Auftragsverarbeitungsvereinbarung

zwischen

Bernhard Hettesheimer

Herr Bernhard Hettesheimer

Am Kindsberg 1

66862 Kindsbach

Auftraggeber (Verantwortlicher)

und

jameda GmbH
St. Cajetan-Straße 41
81669 München

Auftragnehmer (Auftragsverarbeiter)

1. Gegenstand und Dauer der Verarbeitung

a. Der Auftrag umfasst Folgendes:

Der Auftragnehmer stellt dem Auftraggeber eine webbasierte Plattform zur Verfügung. Dabei handelt es sich zum einen um einen Kalender, mit dem die Praxis in die Lage versetzt wird, im Rahmen der notwendigen Praxisorganisation die Termine der Patienten zu verwalten (sogenannte Option „Online Terminvergabe") und zum anderen um eine Plattform zur Terminvereinbarung und Durchführung von Videosprechstunden mit Gesprächspartnern (z.B. Patienten) (sogenannte Option „Videosprechstunde"). Hierüber haben die Parteien unter Zugrundelegung eines Angebots des Auftragnehmers vom 07/05/2020 und der Einbeziehung der Allgemeinen Geschäftsbedingungen des Auftragnehmers einen Hauptvertrag zur Erbringung der Dienstleistungen geschlossen.

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages.

b. Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Vertrag wird auf unbestimmte Zeit geschlossen und endet automatisch mit der Beendigung des Hauptvertrages, bzw. der Kündigung beider Optionen („Online Terminvergabe" und „Videosprechstunde"). Sollte nur eine der Optionen separat gekündigt werden, gilt dieser Vertrag fort, solange der Hauptvertrag im Übrigen fortbesteht.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

Zweck der Datenverarbeitung ist die Bereitstellung eines Praxiskalenders für die Organisation von Terminen und die Terminvereinbarung und Durchführung von Videosprechstunden.

a. Art der Verarbeitung (entsprechend der Definition in Art. 4 Nr. 2 DSGVO):

Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder die Verknüpfung, Einschränkung, Löschen oder die Vernichtung.

b. Art der personenbezogenen Daten (entsprechend der Definition in Art. 4 Nr. 1, 13, 14 und 15 DSGVO):

- Daten zur Person (Titel, Name, Vorname, Geburtsdatum, Geschlecht)
- Adress-Daten (Ort, Straße, PLZ)
- Kontaktdaten (E-Mail-Adr., Telefon-Nr., Handynummer)
- Zahlungs-/Bank-Daten (Konto-Nr., Kreditkarten-Nr., ...)
- technische Daten (IP-Adresse, Benutzer-Kennung, Passwort, Cookie-ID, Mobil-ID, ...)
- besondere Arten von Daten (gesundheitsbezogene Daten), insbesondere Termindaten von Gesprächspartnern (z.B. Patienten), Versicherungsstatus, Termindaten (Datum, Uhrzeit, Terminart) Freitextnachricht, Notizen

c. Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DSGVO):

- Interessenten / Patienten des Auftraggebers / Gesprächspartner in der Videosprechstunde

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

a. Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die

Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

b. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

c. Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen schriftlich oder in einem dokumentierten elektronischen Format.

d. Der Auftraggeber ist berechtigt, sich wie unter Ziff. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

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

f. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

a. Weisungsberechtigte Personen des Auftraggebers sind:

_____

_____

_____

(Vorname, Name, Organisationseinheit, Telefon, E-Mail)

b. Weisungsempfänger beim Auftragnehmer sind die bestellten Datenschutzkoordinatoren, zu erreichen unter:

E-Mail: datenschutz@jameda.de
Tel.: 089 - 2000 185 70

c. Für Weisung zu nutzende Kommunikationskanäle:

jameda GmbH Datenschutz
St. Cajetan-Straße 41
81669 München
datenschutz@jameda.de

5. Pflichten des Auftragnehmers

a. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

b. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

c. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

d. Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftrag-geber sorgfältige und regelmäßige Überprüfungen in seinem Bereich durchzuführen und dies zu dokumentieren.

e. Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DSGVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an folgende Stelle des Auftraggebers weiterzuleiten:

_____

_____

(Vorname, Name, Organisationseinheit, Telefon, E-Mail)

f. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

g. Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

h. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

i. Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO). Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

j. Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind.

k. Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

l. 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 für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Die Verschwiegenheitsverpflichtung berücksichtigt insbesondere auch die besonderen Anforderungen des § 203 StGB. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

m. Beim Auftragnehmer ist als Beauftragter für den Datenschutz

Jürgen Kempter
Hubert Burda Media Holding Kommanditgesellschaft
Hauptstraße 130 in 77652 Offenburg
konzerndatenschutz@burda.com

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener

Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

a. Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Zustimmung des Auftraggebers gestattet, Art. 28 Abs. 2 Satz 1 Alt. 1 DSGVO, welche auf einem der o.g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

b. Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzuhalten, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

c. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

d. Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

e. Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) sorgfältig zu überprüfen. Das Ergebnis der Überprüfung ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

f. Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

g. Zurzeit sind für den Auftragnehmer die in Anhang I mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

8. Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

a. Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird. Hierzu wird eine anerkannte Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten der Betroffenen berücksichtigt.

