Bericht

zum Rezertifizierungsaudit nach
DATENSCHUTZSTANDARD DS-BVD-GDD-01
"Anforderungen an Auftragnehmer nach § 11 BDSG"

für

MedicalContact AG

über die Leistungen
1. Versorgungsmanagement (Morbiditätsmanagement) für Krankenversicherungsträger (Gesundheits-Coaching für Krankenversicherer)
2. Betriebliches Gesundheitsmanagement für Unternehmen (Gesundheits-Coaching für Unternehmen)

Berichtersteller	Dr. Niels Lepperhoff
Zertifizierungs-nummer DSZ.	Z-001
Anschrift	Xamit Bewertungsgesellschaft mbH Monschauer Str. 12 40549 Düsseldorf
Berichts-Datum	23.11.2017

Inhaltsverzeichnis

1. Einführung

Dieser Bericht wurde von DR. NIELS LEPPERHOFF erstellt und beschreibt die Tätigkeiten bzgl. unten stehender Auditaktivitäten:

Organisation	Erstprüfung / Verlängerung	Audittermin (Start)
MedicalContact AG Kronprinzenstraße 5 – 7 45128 Essen	☐ Erstprüfung X Verlängerung	09.11.2017 2 Tage

1.1. Ziel des Audits

Das Ziel des Audits zur Rezertifizierung war eine erneute Überprüfung der im Anwendungsbereich beschriebenen Leistungen, um zu gewährleisten, dass die im Anwendungsbereich getroffenen Maßnahmen und erforderlichen Umsetzungen nach dem DATENSCHUTZSTANDARD DS-BVD-GDD-01 "Anforderungen an Auftragnehmer nach § 11 BDSG" und sonstigen Vorgaben der Zertifizierungsgesellschaft erfüllt werden. Es mündet in der Empfehlung hinsichtlich einer Weiterführung der Zertifizierung.

Das Audit mit dem Ziel der Zertifizierung nach dem DATENSCHUTZSTANDARD DS-BVD-GDD-01 "Anforderungen an Auftragnehmer nach § 11 BDSG" dient folgenden Aspekten:

- Auftraggeber können die Zertifizierung ihrem eigenen Kontrollermessen gemäß § 11 Abs. 2 BDSG zugrunde legen.
- Das Unternehmen signalisiert als Auftragnehmer sein gesetzeskonformes Datenschutzniveau.

Dieses vor Ort durchgeführte Audit basiert auf Stichproben. Es kann somit nicht ausgeschlossen werden, dass Abweichungen nicht erkannt werden.

Wenn Sie diesen Auditbericht an Dritte weiterleiten möchten, sind alle Teile des Berichtes zu übermitteln. Auszüge oder Teile des Berichts dürfen nicht an Dritte weitergeleitet werden.

Mit dem Wirksam werden der Datenschutz-Grundverordnung (DS-GVO) am 25.05.2018 ändert sich das Datenschutzrecht während der Zertifikatslaufzeit. Die meisten Vorgaben und Anforderungen des Prüfstandards DS-BvD-GDD-01 erfüllen bereits die neuen gesetzlichen Anforderungen. Weitere Anforderungen der DS-GVO wurden im Rahmen der Rezertifizierung berücksichtigt und in diesem Bericht gesondert ausgewiesen. Da die DS-GVO noch nicht wirksam ist, werden Mängel informatorisch berichtet und haben keinen Einfluss auf die Zertifikatsverlängerung. Gleichwohl besteht die Erwartung, dass die Mängel bis zum Wirksamwerden der DS-GVO aufgrund der für die MedicalContact AG bestehenden gesetzlichen Verpflichtungen behoben sind.

1.2. Anwendungsbereich der Zertifizierung Reg. Nr. A-003

Ort	Auditierte Leistung
MedicalContact AG Kronprinzenstraße 5 – 7 45128 Essen	1. Versorgungsmanagement (Morbiditätsmanagement) für Krankenversicherungsträger 2. Betriebliches Gesundheitsmanagement für Unternehmen

Durchführung von vorstrukturierten Gesundheitsberatungen (Gesundheitsinformation, -coaching und Fallmanagement) im Rahmen

a) des Versorgungsmanagements (Morbiditätsmanagement) für Krankenversicherungsträger (nach der Zertifizierung zwischenzeitlich unbenannt in „Gesundheits-Coaching für Krankenversicherer") und

b) des Betrieblichen Gesundheitsmanagements für Unternehmen (nach der Zertifizierung zwischenzeitlich unbenannt in „Gesundheits-Coaching für Unternehmen").

