Vertrag über die Auftragsverarbeitung von personenbezogenen Daten

Stand 08.05.2018

TopM Software GmbH

Bobingen, 08.05.2018

TopM Software GmbH
Albert-Einstein-Straße 1 – 1a
D-86399 Bobingen
Telefon: 0 82 34 / 96 52-0
Telefax: 0 82 34 / 96 52-49
www.topm.de

Inhaltsverzeichnis

TopM Software GmbH
Albert-Einstein-Straße 1 – 1a
D-86399 Bobingen
Telefon: 0 82 34 / 96 52-0
Telefax: 0 82 34 / 96 52-49
www.topm.de

Zwischen dem Verantwortlichen

Medical Services Karasek GmbH

Welserstraße 2
87463 Dietmannsried

(nachfolgend als Auftraggeber bezeichnet)

und dem Auftragsverarbeiter
TopM Software GmbH,
Albert-Einstein-Str. 1-3, 86399 Bobingen,
(nachfolgend als Auftragnehmer bezeichnet)

wird der nachfolgende Vertrag geschlossen.

1 Gegenstand des Auftrages

Dieser Vertrag zum Datenschutz bei Datenverarbeitung im Auftrag gemäß § 11 Bundesdatenschutzgesetz (BDSG) bzw. Art. 28 Datenschutz-Grundverordnung (DS-GVO) findet Anwendung auf alle Tätigkeiten, die in Zusammenhang mit separat abzuschließenden Hauptverträgen (Aufträge oder Wartungsverträge) stehen und bei denen Beschäftigte des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten („Daten") des Auftraggebers erheben, verarbeiten oder nutzen. Der Vertrag regelt auch die Rechte und Pflichten von Auftraggeber und Auftragnehmer („Parteien") im Rahmen einer Auftragsverarbeitung.

Abhängig von den Inhalten des zusätzlich abgeschlossenen Hauptvertrags führt die TopM unter anderem folgende Tätigkeiten aus:

- Installation einer Anwendungssoftware für betriebliche Zwecke
- Kundenspezifische Anpassung der Software (Programmierung und Customizing)
- Schulung der Anwender
- Wartung der Software
- Weiterentwicklung der Software
- Ggf. Hosting der Software

TopM Software GmbH
Albert-Einstein-Straße 1 – 1a
D-86399 Bobingen
Telefon: 0 82 34 / 96 52-0
Telefax: 0 82 34 / 96 52-49
www.topm.de

2 Dauer des Auftrags

Der Auftrag wird wirksam ab Unterschrift auf diesem Dokument, aber nicht vor Zusendung (in Schriftform oder als gescanntes Dokument) an die TopM. Der Auftrag läuft auf unbestimmte Zeit bis zur Kündigung dieses Vertrags.

3 Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten

Eine Erhebung, Verarbeitung oder Nutzung der Daten erfolgt nur im Rahmen des zwischen Auftragnehmer und Auftraggeber für die genannten Tätigkeiten geschlossenen Hauptvertrags. Dem Auftragnehmer ist bekannt, dass eine Erhebung, Verarbeitung oder Nutzung der Daten zu anderen Zwecken ohne vorherige Weisung durch den Auftraggeber nicht erlaubt ist. Ausdrücklich ausgeschlossen wird die Weitergabe an Dritte. Auch wird der Auftragnehmer keine Auskunft über die betreffenden personenbezogenen Daten an Dritte geben.

Personenbezogene Daten werden im Rahmen der folgenden Tätigkeiten verarbeitet:

- Datenmigration
- Konfiguration und Benutzerverwaltung,
- Wartung der Anwendung
- Bearbeitung von Anwenderfragen zur Nutzung des System
- Unterstützung bei der Beseitigung von Störungen des Systems
- Ggf. Hosting der Software durch die TopM

Der Zugriff auf die Daten durch die TopM erfolgt direkt vor Ort, per Fernwartung oder als direkter Zugriff auf zur Verfügung gestellte Datenkopien. Zweck des Zugriffs ist die Aufrechterhaltung des Systems.

Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien und sonstige Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung oder zur Durchführung des Auftrages erforderlich sind, sowie Daten, die einer gesetzlichen Aufbewahrungspflicht unterliegen.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung erfolgt ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der §§ 4b, 4c BDSG bzw. Art. 44 ff. DS-GVO erfüllt sind.

TopM Software GmbH
Albert-Einstein-Straße 1 – 1a
D-86399 Bobingen
Telefon: 0 82 34 / 96 52-0
Telefax: 0 82 34 / 96 52-49
www.topm.de

4 Art der Daten

Es werden folgende Arten von Daten verarbeitet:

Daten:	Benutzername, Name, Vorname, Adresse, Telefon-Nr., E-Mail-Adresse, Bankverbindungsdaten, Angebote, Bestellungen, Aufträge, Zahlungsart, Rechnungen, Gutschriften, Mahnungen; Arbeitszeiten von Mitarbeitern
Datenkategorie:	Personenbezogene Daten zur Abwicklung von Aufträgen; Logdateien (Transaktionsprotokoll, Fehlerprotokoll)

4.1 Weitere Arten von Daten in der Software san6

Sofern der Auftraggeber die Software san6 einsetzt, werden zusätzlich zu oben genannten Daten folgende Arten von besonderen personenbezogenen Daten verarbeitet:

Daten:	Patientenstammdaten (z.B. Name, Adresse, Geburtsdatum, weitere Kontaktdaten), Kostenträger, Versichertenstatus, Versichertennummer; Gesundheitsdaten (z. B. Verordnungsinhalte, Diagnosen, Wunddokumentation, Fotodokumentationen, Maßblätter); Abrechnungsrelevante Informationen (z. B. Mehrkosten, Eigenanteil, Lieferscheine, Kontodaten des Patienten); Status über gesetzliche Vertretungen / Betreuungen / Bevollmächtigungen und deren Kontaktdaten; sonstige Bildarchive
Datenkategorie:	Besondere personenbezogene Daten zur Abwicklung von Aufträgen in der Gesundheitsbranche

5 Kreis der Betroffenen

Die folgenden Personen, Firmen und Institutionen sind vom Datenschutz betroffen:

- Mitarbeiter
- Kunden
- Lieferanten und externe Dienstleister
- Interessenten, Makler, Händler, Bewerber

TopM Software GmbH
Albert-Einstein-Straße 1 – 1a
D-86399 Bobingen
Telefon: 0 82 34 / 96 52-0
Telefax: 0 82 34 / 96 52-49
www.topm.de

6 Pflichten des Auftraggebers

Der Auftraggeber ist im Rahmen dieses Vertrags für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („Verantwortlicher" im Sinne des Art. 4 Nr. 7 DS-GVO).

Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen in Schriftform oder in einem elektronischen Format („dokumentiert"). In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich und vollständig, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person oder einen Dritten hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftraggeber den Auftragnehmer bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten unentgeltlich zu unterstützen.

7 Technische und organisatorische Maßnahmen

Der Auftragnehmer hat alle notwendigen technischen und organisatorischen Maßnahmen bzgl. der Datensicherheit nach § 9 BDSG (und der Anlage zu § 9 Absatz 1 BDSG) bzw. Art. 28 Abs. 3 lit. c und 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1 und Abs. 2 DS-GVO zu treffen. Diese Datensicherheitsmaßnahmen dienen der Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität sowie der Verfügbarkeit und Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.

Die dokumentierten Datensicherheitsmaßnahmen sind Grundlage des Auftrags und definieren das vom Auftragnehmer geschuldete Minimum. Der Auftragnehmer gewährleistet die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber. Soweit eine Prüfung der technischen und organisatorischen Maßnahmen durch den Auftraggeber oder eine Kontrolle des Auftraggebers (vgl. Ziffer 13) einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative

TopM Software GmbH
Albert-Einstein-Straße 1 – 1a
D-86399 Bobingen
Telefon: 0 82 34 / 96 52-0
Telefax: 0 82 34 / 96 52-49
www.topm.de

adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen hiervon sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, oder technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

Im Rahmen der Auftragsverarbeitung beim Auftragnehmer anfallendes Test- und Ausschussmaterial ist unverzüglich durch den Auftragnehmer zu vernichten. Bis zur Vernichtung ist dieses Material gesichert aufzubewahren. Die Vernichtung hat mit einem Verfahren, das dem Stand der Technik entspricht, zu erfolgen.

