Bericht

zum Zertifizierungsaudit nach

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

für

MedicalContact AG

über die Leistungen

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

Berichtersteller	Dr. Niels Lepperhoff
Zertifizierungs-nummer DSZ.	Z-001
Anschrift	Xamit Bewertungsgesellschaft mbH Monschauer Str. 12 40549 Düsseldorf
Berichts-Datum	20.10.2015

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	X Erstprüfung ☐ Verlängerung	30.09.2015 10 Tage

1.1. Ziel des Audits

Das Ziel des Audits war eine Überprüfung der im Anwendungsbereich beschriebenen Leistung, 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 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.

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 und
b) des Betrieblichen Gesundheitsmanagements 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).

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 Zertifizierungsaudit der Leistungen

a) Versorgungsmanagement (Morbiditätsmanagement) für Krankenversicherungsträger und
b) Betriebliches Gesundheitsmanagement für Unternehmen

fand im Zeitraum vom 30.09.2015 bis zum 19.10.2015 statt. Dem Auditor standen zahlreiche Dokumente wie z.B. Prozessbeschreibungen, Vertragsmuster, technische Beschreibungen und

Konzepte zur Einsichtnahme vor Ort zur Verfügung. Weitere Dokumente wurden im Rahmen der Vor-Ort-Termine gezeigt und erläutert. In Vor-Ort-Terminen 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 und
b) Betriebliches Gesundheitsmanagement 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.

Die Anpassung des Standardangebots durch Umsetzung spezieller Anforderungen oder Weisungen von Auftraggebern ist insbesondere über Change-Prozesse vorgesehen. Diese werden für interne Changes entsprechend angewendet. Hierbei ist durch die Prozessgestaltung sichergestellt, dass die Anpassungen dahingehend geprüft und gestaltet werden können, dass durch sie das auditierte Schutzniveau der Dienstleistungserbringung nicht unterschritten wird.

Die Aufgabenverteilung und Verantwortung des Auftraggebers sind durch vertragliche Vereinbarung festgelegt. Sie werden durch Prozesse und systemgestützte Workflows umgesetzt, die Mitwirkungen des Auftraggebers sowie auch Aktivitäten von Unterauftragnehmer umfassen. Die Leistungserbringung ist durch eine umfangreiche Protokollierung nachvollziehbar und den verantwortlichen Personen zurechenbar.

Die Leistungserbringung sowohl durch die MedicalContact AG selber wie durch Unterauftragnehmer erfolgt soweit wie möglich innerhalb der Systeme der MedicalContact AG. Dadurch wird eine durchgängige Dokumentation, Workflowsteuerung und Sicherheit der Daten ermöglicht.

Aktive Managementsysteme kontrollieren die Leistungserbringung, die Einhaltung von Vertragsvereinbarungen und Datenschutzvorschriften sowie die Wirksamkeit der eingesetzten IT-Sicherheitsmaßnahmen. Diese Kontrollen erstrecken sich auf die interne Leistungserbringung und auch auf Unterauftragnehmer.

Angemessene Maßnahmen und Prozesse zu Datenschutz und IT-Sicherheit wurden durch Dokumentationen bzw. im Vor-Ort-Termin (Besichtigung des Rechenzentrums (RZ), der Unterauftragnehmer, Interviews mit Fachverantwortlichen, Demonstrationen) schlüssig dargestellt.

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

Mit Schreiben vom 30.9.2015 hat die DSZ den Antrag der MedicalContact AG auf Reduktion des Prüfkontingents in Höhe von 48 Std. bewilligt, da beide Leistungen überwiegend identische Prozesse nutzen und gleichartig aufgebaut sind.