Diese beinhalten

- die Bereitstellung von Beratungshotlines,
- den Versand von schriftlichen Gesundheitsinformationen (Remindern) bei Programmteilnehmern,
- die Durchführung von indikationsbezogenen telefonischen Beratungen (Coachings) bei Programmteilnehmern,
- die Beratung von Programmteilnehmern vor Ort (nur Versorgungsmanagement (Morbiditätsmanagement) für Krankenversicherungsträger).
- Webbasierte psychologische Gefährdungsbeurteilung (Betriebliches Gesundheitsmanagement)

Die einzelnen Leistungsbestandteile können modular beauftragt werden.

Die Umsetzung der Programme wird unterstützt durch:

- die Bereitstellung eines Online-Portals „der Geschäftskundenbereich" als sichere Plattform für den Austausch personenbezogener Daten / Sozialdaten und anderer Materialien mit sensiblen Informationen,
- die speziell auf die Beratungsprogramme zugeschnittenen CRM-Systeme,
- die regelmäßige Erstellung von Qualitätssicherungsberichten bzw. deskriptiven Reports,
- die Durchführung von Zufriedenheitsbefragungen.

Folgende Tätigkeiten und Leistungen der MedicalContact AG sind nicht Teil der Zertifizierung:

- Beratung der Auftraggeber,
- Klientenidentifikation im Auftrag,
- Evaluation im Auftrag und
- Individual-Projekte.

Bei mehreren Leistungen:

X Der vorliegende Bericht ist der Referenzbericht

☐ Der vorliegende Bericht ist nur gültig im Zusammenhang mit dem Referenzbericht:

_____. Er beschränkt sich im Folgenden auf abweichende Feststellungen.

2. Management Summary / Zusammenfassung

Das Rezertifizierungsaudit der Leistungen

a) Versorgungsmanagement (Morbiditätsmanagement) für Krankenversicherungsträger (nach der Zertifizierung zwischenzeitlich unbenannt in „Gesundheits-Coaching für Krankenversicherer“) und
b) betrieblichen Gesundheitsmanagement für Unternehmen (nach der Zertifizierung zwischenzeitlich unbenannt in „Gesundheits-Coaching für Unternehmen“)

fand im Zeitraum vom 09.11.2017 bis zum 15.11.2017 statt. Alle benötigten Dokumente wurden im Rahmen eines Vor-Ort-Termins gezeigt und erläutert. Darüber hinaus standen dem Auditor, die von ihm angeforderten Dokumente zur Detailprüfung zur Verfügung. Im Vor-Ort-Termin wurden die Fragen des Auditors vollumfänglich ohne Vorbehalte fachkundig beantwortet und auf Wunsch durch Demonstrationen im System oder Einsichtnahme in Dokumentationen belegt.

Die Leistungserbringung erfolgt für beide Leistungen ausschließlich auf der Basis von Weisungen der Auftraggeber. Diese umfassen insbesondere Inhalte und Ziele der Informationsmaterialen und Beratungsgespräche und legen im Versorgungsmanagement (Morbiditätsmanagement) auch die teilnehmenden Versicherten fest. Aus diesem Grund handelt es sich um eine Auftragsdatenverarbeitung und nicht um eine Funktionsübertragung. Das im betrieblichen Gesundheitsmanagement für Unternehmen vereinbarte Verbot, Daten von am Programm teilnehmenden Mitarbeiter dem Arbeitgeber zu übermitteln, stellt die Vertraulichkeit für die Arbeitnehmer sicher und steht der Auftragsdatenverarbeitung nicht entgegen.

Beide Leistungen werden im Wesentlichen durch die gleichen Abläufe erbracht und die gleichen Konzepte und Managementsysteme kontrolliert. Aus diesem Grund behandelt dieser Auditbericht beide Leistungen zusammen. Auf Unterschiede wird an den jeweiligen Stellen eingegangen. Die unterschiedlichen Rechtsgrundlagen (für a) SGB X und für b) BDSG) gehen – auch ohne gesonderte Erwähnung – in die Prüfung und Bewertung ein.

Als privatwirtschaftliches Unternehmen unterliegt die MedicalConact AG als Auftragsdatenverarbeiter vollumfänglich § 11 BDSG und ist nach DS-BvD-GDD-01 zertifizierungsfähig. Die für Krankenversicherungsträger korrespondierende Vorschrift stellt § 80 SGB X dar, der nicht in einem inhaltlichen Widerspruch zu § 11 BDSG steht. Die Vertragsbeziehung mit Krankenversicherungsträger setzt faktisch beide Vorschriften um.

