 DSGVO erfüllen kann, z.B. die Information und Auskunft an den Betroffenen, die Berichtigung oder Löschung von Daten, die Einschränkung der Verarbeitung oder das Recht auf Datenübertragbarkeit und Widerspruch.

IV. Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (siehe Anhang)

1. Für die auftragsgemäße Bearbeitung der Daten nutzt der Auftragnehmer nach dem Stand der Technik leistungsfähige daten– und ausfallsichere Einrichtungen der Hard– und Software.

2. Die im Anhang beschriebenen technischen und organisatorischen Maßnahmen werden als verbindlich festgelegt. Hierdurch sollen die in Art. 32 DSGVO genannten Sicherheitsziele erreicht werden. Insbesondere gewährleistet der Auftragnehmer

- eine klare Aufgabenverteilung, beispielsweise bei der Vergabe von Zugriffsrechten,
- die Abschottung von Netzen: Es werden Maßnahmen ergriffen werden, um ein unberechtigtes Eindringen in Rechnernetze soweit möglich zu verhindern,
- Maßnahmen zur Verschlüsselung beim elektronischen Datentransfer,
- qualitativ hochwertige Maßnahmen zur Anmeldung am System und sämtlichen datenwesentlichen Anwendungen.

3. Der Auftragnehmer beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschrieben Datensicherheitsmaßnahmen.

4. Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber auf Anforderung zur Beurteilung mitzuteilen.

5. Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

6. Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers, oder bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen, oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen, oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit, soweit Daten des Auftraggebers von dem Ereignis betroffen sind. Dies gilt vor allem auch im Hinblick auf eventuelle Informationspflichten des Auftraggebers nach Art. 33 DSGVO. Dem Auftragnehmer ist bekannt, dass der Auftraggeber verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten (Art. 4 Nr. 12 DSGVO) zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person binnen 72 Stunden zu melden. Sofern es zu solchen Verletzungen gekommen ist, wird der Auftragnehmer dem Auftraggeber gemäß Art. 28 Abs. 3 lit. f DSGVO bei der Einhaltung seiner Meldepflichten unterstützen. Er wird die Verletzungen dem Auftraggeber melden und hierbei zumindest folgende Informationen mitteilen:

- eine Beschreibung der Art der Verletzung, der Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze,
- Name und Kontaktdaten eines Ansprechpartners für weitere Informationen,
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung sowie,
- eine Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

Grundlagen zum Datenverarbeitungsauftrag
(Datenschutz für Abrechnungsdienstleistungen)

7. Der Auftragnehmer bietet nach Maßgabe des Art. 28 Abs. 1, 5 DSGVO hinreichende Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen durchgeführt werden, die gewährleisten, dass die Verarbeitung im Einklang mit der DSGVO und den Rechten der betroffenen Person steht.

8. Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen, die den Vorgaben des Art. 32 DSGVO entsprechen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und unterstützt den Auftraggeber bei der Einhaltung der in Art. 32 DSGVO genannten Pflichten (Art. 28 Abs. 3 lit. c, f DSGVO), die sich auf die Datenverarbeitung am Standort des Auftragnehmers bzw. Unterauftragsnehmer bezieht. Bereits vereinbarte Dokumentationen und IT-Sicherheitskonzepte behalten ihre Wirksamkeit.

9. Der Auftragnehmer wirkt nach Maßgabe des Art. 28 Abs. 3 lit. f DSGVO bei der Erstellung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden gemäß Art. 36 DSGVO mit. Er hat dem Auftraggeber die erforderlichen Angaben und Dokumente auf Anfrage offen zu legen.

V. Haftung

1. Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung vorsätzlich oder grob fahrlässig verursachen.

2. Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem BDSG (neu) und der DSGVO oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Daten- verarbeitung im Rahmen des Auftragsverhältnisses erlei- det, ist der Auftraggeber gegenüber dem Betroffenen verantwortlich. Soweit der Auftraggeber zum Schadener- satz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten.