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 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
Die Herstellung ist modular aufgebaut. Die Module werden Auftraggebern hinsichtlich ihrer Leistung wie auch ihres Ablaufs allgemein beschrieben. Die Leistungserbringung erfolgt durch standardisierte und beschriebene Prozesse sowie innerhalb verschiedener CRM-Systeme. Workflows unterstützen eine auftragsgemäße Leistungserbringung. Auftraggeber erhalten regelmäßig nicht personenbezogene Berichte über die Leistungserbringung. Beteiligte Unterauftragnehmer werden bei Vertragsschluss bekannt gegeben. Personenbezogene Daten werden ausschließlich im RZ gespeichert. Massenaussendungen erfolgen durch zwei Druckstraßen. Zur standardisierten Datenerhebung vor Ort beim Versicherten führen beauftragte lokale Pflegedienste/Pflegeberater Hausbesuche durch, um eine bundesweite Abdeckung sicherzustellen. **Prüfungshandlung:** Dokumentensichtung, Interviews, Demonstration ausgewählter Prozesse vor Ort, Beobachtung von Mitarbeitern bei der Bearbeitung vor Ort, Vor-Ort-Prüfung des RZ, einer Druckstraße und eines Pflegedienstes

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: Für die Übermittlung der für die Leistungserbringung notwendigen personenbezogenen Daten stehen Auftraggebern verschiedene Wege zur Verfügung: • Eröffnung einer Datenbereitstellung via bitInfoNet: Die Datenübermittlung erfolgt innerhalb des RZ. • Einstellen in das Geschäftskundenportal (GKP) der MedicalContact AG: Das GKP dient dem Datenaustausch und wird durch unterschiedliche Maßnahmen gesichert, wie z.B. Transportverschlüsselung, individuelle Nutzerrechte, automatische Datenlöschung und Systemhärtung. • Verwendung der Datenaustauschplattform des Auftraggebers. Pflegedienste/Pflegeberater verwenden das GKP, um ihre Dokumentation zu übermitteln. Im Rahmen von Telefonaten mit Versicherten werden weitere für die Leistungserfüllung benötigte Daten vom Versicherten erfragt und in einem CRM-System für die weitere Leistungserbringung gespeichert. Datenimporte und Dateneingaben werden systemseitig automatisch protokolliert. **Betriebliches Gesundheitsmanagement für Unternehmen:** Personenbezogene Daten der Mitarbeiter des Auftraggebers werden nicht an die MedicalContact AG übermittelt. Der Auftraggeber informiert seine Mitarbeiter in eigener Verantwortung über das Angebot. Mitarbeiter melden sich anschließend freiwillig telefonisch bei der MedicalContact AG. Gesundheitstelefon: Es werden nur dann personenbezogene Daten (Adresse) erfasst, wenn ein Rückruf (Name, Telefonnummer) vereinbart oder eine postalische Zusendung von Informationen (Name, Adresse) gewünscht wird. Coaching: Nach Abgabe einer Einwilligungserklärung, die der Arbeitgeber aushändigt, speichert die MedicalContact	

AG die telefonisch gemachten Angaben, um die Beratung erbringen zu können.

Mitarbeiterbefragung: Die Fragenbögen werden vom Auftraggeber verteilt. Die Mitarbeiter senden Ihre anonymen Antworten direkt an die MedicalContact AG.

Dateneingaben werden systemseitig automatisch protokolliert.

Prüfungshandlung:

Dokumentensichtung, Interviews, Demonstration ausgewählter Prozesse vor Ort, Beobachtung von Mitarbeitern bei der Bearbeitung vor Ort, Vor-Ort-Prüfung eines Pflegedienstes

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. Die Prozesse umfassen die Mitwirkung des Auftraggebers, die Leistungserbringung beim Auftragnehmer wie auch die Tätigkeiten der Unterauftragnehmer. Sie beschreiben die gesamte Lieferkette. Soweit wie möglich erfolgt die Leistungserbringung auf den Systemen der MedicalContact AG, die durch Workflows eine prozesskonforme Leistungserbringung unterstützen.