Nach den Erkenntnissen der Dokumentenprüfung und des Vor-Ort-Audits sind die Leistungen

a) Versorgungsmanagement (Morbiditätsmanagement) für Krankenversicherungsträger (nach der Zertifizierung zwischenzeitlich unbenannt in „Gesundheits-Coaching für Krankenversicherer“) und
b) betrieblichen Gesundheitsmanagement für Unternehmen (nach der Zertifizierung zwischenzeitlich unbenannt in „Gesundheits-Coaching für Unternehmen“)

hinreichend schlüssig im Hinblick den DATENSCHUTZSTANDARDS DS-BVD-GDD-01 "Anforderungen an Auftragnehmer nach § 11 BDSG" durch die MedicalContact AG dokumentiert und wirksam implementiert.

Seit dem Zertifizierungsaudit haben sich nur wenige Änderungen ergeben. Diese waren Schwerpunkt des vorliegenden Rezertifizierungsaudits.

Die der Leistungserbringung zu Grunde liegenden Prozesse haben sich seit der Zertifizierung nicht verändert. Das betriebliche Gesundheitsmanagement wurde um den Zusatzservice „psychologische Gefährdungsbeurteilung“ ergänzt. Die Befragung erfolgt webbasiert und anonym. Der Mitarbeiter erhält einen automatisch erzeugten individuellen Bericht. Der Auftraggeber erhält einen aggregierten Bericht basierend auf den Antworten der Mitarbeiter. Dabei werden Merkmalskombinationen mit weniger als 10 Fragebögen nicht ausgewiesen.

Den Empfehlungen des Zertifizierungsaudits wurde überwiegend gefolgt:

- Die Anregung zum Sicherheitskonzept, aus einer systematischen Betrachtung von Risiken oder Gefahren die Maßnahmen abzuleiten, wurde aufgegriffen. Basierend auf Schadensereignissen werden Schadensereignisse für jede Gruppe von Assets bestimmt. An die Risikobetrachtung schließt das im Vergleich zur Zertifizierung ansonsten im Wesentlichen unveränderte Sicherheitskonzept an. Es wird angeregt, die Risikoanalyse weiter auszubauen und Gefahren explizit in den Blick zunehmen, d.h. die Schadensereignisse mit Gefahren zu verbinden und auf Vollständigkeit zu prüfen.
- Das in der Zertifizierung geprüfte Datenschutz-Managementsystem zur nachhaltigen Sicherstellung des Datenschutzes wurde weiterentwickelt. Durch vertragliche Vereinbarungen wird stärker auf die Bestellung eines Datenschutzbeauftragten bei den Unterauftragnehmern eingewirkt. Weiterhin wird die persönliche Kontrolle der Unterauftragnehmer durch eine webgestützte Befragung ergänzt.
- Ansprechpartner vom Kunden werden nach Auftragsende oder wenn sie durch Ausscheiden oder Versetzung nicht mehr zuständig sind gelöscht.

Weil der Standard DS-BvD-GDD-01 bereits zahlreiche Anforderungen der Datenschutz-Grundverordnung (DS-GVO) umsetzt, erfüllt die MedicalContact AG im Rahmen des Zertifizierungsscope die entsprechenden Anforderungen der DS-GVO bereits. Mit Blick auf die gesetzliche Pflicht auch des Auftragnehmers die DS-GVO einzuhalten, wird empfohlen bis Mai die Lücken zu schließen.

Um eine einfache Vergleichbarkeit mit dem Zertifizierungsaudit zu wahren, werden im Folgen die in der Zertifizierung verwendeten Leistungsbezeichnungen verwendet.