b. Im Anhang II sind die technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach dem Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dargestellt.

c. Auftragnehmer und Auftraggeber stimmen sich über ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung ab.

d. Der Auftragnehmer hat in regelmäßigen Abständen bzw. bei gegebenem Anlass, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DSGVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber auf Anfrage mitzuteilen.

e. Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

f. Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DSGVO

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber - spätestens mit Beendigung der Leistungsvereinbarung - hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht zu vernichten oder nach vorheriger Aufforderung auszuhändigen. Dies gilt auch, wenn eine gebuchte Option separat gekündigt wurde, für die im Hinblick auf diese Option verarbeiteten personenbezogenen Daten. Gleiches gilt für Test- und Ausschussmaterial. Die Löschung oder Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format auf Anfrage zu bestätigen.

10. Haftung

Die gesetzliche Haftung von Auftraggeber und Auftragnehmer bestimmt sich nach den Vorgaben des Art. 82 DSGVO. Für die vertragliche Haftung zwischen Auftraggeber und Auftragnehmer finden die Haftungsregelungen aus den Allgemeinen Geschäftsbedingungen des Auftragnehmers Anwendung.

11. Sonstiges

a. Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

b. Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

c. Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

d. Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

e. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

München, 13/05/2020	Kindsbach, 13/05/2020 13.05.2020 | 15:13 CEST
(Ort, Datum)	(Ort, Datum)
	DocuSigned by: Bernhard Hettesheimer 119F9E12D1EF4EE...
Dr. Florian Weiß und Fritz Edelmann	Bernhard Hettesheimer
Auftragnehmer	**Auftraggeber** (Name Arzt / Heilberufler eintragen)

Anlagen

Anhang I: Zugelassene Subunternehmer gem. Ziffer 7. g.
Anhang II: Sicherheitshandbuch der jameda GmbH

jameda

Anhang I: Zugelassene Subunternehmer gem. Ziffer 7. g.

Name	Anschrift	Auftragsinhalt
CM Telecom Germany GmbH	Mainfrankenpark 53 97337 Dettelbach	SMS-Versand
sms77 e.K.	Köhlerkoppel 19 24109 Melsdorf	SMS-Versand
Burdas Services GmbH	Arabellastraße 23 81925 München	Verwaltung, Rechnungswesen, Personaldienstleistungen
Amazon Web Services Inc.	410 Terry Avenue North, Seattle, WA 98109-5210, USA	Hosting
GTC TeleCommunication GmbH	Zimmermannstraße 15 70182 Stuttgart	Fax-Versand
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen	Hosting
Sipgate GmbH	Gladbacher Straße 74 40219 Düsseldorf	Telefonische Anfragen
ZOHO CORPORATION B. V.	Hoogoorddreef 15 1101BA Amsterdam	Verwaltung, Kundenservice, Vertrieb

jameda

Anhang II: Sicherheitshandbuch

Sicherheitshandbuch

Ein Überblick über die technischen und organisatorischen Maßnahmen

der

jameda GmbH

Version 15.05.2019

jameda

Inhalt

1. Allgemeine Angaben

Die jameda GmbH ist ein Tochterunternehmen des Medienkonzerns Hubert Burda Media.
Auf jameda.de finden Patienten unter allen niedergelassenen Ärzten Deutschlands den passenden Arzt für ihre Bedürfnisse. Dabei helfen ihnen die Empfehlungen anderer Patienten und die von den Ärzten bereitgestellten Informationen. Zudem können Patienten auf den Profilen vieler Ärzte und weiterer auf jameda.de gelisteter Leistungserbringer im Gesundheitswesen ihren Termin direkt online buchen. Die Leistungen im Hinblick auf jameda.de werden von dem Standort München aus erbracht.
Darüber hinaus bietet die jameda GmbH unter anderem unter dem Label Patientus einen zertifizierten Videodienst für die Kommunikation im medizinischen und therapeutischen Bereich an. Diese Leistung umfasst Videogespräche zwischen Leistungserbringern im Gesundheitswesen und deren Gesprächspartnern (z.B. Patienten) und die dazugehörige Terminkoordination über eine Online-Plattform (www.jameda.de). Die Leistungen im Hinblick auf die Videosprechstunde werden vom Standort Berlin aus erbracht.

Ziel des Sicherheitshandbuches

Das vorliegende Dokument gibt Auskunft über die getroffenen technischen und organisatorischen Maßnahmen zur Einhaltung des Datenschutzes, zu deren Gewährleistung sich das Unternehmen gemäß Datenschutzgrundverordnung (DSGVO) und neuem Bundesdatenschutzgesetz (BDSG-neu) verpflichtet. Es wird gezeigt, wie ein - dem jeweiligen Risiko der Datenverarbeitung angemessenes - Schutzniveau erreicht wird. Das Unternehmen kommt damit der von Seiten des Gesetzgebers geforderten Dokumentations- und Informationspflicht in umfassender Weise nach. Das vorliegende Dokument kann im Rahmen datenschutzrechtlicher Prüfungen, z.B. durch öffentliche Stellen wie Aufsichtsbehörden, herangezogen werden. Es dient des Weiteren als Grundlage für die Auftragsverarbeitung und kann in diesem Zusammenhang einem Vertrag zur Auftragsverarbeitung mit dem jeweiligen Auftraggeber als Anlage beigefügt werden.Das vorliegende Dokument wird bei Bedarf aktualisiert. Änderungen oder Ergänzungen dürfen nur nach Genehmigung durch den Dokumenteneigentümer vorgenommen werden.