VI. Schriftform, Wirksamkeit dieser Anlage

1. Für Nebenabreden ist die Schriftform oder das elektronische Format erforderlich.

2. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit des Datenverarbeitungsauftrages nebst dieser Anlage und Anhang im Übrigen nicht.

3. Änderungen zu diesem Vertrag werden dem Vertragspartner in Textform mitgeteilt. Sollte der Vertragspartner nicht innerhalb von 6 Wochen seit dem Zugang der Änderung, der Änderung nicht in Textform widersprochen haben, gilt die Änderung als vereinbart.

Anhang: Beschreibung der technischen und organisatorischen Maßnahmen zu IV. Datensicherungsmaßnahmen

1. Zutrittskontrolle (Vertraulichkeit und Integrität)

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogenen Daten verarbeitet werden:

- Schließsysteme / Sicherheitsschlüssel
  - Nach Aufgaben abgestufte Berechtigungen
  - Während der Geschäftszeiten: Permanent besetzter Empfang
  - Alarmanlage
  - Videoüberwachung aller Ein- und Ausgänge sowie Fensterfronten
  - Schlüsselverzeichnis

2. Zugangskontrolle (Vertraulichkeit und Integrität)

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und –verfahren benutzen:

- Benutzernamen / Passwortkontrolle, nach BSI- Verschlüsselung der Festplatten von mobilen Endgeräten
- Einsatz verschiedener anwendungsorientierter Firewalls

3. Zugriffkontrolle (Vertraulichkeit und Integrität)

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

- Zugriffsberechtigungen der Mitarbeiter nach Aufgabengebiet

- Zugriffsberechtigungen sind dokumentiert durch Administratoren
- Änderung der Konfiguration der Datenverarbeitungsanlagen nur durch berechtigtes Personal

(Systemadministratoren)
- Geschützter Server-Raum (durch Zutritts– und Zugangskontrollen, Berechtigungsüberprüfung auch durch Fingerprint sowie durch Videoüberwachung)

Grundlagen zum Datenverarbeitungsauftrag
(Datenschutz für Abrechnungsdienstleistungen)

4. Weitergabekontrolle (Vertraulichkeit und Integrität)

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungenzur Datenübertragung vorgesehen ist.

Einsatz eines VPN-Systems (Lancom)
- Versand von Datenträgern nur in den gesetzlichen bestimmten Fällen (z.B. §§ 300, 302 SGB V).
- Ausgesonderte Datenträger werden im Rahmen der Aktenvernichtung durch ein zertifiziertes Unternehmen (Reißwolff) unwiederherstellerbar zerstört.

5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.

- Protokollierung der Eingaben bei der Datenerhebung, -Verarbeitung und –Löschung

6. Auftragskontrolle (Vertraulichkeit und Integrität)

Gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Eindeutige Vertragsgestaltung gemäß Art. 28 DSGVO
- Einsatz von Standardverträgen
- Definierter Prozess zur Auftragsvergabe (§§ 300 und 302)

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Speicherung der Daten zentral auf Servern und einem Bandroboter
- Tägliche Datensicherung (vier Generationen)
- Aufbewahrung der Sicherungsmedien in einem feuergesicherten Schutzschrank
- Ständige Kontrolle des Backup Verfahrens
- Einsatz von Virenscannern, die Virenscanner werden automatisch aktualisiert .
- Regelmäßige Einspielung sicherheitsrelevanter Updates und Patches

8. Trennungskontrolle (Vertraulichkeit und Integrität)

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Organisatorische Regelungen
- Funktionstrennung im Rahmen der Zugriffskontrolle

9. Regelmäßiges Verfahren zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen durch ein jährliches Re-Audit durch eine externe Zertifizierungsstelle werden die in diesem Abschnitt genannten Maßnahmen regelmäßig überprüft.