3. Obligatorische Anforderungen / Scoping

3.1. Prüfungsrelevante Kernmodule

Modul			relevant
4.1 Leistungsbeschreibung	4.1.1	Beschreibung der Leistung	**Ja**
	4.1.2	Beschreibung der Auftragsbearbeitung (Herstellung)	**Ja**
4.2 Input-Management			**Ja**
4.3 Auftragsmanagement			**Ja**
4.4 Output-Management			**Ja**
4.5 Datenschutzkonzept	4.5.1	Eingabekontrolle	**Ja**
	4.5.2	Trennungsgebot	**Ja**
	4.5.3	Auftragskontrolle	**Ja**
	4.5.4	Prozessbeschreibung Auskunft	**Ja**
	4.5.5	Prozessbeschreibung Berichtigung	**Ja**
	4.5.6	Prozessbeschreibung Sperrung	**Ja**
	4.5.7	Prozessbeschreibung Löschung	**Ja**
	4.5.8	Prozessbeschreibung Sicherheitsvorfall	**Ja**
4.6 IT-Sicherheitskonzept	4.6.2.1	Erstellung und Verwendung des IT-Sicherheitskonzepts	**Ja**
	4.6.2.2	Mindeststandard Gebäudesicherheit	**Ja**
	4.6.2.3	Mindeststandard Zutrittsschutz	**Ja**
	4.6.2.4	Mindeststandard Zugangsschutz	**Ja**
	4.6.2.5	Mindeststandard Zugriffsschutz	**Ja**
	4.6.2.6	Mindeststandard Verfügbarkeit	**Ja**
	4.6.2.7	Mindeststandard Datenübertragung	**Ja**
4.7 Datenschutz-Managementsystem	4.7.4.1	Der Datenschutzbeauftragte	**Ja**
	4.7.4.2	Kontrolle des Datenschutzkonzeptes	**Ja**
	4.7.4.3	Kontrolle der Unterauftragnehmer	
4.8 IT-Sicherheitsmanagementsystem			**Ja**
4.9 Auftragsmanagementsystem			**Ja**

3.2. Prüfungsrelevante Module in Abhängigkeit des Leistungsumfangs

Modul		relevant
5.1 Vertrag		**Ja**
5.2 Beendigung der Leistungsbeziehung		**Ja**

3.3. Genehmigte Ausnahmen

Es wurden keine Ausnahmen im Folgeaudit beantragt.

4. Auditierte Bereiche & Feststellungen

4.1. Kernmodule:

4.1.1. Leistungsbeschreibung

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.1.1 Beschreibung der Leistung	Die Vorgaben und Anforderungen des Standards werden vollständig umgesetzt.
Prüfmethode / Prüfhandlung	
Die Leistungen richten sich an unterschiedliche Zielgruppen (Krankenversicherungsträger oder Unternehmen), die jeweils spezifisch angesprochen werden. Leistungsbeschreibungen finden sich mit unterschiedlichen Schwerpunkten sowohl auf der Webseite wie auch in Informationsmappen. Die Leistung „betriebliches Gesundheitsmanagement für Unternehmen" wurde um den Zusatzservice „psychologische Gefährdungsbeurteilung" ergänzt. Abgesehen von der webgestützten Befragung und Auswertung werden die bei der Zertifizierung geprüften Prozesse zur Leistungserbringung verwendet. Die Befragung erfolgt anonym, so dass weder die MedicalContact AG noch der Auftraggeber einen Personenbezug herstellen kann. Der Mitarbeiter erhält einen automatisch erzeugten individuellen Bericht. Der Auftraggeber erhält einen aggregierten Bericht basierend auf den Antworten der Mitarbeiter. Dabei werden Merkmalskombinationen mit weniger als 10 Fragebögen nicht ausgewiesen. Der Mitarbeiter kann durch einen im Rahmen der Befragung mitgeteilten Code anonym eine Beratung bei der MedicalContact AG basierend auf seinen individuellen Antworten erhalten. Die Beschreibung der psychologischen Gefährdungsbeurteilung erfüllt die Anforderungen des Standards. Die Musterverträge für Auftraggeber liegen vor. Das Datenschutzkonzept beschreibt die technischen und organisatorischen Maßnahmen zur IT-Sicherheit und auch wesentliche Datenschutzgrundsätze. Als Vertragsanlage wird das Datenschutzkonzept Grundlage der Zusammenarbeit. Prüfungshandlung: Dokumentensichtung, Interviews.	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.1.2 Beschreibung der Herstellung	Die Vorgaben und Anforderungen des Standards werden vollständig umgesetzt.
Prüfmethode / Prüfhandlung	
Hinsichtlich der Leistungserbringung hat es – bis auf einer zusätzlichen Backupmöglichkeit durch Server im eigenen Serverraum – keine grundsätzlichen Änderungen gegeben. Die Herstellung ist weiterhin modular aufgebaut. Die Module werden Auftraggebern hinsichtlich ihrer Leistung wie auch ihres Ablaufs allgemein beschrieben. Die Einteilung in Module wurde für beide Leistungen umbenannt. Die Umbenennung berührt die zertifizierten Prozesse nicht. Die Leistungserbringung erfolgt wie in der Zertifizierung ausgeführt durch standardisierte und beschriebene Prozesse sowie innerhalb verschiedener CRM-Systeme. Workflows unterstützen eine auftragsgemäße Leistungserbringung. Auftraggeber erhalten regelmäßig nicht personenbezogene Berichte über die Leistungserbringung. **Prüfungshandlung:** Dokumentensichtung, Interviews	