Die Daten von Klienten (Versicherte und Betreute im Rahmen des Betrieblichen Gesundheitsmanagements) werden jeweils in einem CRM-System verwaltet. Die Verarbeitung der Daten von Klienten erfolgt ausschließlich durch die jeweiligen CRM-Systeme, die von Hilfsanwendungen unterstützt werden, so dass eine geschlossene Umgebung entsteht. Eine Bearbeitung mittels Office-Produkten erfolgt nicht.

Der Vertrieb ist der zentrale Ansprechpartner für die Auftraggeber und koordiniert die vertragskonforme Leistungserbringung. Weisungen werden u.a. in einem CRM-System dokumentiert, so dass die Workflows weisungskonform gesteuert werden. Berater haben Zugriff auf die relevanten Informationen am Arbeitsplatz und werden geschult.

Unterauftragnehmer werden von den, für sie fachlich zuständigen, Fachabteilungen betreut.

Auftraggeber erhalten regelmäßig Berichte über die erbrachte Leistung, die sich auf die manuelle und systemseitige Dokumentation der Leistungserbringung stützen.

Zugriffsrechte werden anhand eines Rollenkonzepts, das tätigkeitsorientiert aufgebaut ist, über einen definierten Prozess vergeben.

Daten von Klienten werden automatisch gelöscht, sobald der Zweck der Verarbeitung entfallen ist und der abschließende Bericht erstellt wurde (z.B. Vertragsende, Ausstieg aus dem Betreuungsprogramm). Je nach Programm können gesetzliche Aufbewahrungsfristen eine längere Speicherung vorschreiben.

Die Qualität der Leistungserbringung wird durch verschiedene Maßnahmen kontinuierlich überprüft. Zu den Maßnahmen zählen bspw. Mithören von Beratungsgesprächen, automatische Konsistenzprüfungen und Fallbesprechungen.

Prüfungshandlung:

Dokumentensichtung, Interviews, Demonstration ausgewählter Prozesse vor Ort, Beobachtung von Mitarbeitern bei der Bearbeitung vor Ort, Vor-Ort-Prüfung des RZ, einer Druckstraße und eines Pflegedienstes

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: Die Prozesse zur Datenübermittlung an Auftraggeber, Unterauftragnehmer oder zur Kommunikation mit dem Versicherten sind definiert und werden durch beteiligte Systeme gesteuert und protokolliert. Dies schließt Freigaben durch den Auftraggeber wie auch Aktivitäten von Unterauftragnehmern ein. Je nach Leistung erhalten die Versicherten Informationsmaterial per Post oder persönliche telefonische Beratung. Der Versand erfolgt für kleine Mengen oder bei personalisierten Anlagen durch die MedicalContact AG selber. Große Stückzahlen werden durch die Druckstraßen versandt. Dazu erhalten diese die Druckdaten über das Geschäftskundenbereich (GKP). Die Druckstraßen sind verpflichtet, die Druckdaten nach Auftragserledigung zu löschen. Die Briefe werden von einem Postunternehmen im Auftrag der MedicalContact AG zeitnah abgeholt. Die Beratung erfolgt telefonisch nach Identitätsprüfung durch die MedicalContact AG. Sofern Auftraggeber über die Leistung für einzelne Versicherte entscheiden wollen oder qua Gesetz müssen, erhalten sie die entsprechenden Daten über das Geschäftskundenbereich (GKP) bereitgestellt. Die Genehmigung erfolgt ebenfalls über das GKP. Auftraggeber erhalten regelmäßig Berichte über die erbrachte Leistung, die keinen Personenbezug aufweisen. **Betriebliches Gesundheitsmanagement für Unternehmen:** Gesundheitstelefon: Klienten erhalten zusätzlich zu telefonischen Auskünften auch Informationen per Post. Der Versand erfolgt durch die MedicalContact AG. Coaching: Im Rahmen des Coaching rufen Mitarbeiter der MedicalContact AG Klienten an. Die Beratung erfolgt ausschließlich telefonisch nach Identitätsprüfung. Das beauftragende Unternehmen erhält einen Leistungsbericht, der keinen Personenbezug aufweist. Der Zugriff auf die personenbezogenen Daten ist vertraglich ausgeschlossen. **Prüfungshandlung:** Dokumentensichtung, Interviews, Demonstration ausgewählter Prozesse vor Ort, Beobachtung von Mitarbeitern bei der Bearbeitung vor Ort, Vor-Ort-Prüfung einer Druckstraße	