Ansprechpartner des Auftragnehmers

jameda GmbH, St. Cajetan-Straße 41, 81669 München E-Mail: datenschutz@jameda.de
Dr. Florian Weiß und Fritz Edelmann, Tel. 089 / 2000 185 80, E-Mail: gesundheit@jameda.de

Datenschutzbeauftragter desAuftragsnehmers

Jürgen Kempter, E-Mail: konzerndatenschutz@burda.com

Ansprechpartner IT

Michael Nowak (CTO), Tel. 089 / 200 185 80, E-Mail: gesundheit@jameda.de

Standorte der Rechenzentren:

Hetzner Online GmbH; Gunzenhausen, Deutschland
Amazon Web Services, Inc.; Frankfurt a. M., Deutschland

jameda

2. Organisationskontrolle

Zur Einhaltung der datenschutzrechtlichen Vorgaben gemäß DSGVO und damit der Einhaltung der umfänglichen Nachweis- und Rechenschaftspflicht betreibt Hubert Burda Media konzernübergreifend ein Datenschutzmanagementsystem (DSMS).

Nachfolgend werden die Charakteristika des DSMS genannt und wesentliche Informationen in Bezug auf Aufbau- und Ablauforganisation beschrieben.

Verantwortung der Geschäftsführung

Die rechtliche Verantwortung für die Einhaltung des Datenschutzes liegt beim Unternehmen als Verantwortlichem (Art. 5 Abs. 2 DSGVO) und damit bei der Geschäftsführung. Für Hubert Burda Media bedeutet dies, dass die Geschäftsführung jeder einzelnen Konzerngesellschaft für die Einhaltung des Datenschutzes in ihrer Einheit gegenüber Dritten verantwortlich ist.

Unternehmensintern kann sich die Geschäftsführung zur Wahrnehmung dieser Verantwortung durch interne Ressourcen, wie den Datenschutzkoordinator unterstützen lassen. Die Benennung eines Datenschutzkoordinators entbindet die Geschäftsführung jedoch nicht von ihrer Verantwortung. Sie hat die Arbeit des Datenschutzkoordinators zu begleiten und ihm ausreichend Zeit und Mittel zur Wahrnehmung seiner Aufgaben zur Verfügung zu stellen.

Rollen und Funktionen

Konzern-Datenschutzbeauftragter

Gemäß Art. 37ff. DSGVO hat Hubert Burda Media einen Datenschutzbeauftragten benannt, der in der Rolle des Konzern-Datenschutzbeauftragten eine gesellschaftsübergreifende Funktion innehat.

Der Konzern-Datenschutzbeauftragte verfügt über besonderes datenschutzrechtliches Fachwissen und ist in der Datenschutzpraxis geübt. Er überwacht die Einhaltung des Datenschutzes durch den Verantwortlichen und steht der Geschäftsführung der einzelnen Gesellschaften in Datenschutzfragen beratend zur Seite. Zudem ist er für die Umsetzung der Aufgaben gemäß Art. 39 DSGVO verantwortlich.

Im Außenverhältnis ist er Anlaufstelle für Betroffene und Aufsichtsbehörden.

Die Kontaktdaten des Konzern-Datenschutzbeauftragten sind wie folgt:

Jürgen Kempter, Konzern-Datenschutzbeauftragter
Hubert Burda Media Holding Kommanditgesellschaft
Hauptstraße 130
77652 Offenburg
konzerndatenschutz@burda.com

Datenschutzkoordinatorinnen

Zur Umsetzung der datenschutzrechtlichen Auflagen sind in den einzelnen Gesellschaften sog. Datenschutzkoordinatorinnen benannt worden.

Die Datenschutzkoordinatorin hat im DSMS eine wichtige Rolle. Sie unterstützt seine Geschäftsführung bei der Umsetzung datenschutzrechtlicher Anforderungen in seiner Einheit. Zugleich ist sie für den Konzern-Datenschutzbeauftragten die Schnittstelle in einzelne operative Einheiten.

Prozesse

Zur Einhaltung der datenschutzrechtlichen Vorgaben wurden im Rahmen des DSMSs folgende Prozesse konzernweit implementiert:

- Verzeichnis von Verarbeitungstätigkeit gemäß Art. 30 DSGVO
- Risikobewertung & Datenschutzfolgenabschätzung
- Gewährleistung der Pflichten und Rechte nach Art. 12 bis Art. 23 DSGVO
- Standardabläufe beim Eintritt von Datenschutzvorfällen

Auswahl von Dienstleistern und Lieferanten

Die Auswahl von externen Dienstleistern und Lieferanten erfolgt entsprechend des Einsatzgebietes im Rahmen eines entsprechenden Auswahlverfahrens und nach sorgfältiger Prüfung.