4.1.2. Herstellung

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.2 Input-Management	Die Vorgaben und Anforderungen des Standards werden vollständig umgesetzt.
Prüfmethode / Prüfhandlung	
Versorgungsmanagement (Morbiditätsmanagement) für Krankenversicherungsträger: Es haben sich keine Änderungen im Vergleich zur Zertifizierung ergeben. **Betriebliches Gesundheitsmanagement für Unternehmen:** Es haben sich keine Änderungen im Vergleich zur Zertifizierung ergeben. Personenbezogene Daten der Mitarbeiter des Auftraggebers werden weiterhin nicht an die MedicalContact AG übermittelt. Der Auftraggeber informiert seine Mitarbeiter in eigener Verantwortung über das Angebot. Die Anmeldung zur psychologischen Gefährdungsbeurteilung erfolgt über einen Firmenzugang, d.h. alle Mitarbeiter teilen sich die Zugangsdaten. Damit entsteht weder für die Einladung noch für die Durchführung bei der MedicalContact AG ein Personenbezug. **Ausblick auf die Datenschutz-Grundverordnung** Durch die dokumentierte Datenübertragung, wie sie in der Zertifizierung beschrieben wurde, sind wesentliche Anforderungen der DS-GVO aus der Rechenschaftspflicht nach Art. 5 Abs. 2 bereits umgesetzt. **Prüfungshandlung:** Dokumentensichtung, Interviews	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.3 Auftragsmanagement	Die Vorgaben und Anforderungen des Standards werden vollständig umgesetzt.

Prüfmethode / Prüfhandlung

Die Prozesse zur Leistungserbringung sind beschrieben und im Wirkbetrieb. Sie haben sich gegenüber der Zertifizierung nicht geändert.

Für die psychologische Gefährdungsbeurteilung liegen eine Prozessbeschreibung sowie eine Leistungsbeschreibung vor. Die Mitwirkung des Auftraggebers und die Leistungserbringung beim Auftragnehmer sind darin erläutert. Unterauftragnehmer werden bei der psychologischen Gefährdungsbeurteilung nicht eingesetzt.

Ausblick auf die Datenschutz-Grundverordnung

Durch die dokumentierte Auftragsbearbeitung, wie sie in der Zertifizierung beschrieben wurde, sind wesentliche Anforderungen der DS-GVO bereits umgesetzt.

Prüfungshandlung:

Dokumentensichtung, Interviews, Begehung von Arbeitsplätzen

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.4 Output-Management	Die Vorgaben und Anforderungen des Standards werden vollständig umgesetzt.

Prüfmethode / Prüfhandlung

Versorgungsmanagement (Morbiditätsmanagement) für Krankenversicherungsträger:

Es haben sich keine Änderungen im Vergleich zur Zertifizierung ergeben.

Betriebliches Gesundheitsmanagement für Unternehmen:

Es haben sich keine Änderungen im Vergleich zur Zertifizierung ergeben.

Im Rahmen der psychologischen Gefährdungsbeurteilung erhält der an der Befragung teilnehmende Mitarbeiter am Ende der Onlinebefragung einen automatisch erstellten Bericht mit Handlungsempfehlungen. Er kann den Bericht ausdrucken. Der Auftraggeber, d.h. der Arbeitgeber des teilnehmenden Mitarbeiters, erhält nach Abschluss des Projektes einen Unternehmensbericht. Dieser Bericht zeigt aggregiert die Mittelwerte der Antworten. Merkmalskombinationen mit weniger als 10 Teilnehmern werden nicht im Unternehmensbericht ausgewiesen. Der Auftraggeber hat keinen Zugriff auf die Rohdaten, die ihrerseits anonym sind.

Ausblick auf die Datenschutz-Grundverordnung

Durch die dokumentierte Auftragsbearbeitung, wie sie in der Zertifizierung beschrieben wurde, sind wesentliche Anforderungen der DS-GVO bereits umgesetzt.

Prüfungshandlung:

Dokumentensichtung, Interviews

4.1.3. Datenschutzkonzept

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.5 Datenschutzkonzept	Die Vorgaben und Anforderungen des Standards werden vollständig umgesetzt.