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 und,
- Auftragskontrolle

zählen. Die Erhebung und Verarbeitung von personenbezogenen Daten der Klienten und auch der Kundenansprechpartner mittels CRM-Systeme erlaubt die Umsetzung des Trennungsgebots durch logische Kennzeichnung nach Kunden und Auftrag sowie die Speicherung in getrennten Systemen nach Betroffenengruppen. Jeweils ein CRM für Kunden, Versicherte und die betreuten Mitarbeiter im Rahmen des Betrieblichen Gesundheitsmanagements wird eingesetzt. Die Protokollierung der Datenänderung innerhalb der CRM-Systeme trägt der Eingabekontrolle Rechnung. Zusätzliche Protokolle sowohl auf Netzwerk- und PC-Ebene setzen das Protokollkonzept um. Die Dokumentation der Workflowschritte sorgt für eine wirksame Auftragskontrolle, die auch die Aktivitäten von Unterauftragnehmern umfasst.

Prozesse zur Bearbeitung von Auskunftsersuchen, Berichtigungswünsche, Lösch- und Sperrbegehren sind beschrieben und in den CRM-Systemen abgebildet. Die notwendigen Schnittstellen zu den Auftraggebern sind definiert. Für beide Leistungen laufen die jeweiligen Prozesse nach dem gleichen Schema ab. Beim Versorgungsmanagement (Morbiditätsmanagement) erfolgt die Entscheidung über die Umsetzung sowie die Umsetzung selber beim Auftraggeber. Wenn die Klientendaten nicht auch beim Auftraggeber gespeichert sind, setzt die MedicalContact AG auf Weisung des Auftraggebers die Beauskunftung, Berichtigung, Sperrung, Löschung um, in diesem Fall erfährt der Auftraggeber nicht den Inhalt der Klientendaten, so dass u.a. die Vertraulichkeit der Beratungsinhalte gewahrt bleibt. Beim betrieblichen Gesundheitsmanagement liegt die Entscheidung und Umsetzung bei der MedicalContact. Da den teilnehmenden Mitarbeitern des Auftraggebers Vertraulichkeit zugesichert worden ist, wird der Auftraggeber, d.h. deren Arbeitgeber, nicht informiert.

Ein Prozess zum Umgang mit Sicherheitsvorfällen existiert.

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, Demonstration ausgewählter Prozesse vor Ort

4.1.4. IT-Sicherheitskonzept

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.6 IT-Sicherheitskonzept	Die Vorgaben und Anforderungen des Standards werden vollständig umgesetzt.

Prüfmethode / Prüfhandlung

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 systematische Betrachtung von Risiken oder Gefahren sowie die Ableitung von Maßnahmen sind nicht erkennbar. Diese Schwäche wird durch die getroffenen Maßnahmen erkennbar kompensiert.

Die Server werden im Rahmen eines Housing im RZ betrieben. Der Dienstleister hat potentiellen Zugriff auf Daten des Auftraggebers. Die Sicherheitsmaßnahmen des RZ sind im IT-Sicherheitskonzept integriert.

Unterauftragnehmern wie Druckstraßen und Pflegediensten/Pflegeberatern werden wesentliche Sicherheitsmaßnahmen vertraglich vorgeschrieben. Generell werden Daten soweit wie möglich auf Systemen der MedicalContact AG auch durch Unterauftragnehmer verarbeitet. Bei der Verarbeitung auf Systemen der Unterauftragnehmer liegt der Fokus auf Kapselung innerhalb deren Systeme.