Vom Auftraggeber vergebene Zugangsberechtigungen dürfen nur zur Durchführung der vertraglich vereinbarten Tätigkeiten oder zur Umsetzung der vom Auftraggeber erteilten Weisungen verwendet werden. Eine Weitergabe der Zugangsberechtigungen an unberechtigte Dritte ist untersagt.

Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück. Im separat abzuschließenden Hauptvertrag können die Parteien hierzu eine Vergütungsregelung treffen.

Soweit der Auftragnehmer im Rahmen der Prüfung oder Wartung von automatisierten Verfahren und Datenverarbeitungsanlagen des Auftraggebers defekte oder nicht mehr benötigte Datenspeicher ausbaut, sind diese beim Auftragnehmer gesichert aufzubewahren, bis sie einer Reparatur, Entsorgung oder weiteren Verwendung zugeführt worden sind. Vor einer Weitergabe der Komponenten an Dritte hat der Auftragnehmer sicherzustellen, dass alle darauf gespeicherten Daten des Auftraggebers physisch gelöscht sind. Diese Verfahrensweise ist auch einzuhalten, wenn der Auftragnehmer im Rahmen der Auftragsverarbeitung von ihm genutzte Datenspeicher ausbaut, soweit diese Daten des Auftraggebers enthalten.

Die Auflistung der beim Auftragnehmer bzgl. dieses Vertrags umgesetzten technischen und organisatorischen Maßnahmen ist als Anlage beigefügt.

TopM Software GmbH
Albert-Einstein-Straße 1 – 1a
D-86399 Bobingen
Telefon: 0 82 34 / 96 52-0
Telefax: 0 82 34 / 96 52-49
www.topm.de

8 Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich, personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen zu verarbeiten, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten.

Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten für andere Zwecke außerhalb des Auftrags oder einer Weisung zu verarbeiten, insbesondere nicht für eigene Zwecke, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

Der Auftragnehmer sichert zu, seinen Pflichten nach Art. 32 Abs. 1 lit. d DS-GVO nachzukommen. Er überprüft und bewertet regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

Die in diesem Zusammenhang stehenden Dokumente und Protokolle sind auf Verlangen des Auftraggebers im Rahmen der nach Ziffer 7 dieses Vertrags erfolgten Kontrolle diesem vorzulegen.

Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen vor der Aufnahme ihrer Tätigkeit schriftlich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung der Tätigkeit fort.

Auf Weisung des Auftraggebers hat der Auftragnehmer, die von ihm mit der Auftragsverarbeitung tätigen Personen auch auf weitere Vertraulichkeitsgebote (z.B. Fernmeldegeheimnis oder Postgeheimnis) zu verpflichten, soweit dies gesetzlich gefordert ist.

Der Auftragnehmer hat ihm erteilte Weisungen sowie ggf. deren Umsetzung zu dokumentieren.

Beide Parteien arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

TopM Software GmbH
Albert-Einstein-Straße 1 – 1a
D-86399 Bobingen
Telefon: 0 82 34 / 96 52-0
Telefax: 0 82 34 / 96 52-49
www.topm.de

Der Auftragnehmer hat schriftlich einen Datenschutzbeauftragten bestellt und sichert zu, den Vorschriften der §§ 4f und 4g BDSG bzw. den Art. 38 und 39 DS-GVO Genüge zu leisten. Die Kontaktdaten des Datenschutzbeauftragten lauten:

Herr Joachim Spranz
S.I.G. System Informations GmbH
Zeppelinstr. 5/2
89231 Neu-Ulm

Der Auftragnehmer sichert zu, dass ihm die Inhalte des Bundesdatenschutzgesetzes bzw. der Datenschutz-Grundverordnung bekannt sind.