Prüfmethode / Prüfhandlung

Das Datenschutzkonzept umfasst die Erfüllung spezifischer gesetzlicher Datenschutzvorschriften, zu denen insbesondere die

- Eingabekontrolle,
- Protokollkonzept,
- Trennungsgebot,
- Auftragskontrolle und
- Umgang mit Sicherheitsvorfällen

zählen. Das Konzept ist im Wesentlichen unverändert gegenüber der Zertifizierung.

Ausblick auf die Datenschutz-Grundverordnung

Die Anpassung des Datenschutzkonzeptes an die DS-GVO ist in Arbeit und soll nach Planung der MedicalContact AG bis Mai 2018 abgeschlossen sein. Anzupassen sind insbesondere die Umsetzung der (neuen) Betroffenenrechte, die Umsetzung der Informationspflichten nach Art. 13 und 14 DS-GVO sowie die Erweiterung des Prozesses zum Umgang mit Sicherheitsvorfällen auf die Anforderungen von Art. 33 und 34 DS-GVO. Inhaltlich liegen die notwendigen Angaben vor, um die Informationspflichten nach Art. 13 und 14 DS-GVO umzusetzen.

Im Einzelnen wurden folgende Aspekte betrachtet:

Modul		Feststellung
4.5.1	Eingabekontrolle	**erfüllt**
4.5.2	Trennungsgebot	**erfüllt**
4.5.3	Auftragskontrolle	**erfüllt**
4.5.4	Prozessbeschreibung Auskunft	**erfüllt**
4.5.5	Prozessbeschreibung Berichtigung	**erfüllt**
4.5.6	Prozessbeschreibung Sperrung	**erfüllt**
4.5.7	Prozessbeschreibung Löschung	**erfüllt**
4.5.8	Prozessbeschreibung Sicherheitsvorfall	**erfüllt**

Prüfhandlung:

Dokumentensichtung, Interviews

4.1.4. IT-Sicherheitskonzept

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.6 IT-Sicherheitskonzept	Die Vorgaben und Anforderungen des Standards werden umgesetzt. Es wird angeregt, die Risikoanalyse weiter auszubauen und Gefahren explizit in den Blick zunehmen.

Prüfmethode / Prüfhandlung

Die Anregung aus der Zertifizierung, aus einer systematischen Betrachtung von Risiken oder Gefahren die Maßnahmen abzuleiten, wurde aufgegriffen. Basierend auf Schadensereignissen werden Schadensereignisse für jede Gruppe von Assets bestimmt. Die Assetgruppen fassen die Assets zusammen, die für die Erbringung einer Leistung notwendig sind. An die Risikobetrachtung schließt das im Vergleich zur Zertifizierung ansonsten im Wesentlichen unveränderte Sicherheitskonzept an. Es wird angeregt, die Risikoanalyse weiter auszubauen und Gefahren explizit in den Blick zunehmen, d.h. die Schadensereignisse mit Gefahren zu verbinden und auf Vollständigkeit zu prüfen.

Die Basis der IT-Sicherheit bildet die IT-Sicherheitsrichtlinie. Das IT-Sicherheitskonzept setzt sich aus verschiedenen Dokumenten zusammen. Es beinhaltet eine Ist-Analyse der Räume, Systeme und Geräte, eine Schutzbedarfsfeststellung nach dem Maximum-Prinzip. Maßnahmen werden verallgemeinert im Datenschutzkonzept, das Vertragsbestandteil für die ADV-Verträge mit den Auftraggebern wird, beschrieben. Die Konfiguration und der Betrieb der Systeme werden in Betriebshandbüchern erläutert. Das Notfallkonzept regelt den Umgang mit Notfällen, um den Betrieb aufrecht zu halten. Die Maßnahmen zielen auf eine vergleichsweise sehr geringe maximale Ausfallzeit ab.

Eine zusätzliche Redundanz beim Ausfall von Servern oder die Verbindung zum Server wurde durch den Aufbau eines Backups mit virtuellen Servern im eigenen Serverraum geschaffen.

Weitere Anregungen aus der Zertifizierungen wurden geprüft und auf kompensierende Maßnahmen verwiesen, so dass eine Umsetzung entbehrlich erscheint.

Ausblick auf die Datenschutz-Grundverordnung

Das Sicherheitskonzept berücksichtigt die Risiken für die Betroffenen noch nicht. Es wird empfohlen es um die Vorgaben des Art. 32 DS-GVO zu ergänzen.