Gemäß den Richtlinien ist die Tätigkeit und Dauer der zu erbringenden Dienstleistungen schriftlich in entsprechenden Verträgen zwischen der jeweiligen Gesellschaft der verantwortlichen Stelle als Auftraggeber bzw. Verantwortlicher und dem Auftragnehmer bzw. Auftragsverarbeiter festgehalten.

Werden im Rahmen eines Auftrages personenbezogene Daten durch den externen Dienstleister verarbeitet, so wird zusätzlich zum Dienstleistungsvertrag ein Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO zwischen Auftraggeber und dem Auftragnehmer abgeschlossen. Der Auftragnehmer hat die technischen und organisatorischen Maßnahmen zum Schutz der zu verarbeitenden personenbezogenen Daten darzulegen.

Die Dokumentation der Auftragsverarbeitung erfolgt im zentralen Datenschutz-Tool.

Datensicherheit durch geschulte Mitarbeiter

Verpflichtung auf das Datengeheimnis

Mitarbeiter werden zu Tätigkeitsbeginn auf das Datengeheimnis sowie die Einhaltung weiterer gesetzlicher Auflagen verpflichtet. Der Prozess unterliegt der Verantwortung von Hubert Burda Media Human Resources.

Das unterzeichnete Formular ist Bestandteil der Vertragsunterlagen des Beschäftigten und in der Personalakte des jeweiligen Mitarbeiters hinterlegt.

Schulung & Sensibilisierung

Jeder Mitarbeiter von Hubert Burda Media ist im Rahmen seiner Tätigkeit für die Einhaltung datenschutzrechtlicher Vorgaben verantwortlich. Darauf wird in der Datenschutzleitlinie verwiesen.

Im Rahmen weiterer Schulungen und Richtlinien werden die Mitarbeiter im Hinblick auf Datenschutzbelange hingewiesen und sensibilisiert.

Mitarbeiter von Hubert Burda Media, die im Rahmen ihrer Funktion mit Aufgaben im Bereich des Daten-schutzes betraut werden, werden über ein dafür vorgesehenes eLearning zu daten-schutz-rechtlichen Themen fachgerecht geschult.

Nachweis der Datensicherheit

Der IT-Sicherheitsbeauftragte ist bei Hubert Burda Media konzernweit für alle Fragen hinsichtlich der Sicherheit von Daten und IT-Systemen verantwortlich.

Im Rahmen seiner Tätigkeit überprüft er die Wirksamkeit von vorhandenen Schutzmaßnahmen, wirkt beratend bei der Planung und Installation neuer Verfahren und Systeme mit. Dabei finden auch die Belange des Datenschutzes Berücksichtigung.

Der IT-Sicherheitsbeauftragte berichtet regelmäßig an die Unternehmensführung über den Zustand der IT-Sicherheit im Unternehmen und schlägt Sicherheitsmaßnahmen vor.

3. Zutrittskontrolle

Das Ziel der Zutrittskontrolle ist es, mit Hilfe geeigneter Maßnahmen, Unbefugte nicht mit Daten in Berührung kommen zu lassen. Dies beginnt damit, die Anlagen, mit denen diese Daten verarbeitet werden, räumlich nicht frei zugänglich zu machen.

Betriebsgelände und Bürogebäude Standort München

Die jameda GmbH ist mit ihrer Hauptniederlassung am Standort St. Cajetan-Straße 41 in 81669 München vertreten. Der Zutritt in das Gebäude und damit der Zugang in die allgemeinen Büroräume wird über Zutrittskontrollsysteme (Chipleser) geregelt. Der Zutritt der Mitarbeiter ist nur mittels des entsprechenden Chips und der für das Gebäude entsprechenden Freischaltung möglich. Die Zugangstür ist immer verschlossen. Der Zutritt von Besuchern, Lieferanten und externen Dienstleistern ist nur nach vorheriger Anmeldung möglich. Der Aufenthalt von Besuchern im Gebäude erfolgt unter stetiger Aufsicht des verantwortlichen Mitarbeiters.

Betriebsgelände und Bürogebäude Standort München

Die jameda GmbH ist mit einer Zweigstelle am Standort Berlin (Bismarckstraße 10-12, 10625 Berlin) vertreten. Der Zutritt zum Betriebsgelände und dem Gebäude am Standort ist entsprechend den örtlichen Gegebenheiten durch Umzäunungen und dauerhaft besetzte Pforten gesichert. Zusätzlich erfolgt eine Überwachung des Betriebsgeländes mit Hilfe von Videokameras und Wachpersonal. Der Zutritt in das Gebäude und damit der Zugang in die allgemeinen Büroräume wird über Zutrittskontrollsysteme (digitaler Schlüssel) geregelt. Der Zutritt der Mitarbeiter ist nur mittels des entsprechenden Schlüssels und der für das jeweilige Büro entsprechenden Freischaltung möglich. Der Zutritt von Besuchern, Lieferanten und externen Dienstleistern zu den Büros ist nur nach vorheriger Anmeldung möglich. Der Aufenthalt in den Büros erfolgt unter stetiger Aufsicht des verantwortlichen Mitarbeiters.