Die IT-Sicherheitsmaßnahmen gehen - sachlich angemessen - über den Schutzbedarf normal des BSI hinaus. Durch die strikte Datenverarbeitung innerhalb geschlossener Systeme können die Klientendaten einfacher unter Kontrolle gehalten werden. Regelmäßige Schwachstellentests helfen neue Sicherheitslücken zu entdecken.

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, Vor-Ort-Prüfung des RZ, einer Druckstraße und eines Pflegedienstes

4.1.5. Managementsysteme

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.7 Datenschutz-Managementsystem	Die Vorgaben und Anforderungen des Standards werden vollständig umgesetzt. Es wird angeregt, stärker auf den Aufbau eines Datenschutz-Managementsystems bei Unterauftragnehmern hinzuwirken.

Prüfmethode / Prüfhandlung

Ein Datenschutz-Managementsystem zur nachhaltigen Sicherstellung des Datenschutzes ist dokumentiert und eingeführt. Hierzu zählt insbesondere:

- Die wirksame Bestellung eines Datenschutzbeauftragten (Bestellurkunde und Fachkunde sind nachgewiesen).
- Prozesse zur stichprobenartigen Kontrolle ausgewählte Prozesse und der angebotenen Leistung im Hinblick auf ihre Datenschutzkonformität.
- Prozesse zur Kontrolle von Unterauftragnehmern sind dokumentiert und im Wirkbetrieb. Die Kontrolle der Unterauftragnehmer geschieht regelmäßig durch Interviews und Vor-Ort-Begehungen. Dadurch gleicht das Datenschutz-Managementsystem der MedicalContact AG die nicht durchgängig vorhandenen Datenschutz-Managementsysteme der Unterauftragnehmer aus.

Neben eigenen Kontrolltätigkeiten unterstützt das Datenschutz-Managementsystem die Kontrolltätigkeiten von Auftraggebern.

Prüfhandlung:

Dokumentensichtung, Interviews, Demonstration ausgewählter Prozesse vor Ort, Vor-Ort-Prüfung des RZ, einer Druckstraße und eines Pflegedienstes

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.8 IT-Sicherheitsmanagementsystem	Die Vorgaben und Anforderungen des Standards werden umgesetzt. Es wird angeregt, eine systematische Betrachtung von Gefahren sowie die Ableitung von Maßnahmen aus den Gefahren in das IT-Sicherheitskonzept aufzunehmen.

Prüfmethode / Prüfhandlung

Ein IT-Sicherheits-Managementsystem ist dokumentiert und eingeführt. Die Bestellung eines IT-Sicherheitsbeauftragten (Bestellung, Aufgaben / Befugnisse und Fachkunde) ist dokumentiert.

Regelmäßige Prüfungen auf Schwachstellen finden statt. Der IT-Sicherheitsbeauftragte ist im Change Management-Prozess involviert, um die Auswirkungen von Änderungen auf die IT-Sicherheit zu beurteilen.

Ein Prozess zur kontinuierlichen Verbesserung der IT-Sicherheit ist etabliert, der sich u.a. aus internen und externen Prüfergebnissen speist.

Das RZ verfügt über ein ISO 27001 zertifiziertes IT-Sicherheitsmanagementsystem.

Unterauftragnehmern wie Druckstraßen und Pflegediensten/Pflegeberatern werden wesentliche Sicherheitsmaßnahmen vertraglich vorgeschrieben und deren Einhaltung kontrolliert. Dadurch wird das teilweise Fehlen von IT-

Sicherheitsmanagementsystemen bei Unterauftragnehmern ausgeglichen. Prüfhandlung: Dokumentensichtung, Interviews, Demonstration ausgewählter Prozesse vor Ort, Vor-Ort-Prüfung des RZ, einer Druckstraße und eines Pflegedienstes