Im Einzelnen wurden folgende Aspekte betrachtet:

Modul		Feststellung
4.6.2.1	Erstellung und Verwendung des IT-Sicherheitskonzepts	**erfüllt**
4.6.2.2	Mindeststandard Gebäudesicherheit	**erfüllt**
4.6.2.3	Mindeststandard Zutrittsschutz	**erfüllt**
4.6.2.4	Mindeststandard Zugangsschutz	**erfüllt**
4.6.2.5	Mindeststandard Zugriffsschutz	**erfüllt**
4.6.2.6	Mindeststandard Verfügbarkeit	**erfüllt**
4.6.2.7	Mindeststandard Datenübertragung	**erfüllt**

Prüfhandlung:

Dokumentensichtung, Interviews, Begehung interner Serverraum

4.1.5. Managementsysteme

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.7 Datenschutz-Managementsystem	Die Vorgaben und Anforderungen des Standards werden vollständig umgesetzt.
Prüfmethode / Prüfhandlung	
Das in der Zertifizierung geprüfte Datenschutz-Managementsystem zur nachhaltigen Sicherstellung des Datenschutzes wurde weiterentwickelt. Die Anregungen aus der Zertifizierung, das Datenschutzmanagement bei Unterauftragnehmern zu stärken und stärker zu kontrollieren wurden aufgegriffen. Durch vertragliche Vereinbarungen wird stärker auf die Bestellung eines Datenschutzbeauftragten bei den Unterauftragnehmern eingewirkt. Weiterhin wird die persönliche Kontrolle der Unterauftragnehmer durch eine webgestützte Befragung ergänzt. **Ausblick auf die Datenschutz-Grundverordnung** Durch das Datenschutzmanagementsystem wird die Einhaltung der Datenschutzvorschriften überwacht. Es wird angeregt, ein Vorgehen zur Risikobewertung mit Blick auf die Rechte und Freiheiten von betroffenen Personen einzurichten und einen Unterstützungsprozess für die vom Auftraggeber ggf. durchzuführende Datenschutz-Folgeabschätzung zu etablieren. Es wird der guten Ordnung halber an die Verpflichtung, die Kontaktdaten des Datenschutzbeauftragten an die Datenschutzaufsichtsbehörde zu melden, erinnert. Prüfhandlung: Dokumentensichtung, Interviews, stichprobenhafte Sichtung von internen Prüfberichten des Datenschutzbeauftragten, stichprobehafte Einsicht in die Kontrolle von Unterauftragnehmern	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.8 IT-Sicherheitsmanagementsystem	Die Vorgaben und Anforderungen des Standards werden vollständig umgesetzt.
Prüfmethode / Prüfhandlung	
Das zertifizierte IT-Sicherheits-Managementsystem besteht fort. Wirksamkeitstests werden weiterhin regelmäßig durchgeführt. Dazu zählen Schwachstellenscans genauso wie Pen Tests auf im Internet erreichbare Applikationen. **Ausblick auf die Datenschutz-Grundverordnung** Das IT-Sicherheits-Managementsystem setzt wesentliche Anforderungen insbesondere aus Art. 32 DS-GVO um. Prüfhandlung: Dokumentensichtung, Interviews, Einsichtnahme in Prüfergebnisse interner Kontrollhandlungen	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.9 Auftragsmanagementsystem	Die Vorgaben und Anforderungen des Standards werden vollständig umgesetzt.

Prüfmethode / Prüfhandlung

Die für die Leistungserbringung eingesetzten Prozesse sind dokumentiert und als Workflow in den Systemen abgebildet. Zu den zertifizierten Abläufen tritt die Standardisierung und Beschreibung der Auftragsanbahnung.

Auftraggeber erhalten regelmäßige statistische Berichte über die Leistungserbringung, so dass durchgeführte Aktivitäten nachvollziehbar sind.

Ausblick auf die Datenschutz-Grundverordnung

Es wird empfehlen, einen Prozess zur Information des Auftraggebers über behördliche Anfragen einzurichten. Da in den Musterverträgen die Widerspruchsoption aus Art. 28 Abs. 2 DS-GVO vereinbart werden soll, erscheint die Einführung eines Informationsprozesses über neue Unterauftragnehmer angeraten.