Serverräume Standort München

Der Serverraum ist verschlossen. Der Zutritt in die Serverräume ist nur autorisierten Mitarbeitern gestattet. Die Vergabe persönlicher Zutrittsrechte erfolgt restriktiv, d.h. der einzelne Mitarbeiter erhält nur dann Zutritt, wenn dies zur Erfüllung seines Aufgaben- bzw. Tätigkeitsfeldes und im Rahmen seiner Funktion erforderlich ist. („Need-to-know-Prinzip"). Die Schlüssel werden vom CTO und der Geschäftsführung verwahrt. Zugang haben nur befugte Mitarbeiter, die den Schlüssel vom CTO ausgehändigt bekommen und an diesen zurückgeben müssen. Der Zutritt von Besuchern und externen Dienstleistern ist nur in Begleitung eines jameda Mitarbeiters gestattet. Der Server mit der Web-Applikation und der Datenbank befindet sich nicht im Serverraum der jameda GmbH, sondern in einem Hochsicherheits-Rechenzentrum (Subunternehmer). Dieses Hochsicherheits- Rechenzentrum unterliegt einem gesonderten Schutz- und Sicherheitskonzept.

Serverräume Standort Berlin

Der Zutritt in die Serverräume ist nur autorisierten Mitarbeitern gestattet. Die Vergabe persönlicher Zutrittsrechte erfolgt restriktiv, d.h. der einzelne Mitarbeiter erhält nur dann Zutritt, wenn dies zur Erfüllung seines Aufgaben- bzw. Tätigkeitsfeldes und im Rahmen seiner Funktion erforderlich ist. („Need-to-know-Prinzip"). Räume mit sehr hohem Schutzbedarf (d.h. Räume, in denen datenverarbeitende Systeme vorgehalten werden wie z.B. Rechenzentrum, Backup-Serverräume, etc.) unterliegen einem gesonderten Sicherheitskonzept.

4. Zugangskontrolle

Ziel der Zugangskontrolle ist es, zu verhindern, dass Unbefugte Datenverarbeitungssysteme (Software) nutzen können. Dies geschieht hauptsächlich durch technische Vorrichtungen (z.B. Passwortabfrage) in den IT-Systemen (Anwendungen, Betriebssystemen etc.).

jameda

Zentrale Benutzerverwaltung

Die Anmeldung an den Endgeräten und zentralen Systemen sowie der Zugriff auf zahlreiche unternehmensspezifische Anwendungen erfolgt über eine zentrale, redundant ausgelegte Benutzerverwaltung, die von Systemadministratoren verwaltet wird.

- Verwaltung von Benutzer-, Gruppen-, Computer- und Applikationsobjekten
- Authentisierung und Autorisierung, sowie Protokollierung der Authentisierungs- und Autorisierungsvorgänge
- Komplexe Kennwort-Richtlinien
- Delegierte Administrationsaufgaben durch Applikations- oder Systemadministratoren in der IT und im Fachbereich
- Anbindung von Applikationen oder Systemen
- Inhaltliche Sicherung sämtlicher Objekte
- Single-Sign-On
- Regelmäßige Sicherung zum Zwecke der Wiederherstellung
- Lifecycle-Management für zentral verwaltete Benutzer

Identity & Access Management

Standort München

Windows-Server werden mittels Benutzer und Passwort administriert. Die Möglichkeit eines Remote-Logins aus unixoide Systeme mittels Benutzername und Passwort auf einem System ist deaktiviert. Die Administrationsrechte sind auf den notwendigen Benutzerkreis der verantwortlichen Systemadministratoren (Need-to-know-Prinzip) beschränkt. Sämtliche Zugriffe auf die Server-Systeme werden protokolliert und überwacht.

Standort Berlin

Windows-Server werden mittels Benutzer und Passwort administriert. Die Möglichkeit eines Remote-Logins aus unixoide Systeme mittels Benutzername und Passwort auf einem System ist deaktiviert. Stattdessen wird die Authentifizierung an einem System über SSH-Keys durchgeführt. Die SSH-Keys haben eine Mindestlänge von 2048 Bits und werden nur an autorisierte Mitarbeiter vergeben. Erweiterte Rechte (root-Rechte) werden über sudo definiert. Diese sind auf den notwendigen Benutzerkreis der verantwortlichen Systemadministratoren (Need-to-know-Prinzip) beschränkt. Sämtliche Zugriffe auf die Server-Systeme werden protokolliert und überwacht.

Client Arbeitsplätze

Alle Arbeitsgeräte werden aus Sicherheitsgründen standardmäßig ohne Admin-Rechte ausgeliefert.

Der Mitarbeiter erhält ein Arbeitsgerät mit einer definierten Basis-Installation, im Rahmen derer der Mitarbeiter die für seine Tätigkeit erforderliche Software eingerichtet bekommt und Zugriff auf zentrale Dienste erhält. Die Bereitstellung weiterer Software für den Mitarbeiter, die nicht Teil der Basis-Installation ist, erfolgt im Rahmen eines geregelten Freigabeverfahrens.

Alle Arbeitsplätze sind standardmäßig mit Virenschutzsoftware ausgestattet. Mobile Arbeitsgeräte (Laptops) sind außerdem mit einer Festplattenverschlüsselung versehen.

Alle jameda-Mitarbeiter sind in die zentrale Benutzerverwaltung integriert. Die Zugänge der Arbeitsplätze werden mittels Passwort geschützt. Für weitere Informationen hierzu vgl. Abschnitt „Identity & Access Management".