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. Ein Prozess zur Weisungsbearbeitung sowie interne Changes (Change Management) sind dokumentiert und teilweise durch Workflows gesteuert. Die stichprobenartige Sichtung der Workflow-Protokolle in den CRM-Systemen ergab eine prozesskonforme Nutzung. Dieser Eindruck wurde durch die Beobachtung der Sachbearbeitung bei der Prozessbearbeitung gefestigt. Die sachgerechte Einarbeitung wird durch ein Einarbeitungskonzept erreicht, das verschiedene Stufen der fachlichen Beurteilung umfasst. Mitarbeiter werden über Prozessänderungen und Kundenweisungen informiert. Die ordnungsgemäße Bearbeitung der Aufträge wird durch unterschiedliche Maßnahmen, wie eine Workflowsteuerung, die auch auftraggeberspezifische Vereinbarungen berücksichtigt, systemseitige Plausibilitätsprüfungen sowie Qualitätskontrollen wie z.B. Mithören, kontrolliert. Ein Mithören erfolgt offen und nach vorheriger Einwilligung beider Gesprächspartner. Auftraggeber erhalten regelmäßige statistische Berichte über die Leistungserbringung, so dass durchgeführten Aktivitäten nachvollziehbar sind. Prüfhandlung: Dokumentensichtung, Interviews, Demonstration ausgewählter Prozesse vor Ort, Vor-Ort-Prüfung einer Druckstraße und eines Pflegedienstes	

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 entspre-	

chend 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 einen 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.

Prüfhandlung:

Dokumentensichtung

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
5.2 Beendigung der Leistungsbeziehung	Die Vorgaben und Anforderungen des Standards werden vollständig umgesetzt. Die Umsetzung der Löschung von Kundendaten steht aus. Der Handlungsbedarf ergibt sich aus der in Zukunft ablaufenden Aufbewahrungsfrist.

Prüfmethode / Prüfhandlung

Prozesse zur Beendigung der Leistungsbeziehung, sowie zum Ausstieg einzelner Klienten aus der Leistungserbringung sind dokumentiert und wirksam. Generell werden Klientendaten nach Erstellung des letzten sie betreffenden Leistungsberichts an den Auftraggeber gelöscht, soweit diese nicht ohne Personenbezug für Abrechnungszwecke benötigt werden.

Sofern gesetzlich nicht vorgeschrieben erhalten Auftraggeber die, von der MedicalContact AG im Rahmen der Beratung erhobenen Daten der Klienten nicht vor der Löschung ausgehändigt.

Unterauftragnehmer müssen personenbezogene Daten unmittelbar nach Auftragsbearbeitung löschen/vernichten oder an den Auftragnehmer per Einschreiben zusenden.

Zugriffsrechte zum Geschäftskundenbereich werden entzogen.

Prüfhandlung:

Dokumentensichtung, Interviews, Vor-Ort-Prüfung einer Druckstraße und eines Pflegedienstes

5. Audit Teilnehmer

Beteiligte Stellen / Unterauftragnehmer / Dienstleister / sonstige Dritte

Name / Adresse	Aufgabe bei der Leistungserbringung
RZ: BITMARCK Service GmbH Brunnenstraße 15-17 45128 Essen	Housing der Racks für Produktivbetrieb und Backup
Druckstraße: Wagner Druck und Werbe GmbH Heinrich-Held-Straße 50 45133 Essen	Massendruck im Auftrag der MedicalContact AG
Pflegedienst: DRK KV Duisburg Mitte/Süd Mündelheimer Str. 24 47259 Duisburg	Standardisierte Erhebung bei Hausbesuchen im Auftrag der MedicalContact AG

6. 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 Erteilung des Zertifikats empfohlen.

Bemerkungen der DSZ Datenschutz Zertifizierungsgesellschaft mbH

Das Siegel wird erteilt

Ja

Nummer des Zertifikats:

U-003

Gültigkeit des Zertifikats:

24.11.2017