Prüfhandlung:

Dokumentensichtung, Interviews, stichprobenhafte Begehung von Büroräumen

4.2. Module in Abhängigkeit des Leistungsumfangs

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
5.1 Vertrag	Die Bewertung erfolgt summarisch ohne Rechtsprüfung und Einbeziehung der Hauptverträge. Die Vorgaben und Anforderungen des Standards werden vollständig umgesetzt.

Prüfmethode / Prüfhandlung

Gemäß § 11 BDSG sind Aufträge zur Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten schriftlich zu erteilen.

Soweit der Auftragnehmer hierzu einen eigenen Mustervertrag vorhält, muss er den Anforderungen des § 11 BDSG entsprechen und insbesondere die Weisungen zu den technischen und organisatorischen Maßnahmen entsprechend der Anlage des § 9 BDSG in angemessener Weise beinhalten.

Die MedicalContact AG bietet leistungsbezogene Musterverträge zur Auftragsdatenverarbeitung standardmäßig an.

Diese beziehen sich insbesondere auf die

- Umsetzung der Anforderungen der §§ 80 und § 78a SGB X (Krankenversicherungsträger) / §§ 9 und 11 BDSG (Unternehmen).
- Kontrollrechte des Auftraggebers.
- Umgang mit Auskunfts-, Lösch-, Sperr- und Berichtigungsbegehren.
- Regelungen zur vertraglichen Bindung von Unterauftragnehmern an die Weisungen des Auftraggebers.

Ein Prüfungsgesichtspunkt war die Frage, ob es sich um eine Auftragsdatenverarbeitung handelt, die sich u.a. durch ein umfassendes Weisungsrecht des Auftraggebers gegenüber einer Funktionsübertragung abgrenzt. Die

Musterverträge zur Auftragsdatenverarbeitung enthalten angemessene Regelungen zur Weisungsbefugnis des Auftraggebers. Die Weisungen werden in Workflows durch ein entsprechendes CRM-System abgebildet, so dass die Einhaltung gewahrt und Dokumentation durchgeführt wird.

Die Leistungserbringung erfolgt für beide Leistungen ausschließlich auf der Basis von Weisungen der Auftraggeber. Diese umfassen insbesondere Inhalte und Ziele der Informationsmaterialen und Beratungsgespräche und legen im Versorgungsmanagement (Morbiditätsmanagement) auch die teilnehmenden Versicherten fest. Aus diesem Grund handelt es sich um eine Auftragsdatenverarbeitung. Das im betrieblichen Gesundheitsmanagement für Unternehmen vereinbarte Verbot, Daten von am Programm teilnehmenden Mitarbeiter dem Arbeitgeber zu übermitteln, stellt die Vertraulichkeit für die Arbeitnehmer sicher und steht der Auftragsdatenverarbeitung nicht entgegen.

Ausblick auf die Datenschutz-Grundverordnung

Es wird empfohlen die geplante Anpassung der Musterverträge an die Anforderungen von Art. 28 DS-GVO fristgerecht vorzunehmen.

Prüfhandlung:

Dokumentensichtung

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
5.2 Beendigung der Leistungsbeziehung	Die Vorgaben und Anforderungen des Standards werden vollständig umgesetzt.

Prüfmethode / Prüfhandlung

Die zertifizierten Prozesse zur Beendigung der Leistungsbeziehung, sowie zum Ausstieg einzelner Klienten aus der Leistungserbringung sind unverändert und wirksam.

Die Anregung aus der Zertifizierung, Ansprechpartner vom Kunden zu löschen, wurde umgesetzt.

Ausblick auf die Datenschutz-Grundverordnung

Die Vorgaben der DS-GVO zur Beendigung der Leistungsbeziehung, d.h. insbesondere zur Löschung der im Rahmen des Auftrags verarbeiteten Daten, werden umgesetzt.

Prüfhandlung:

Dokumentensichtung, Interviews

5. Prüfergebnis / Prüfvermerk

Die im Scope des Audits stehenden Leistungen

1. Versorgungsmanagement (Morbiditätsmanagement) für Krankenversicherungsträger
2. Betriebliches Gesundheitsmanagement für Unternehmen

werden gemäß den Erkenntnissen des Audits nach den Maßgaben des DATENSCHUTZSTANDARD DS-BVD-GDD-01 "Anforderungen an Auftragnehmer nach § 11 BDSG" angeboten und erbracht.

Daher wird die Verlängerung des Zertifikats empfohlen.

Bemerkungen der DSZ Datenschutz Zertifizierungsgesellschaft mbH

Das Siegel wird erteilt

Nummer des Zertifikats: U-003

Gültigkeit des Zertifikats: 24.11.2019