Im Rahmen von Sicherheits- und Verhaltensrichtlinien, die seitens der Konzernsicherheit verabschiedet worden sind, werden die jameda-Mitarbeiter im sicheren Umgang mit den ihnen zur Verfügung gestellten Arbeitsgeräten geschult. Zu diesen Regelungen zählen unter anderem die Aktivierung des Bildschirmschoners bei Verlassen des Arbeitsplatzes oder das Verhalten im Falle von Verlust mobiler Arbeitsgeräte.

Remote Arbeitsplätze

Zugriffe innerhalb des Konzern-Netzwerkes

Das Konzern-Netzwerk ist in unterschiedliche Sicherheitszonen unterteilt. Die Übergänge sind durch Firewalls geschützt. Die Arbeitsgeräte (PC, Laptops) von Burda-Mitarbeitern, die an den jeweiligen Standorten arbeiten, sind am „internen" Netzwerk (Büro-LAN, Büro-WLAN) mit Anbindung an das Internet angeschlossen.

Mobile Arbeitsgeräte (Smartphones, Tablets) sind über ein vom internen Netz getrenntes WLAN zum Internet hin angebunden. Externe Mitarbeiter und Besucher nutzen ein separates Gäste-WLAN zur Verbindung mit dem Internet.

Zugriffe außerhalb des Konzern-Netzwerkes für jameda-Mitarbeiter

jameda-Mitarbeiter, welche im Rahmen von Telearbeit auf Systeme und Anwendungen des Unternehmens zugreifen, tun dies über eine gesicherte VPN-Verbindung, wobei der Zugriff auf das Konzern-Netzwerk doppelt abgesichert ist: Die Anmeldung am VPN-Client erfolgt über ein benutzerindividuelles Passwort; die Authentisierung erfolgt anschließend über ein Einmalpasswort, welches der Mitarbeiter auf separatem Wege erhält. Am Standort München erfolgt dies per SMS. Die dafür verwendeten Handynummern der Mitarbeiter werden durch den Systemadministrator verwaltet.

Zugriffe außerhalb des Konzern-Netzwerkes für externe Mitarbeiter und Dienstleister

Im Rahmen von Projekten oder Störungsfällen kann es notwendig sein, dass externe Dienstleister von außerhalb der jameda-Infrastruktur Zugriff auf Anwendungen benötigen. In derartigen Fällen wird der Zugang zur Anwendung durch geeignete technische und organisatorische Maßnahmen zeitlich und inhaltlich beschränkt.

5. Zugriffskontrolle

Ziel der Zugriffskontrolle ist es zu gewährleisten, dass nur die zur Benutzung eines Datenverarbeitungssystems Berechtigten auf Daten, entsprechend ihrer Zugriffsberechtigung zugreifen und diese verarbeiten können.

Aufgabenbezogene Berechtigungen

Die Definition von Berechtigungen orientiert sich am Grundprinzip des Aufgabenbezugs. Entsprechend werden Berechtigungen in Form von Rollen bzw. Gruppen definiert, die einem typischen Tätigkeitsprofil entsprechen. Dabei werden, abhängig von diesem Profil, Einschränkungen auf Umfang der Daten und Art des Zugriffs vorgenommen.

Die Ausgestaltung der Rollen bzw. Gruppen erfolgt in Abstimmung mit dem jeweiligen Auftraggeber. Neben dem Grundprinzip des Aufgabenbezugs sind dabei auch Faktoren wie der Schutzbedarf der Daten, der Implementierungs- und Wartungsaufwand für Rollen und Gruppen sowie die technischen Möglichkeiten der jeweiligen Applikation zu berücksichtigen.

Die Vergabe von Berechtigungen erfolgt nach einem mit dem Auftraggeber abgestimmten Prozess und wird entsprechend der jeweiligen Vereinbarung dokumentiert.

Die bezüglich der Berechtigungsdefinition mit dem Auftraggeber abgestimmten Rahmenbedingungen werden dokumentiert. Abhängig von Umfang und Komplexität der Anwendung wird hierfür ein Benutzer- und Berechtigungskonzept erstellt. In diesen Regelungen können auch Abweichungen für bestimmte Sachverhalte definiert werden.

Protokollierung von Benutzeraktivitäten

Die Protokollierung von Benutzeraktivitäten wird je nach Kritikalität der Anwendung und der Daten auf "wesentliche sicherheitsrelevante Ereignisse" beschränkt (z.B. mehrfaches Anmelden mit falschem Passwort).

Überprüfungen im Rahmen der IT-Revision

- Protokollierung des Zugriffs auf bestimmte Dateien
- maschinelle Überprüfung der Berechtigungen
- regelmäßige Kontrolle der Gültigkeit der Berechtigungen (Protokollierung)

6. Weitergabekontrolle

Ziel der Weitergabekontrolle ist es zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welcher Stelle eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Gesicherte Übertragung

Die Übertragung von Daten wird abhängig vom Schutzbedarf und unter Berücksichtigung der technischen Möglichkeit der beteiligten Anwendungen, Systeme und Partner abgesichert. Auf Transportebene werden bevorzugt verschlüsselte Übertragungsprotokolle wie bspw. HTTPS oder SFTP eingesetzt. Optional kann eine Verschlüsselung der Daten im Vorfeld der Übertragung stattfinden.

Alle Formulare auf der Webseite, über die personenbezogene Daten übertragen werden, sind HTTPS-verschlüsselt.

Da oftmals nur der Auftraggeber selbst den Schutzbedarf der Daten bewerten kann, obliegt es ihm, die Kritikalität der zu übertragenden Daten im Vorfeld anzuzeigen, sodass ggf. geeignete Schutzmaßnahmen getroffen werden können.

Dokumentation der zu erbringenden Dienstleistung

Die zu erbringenden Dienstleistungen werden in separaten Dienstleistungsverträgen mit dem Kunden festgeschrieben. Die Dienstleistungsverträge sind in digitaler Form zentral beim Auftragnehmer abgelegt.

Weitergabe von Daten an Dritte

Die Weitergabe von Daten an Dritte erfolgt nur auf Basis einer Anforderung bzw. Freigabe

durch den Auftraggeber oder durch einen von ihm benannten Personenkreis. Dabei kann es sich sowohl um einen einmaligen als auch um einen wiederkehrenden oder dauerhaften Auftrag handeln. Abhängig von der Art der Verarbeitung kann sich die Anforderung bzw. Freigabe aber alternativ auch direkt oder indirekt aus der Beauftragung ergeben.

Sofern es sich um eine manuelle Form der Weitergabe handelt, werden die Daten bevorzugt dem Auftraggeber bereitgestellt, der die Daten nach eigenem Ermessen an den tatsächlichen Empfänger weiterleitet. Dies ermöglicht dem Auftraggeber eine vorherige Kontrolle des Umfangs und der Inhalte, was eine zusätzliche Kontrollinstanz darstellt.

Auch der Einsatz von Sub-Dienstleistern kann unter Umständen eine Weitergabe von Daten darstellen. Inwieweit dies mit oder ohne explizite Freigabe zulässig ist, wird durch die vertragliche Vereinbarung mit dem Auftraggeber festgelegt.

Für den Einsatz von Sub-Dienstleistern gelten die gleichen Regelungen und Anforderungen der DSGVO. Es werden nur geprüfte Dienstleister eingesetzt mit denen entsprechende AVV abgeschlossen werden.

Datenlöschung und Datenträgervernichtung

Die Löschung von (Kunden-)Daten erfolgt gemäß der vom Auftraggeber definierten Löschfristen. Nach Ende eines Betriebsauftrags ist sichergestellt, dass die bestehenden Datenbestände auf dem laufenden System ordnungsgemäß an den Kunden übergeben werden.

Die endgültige Löschung von Daten bzw. die Entsorgung von nicht mehr benötigten Datenträgern erfolgt nach einem geregelten Prozess.

Als Basis dienen gesetzliche Vorgaben für die Aufbewahrung von Dokumenten (z.B. HGB), sowie einschlägige Normen (z.B. DIN 66 398).

7. Eingabekontrolle

Das Ziel der Eingabekontrolle ist es zu gewährleisten, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Systemprotokollierung

Eingaben in die IT-Systeme und Anwendungen durch Benutzer und Administratoren werden je nach Anforderungen des Kunden und den technischen Möglichkeiten protokolliert und regelmäßig auf Auffälligkeiten geprüft.

Die Protokolle werden entsprechend den Inhalten und/oder gesetzlichen Vorgaben archiviert oder nach Zweckerreichung gelöscht bzw. die Verarbeitung gesperrt. Der Zugriff auf die Protokolle und Audit-Werkzeuge wird auf autorisierte Anwender beschränkt.

jameda

8. Auftragskontrolle

Ziel der Auftragskontrolle ist es zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Alle Weisungen werden schriftlich dokumentiert.

Arten der Datenübermittlung

Prinzipiell geschieht die Datenübermittlung immer unter der Initiative der Datenübertragungssysteme. Die Daten werden entweder von einer externen Datenaustauschplattform abgeholt oder an eine externe Datenaustauschplattform übertragen.

Die Ausnahme bilden Übertragungen per E-Mail, wobei externe Partner-Systeme auch Daten an Burda-Empfänger senden. Im Allgemeinen werden mit externen Partner-Systemen Dateien per SFTP-Protokoll ausgetauscht. Gelegentlich wird auch HTTPS als Übertragungsprotokoll genutzt. Daneben sind INUBIT und SAP Business Connector im Einsatz.

Protokollierung der Datenübermittlung mit Externen

Die einzelnen Datenübertragungsvorgänge werden protokolliert und die Ansprechpartner des Kunden zusätzlich per E-Mail von einer Übertragung benachrichtigt (sofern keine abweichenden Regelungen schriftlich mit dem Kunden vereinbart wurden).

In den meisten Übertragungsverfahren ist ein Archiv organisiert, das einen Rückgriff auf bereits übertragene Dateien ermöglicht.

Verschlüsselung sensibler Daten bei der Übertragung

Daten werden abhängig vom Schutzbedarf vor der Übertragung verschlüsselt. Es kommen asymmetrische (private/public-key Verfahren) wie GnuPG oder symmetrische Verfahren mit gemeinsam bekannten Schlüsseln wie ArchivCryptx zum Einsatz.

9. Verfügbarkeitskontrolle

Ziel der Verfügbarkeitskontrolle ist es zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Generelle Maßnahmen zur Erhöhung der Verfügbarkeit von IT-Systemen Standort München

- Separater Rechnerraum
- Unterbrechungsfreie Stromversorgung
- Kühlung der Server- und Stromversorgungsräume
- Brandmeldeanlage
- Redundante Notstromversorgung

Generelle Maßnahmen zur Erhöhung der Verfügbarkeit von IT-Systemen Standort Berlin

- Separater Rechnerraum
- Unterbrechungsfreie Stromversorgung
- Automatische Rauch- und Brand Früherkennungssysteme
- Lösch-/Brandmeldeanlage
- Redundante Notstromversorgung

Datensicherungskonzepte

Standort München

Um das Risiko des Datenverlustes zu minimieren, erfolgt die Sicherung bestimmter Systeme an einem zweiten, räumlich und netzwerktechnisch von den Neuen Serverräumen getrennten Standort. Die Datenbank der Webapplikation wird über den Managed-Service von AWS-RDS in einem täglichen Snapshot gebackupt.

Standort Berlin

Um das Risiko des Datenverlustes zu minimieren, erfolgt die Sicherung bestimmter Systeme durch unseren Dienstleister aufgrund von uns definierter Anforderungen.

Notfallkonzepte

Für eine Notfallbewältigung sind sämtliche erforderliche Prozesse und Reaktionsmaßnahmen definiert, die es nach Eintritt eines Notfalls bis zur Wiederaufnahme des Geschäftsbetriebs umzusetzen gilt. Die Handlungsanweisungen im Rahmen der Teilprozesse wie (1) Annahme der Störung und Weitergabe an die verantwortlichen Mitarbeiter, (2) Klassifizierung der Störungsmeldung und (3) Störungsbehebung sind dokumentiert. Die verantwortlichen Mitarbeiter werden in regelmäßigen Abständen hierzu geschult.

10. Sicherheit der Verarbeitungen

Ziel der Verschlüsselung ist es, die von den Nutzern zur Verfügung gestellten Daten und Informationen gegenüber unbefugtem Zugriff zu schützen und vertraulich übermitteln zu können.

Pseudonymisierung im Arztsuche- und Bewertungsportal

User und Kunden werden über IDs referenziert (Ärzte- bzw. Nutzer-ID). Die Ärzte-ID ist in der URL zu sehen, wenn der Arzt aufgerufen wird, die Nutzer-ID nicht.

Pseudonimisierung im Rahmen der Videosprechstunde

Es werden keine in der URL sichtbaren IDs unserer Nutzer verwendet. Es wird ein pseudonymer

Hash zur Identifikation durch jameda verwendet, der für Externe nicht zu entschlüsseln ist.

Passwörter für Kunden (Leistungserbringer) und Nutzer (Patienten)

Die Passwortrichtlinie für Online-Konten der Nutzer und Ärzte umfasst mindestens 8 Zeichen, 3aus4 (Zahl, Buchstabe, Sonderzeichen).

Zweck- und Mandantentrennung

Die Trennung Kunden- und Ärzte/Beraterdaten erfolgt über einzelne Tabellen in der Datenbank. Die Entwicklung erfolgt auf lokalen Datenbanken. Ab der Stufe Systemtest erfolgt die Verarbeitung in der Live-Datenbank mit Testdaten.

Weitergabekontrolle

Weitergabekontrolle unter dem Aspekt der Integrität

Das Sicherstellen der Integrität der Daten erfolgt durch die durchgängige Nutzung der TLS-Transportverschlüsselung sowie dem Einsatz geeigneter Hashing-Verfahren. Grundsätzlich werden alle Änderungen an Einträgen in der Datenbank gespeichert. Die Löschung bzw. Anonymisierung von Daten erfolgt nach den gesetzlichen Vorgaben und ist in einem eigenen Löschkonzept festgeschrieben.

Maßnahmen zur Sicherheit besonders schützenswerter personenbezogener Daten

Im Arztsuche- und Bewertungsportal

Alle personenbezogenen Daten im Kontext der Onlineterminbuchung werden in der Datenbank von Amazon Web Services verschlüsselt abgelegt. Als Verschlüsselungsroutine wird AES-256-CBC verwendet. Die Speicherung des Schlüssels erfolgt im Key Vault der Microsoft Azure Cloud (Europa). Daten, die über die Webseite ausgetauscht werden, sind mittelt TLS transportverschlüsselt.

Im Rahmen der Videosprechstunde

Alle personenbezogenen Daten im Kontext der Onlineterminbuchung werden in der Datenbank von Hetzner verschlüsselt abgelegt. Als Verschlüsselungsroutinen werden SHA256 / AES-256 / HMAC und CBC verwendet. Die Speicherung des Schlüssels erfolgt außerhalb der Datenbank von Hetzner auf einem separaten Backendserver von Hetzner. Alle Daten, die über die Webseite ausgetauscht werden, sind mittels TLS transportverschlüsselt. Die Videosprechstunde ist SSL-verschlüsselt.