9 Durchführung der Fernwartung

Werden Auftragsleistungen per Fernwartung über Teamviewer oder ASP-Zugang durchgeführt, gelten zusätzlich folgende Vereinbarungen:

Der Auftragnehmer führt die Fernwartung ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers durch. Die Fernwartung erfolgt, soweit möglich, ohne gleichzeitige Speicherung von Daten.

Der Auftragnehmer wird personenbezogene Daten, die er bei der Fernwartung erhalten oder gewonnen hat, unverzüglich sicher löschen oder dem Auftraggeber zurückgeben, wenn sie für die Durchführung der Fernwartungsarbeiten nicht mehr erforderlich sind.

Zu Zwecken der Fernwartung notwendige Datenübertragungen erfolgen in hinreichend verschlüsselter Form, Ausnahmen werden vorab mit dem Auftraggeber abgestimmt.

Die Fernwartung wird in der Regel durch den Auftragnehmer angekündigt und anschließend durch den Auftraggeber initiiert. Dadurch hat der Auftraggeber die Möglichkeit die durchgeführten Maßnahmen zu überwachen.

Davon abweichend kann der Auftraggeber den Fernzugriff dauerhaft einrichten und gewähren. In diesem Fall erfolgt keine explizite Ankündigung der Fernwartung seitens des Auftragnehmers.

In jedem Fall erfolgt eine Fernwartung durch den Auftragnehmer nur auf Grund von Störungsmeldungen oder sonstiger ausdrücklicher Anforderungen Seitens des Auftraggebers. Nach Abschluss der Fernwartung wird der Auftraggeber über die durchgeführten Tätigkeiten informiert.

TopM Software GmbH
Albert-Einstein-Straße 1 – 1a
D-86399 Bobingen
Telefon: 0 82 34 / 96 52-0
Telefax: 0 82 34 / 96 52-49
www.topm.de

Der Auftraggeber hat das Recht, die Fernwartung zu unterbrechen, wenn der Auftragnehmer von den vereinbarten Sicherheitsmaßnahmen abweicht oder die Fernwartung mit nicht vereinbarten Softwarekomponenten durchgeführt wird.

10 Mitteilungspflichten des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in § 42a BDSG bzw. Art. 33 und 34 DS-GVO genannten Meldepflichten bei Datenpannen. Hierfür stellt er dem Auftraggeber sämtliche in diesem Zusammenhang relevanten Informationen unverzüglich zur Verfügung. Der hierbei anfallende Aufwand wird durch die TopM mit den jeweils aktuellen Stundensätzen gem. TopM-Preisliste abgerechnet.

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften – im Besonderen die Europäische Datenschutz-Grundverordnung, das Bundesdatenschutzgesetz oder sonstige Datenschutzvorschriften – verstößt. Der Auftragnehmer ist berechtigt, die Umsetzung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber

- bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten,
- bei Durchführung der Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) sowie
- bei vorheriger Konsultation der Aufsichtsbehörde (Art. 36 DS-GVO)

zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten. Der hierbei anfallende Aufwand wird durch die TopM mit den jeweils aktuellen Stundensätzen gem. TopM-Preisliste abgerechnet.

Soweit der Auftraggeber einer Kontrolle der Datenschutz-Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen. Der hierbei anfallende Aufwand wird durch die TopM mit den jeweils aktuellen Stundensätzen gem. TopM-Preisliste abgerechnet.

Über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde beim Auftragnehmer ist der Auftraggeber unverzüglich zu informieren, soweit sie sich auf diese Auftragsverarbeitung beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ord-

TopM Software GmbH
Albert-Einstein-Straße 1 – 1a
D-86399 Bobingen
Telefon: 0 82 34 / 96 52-0
Telefax: 0 82 34 / 96 52-49
www.topm.de

nungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers – Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen, erhebliche Störungen des Verarbeitungsablaufs, Verlust oder Beschädigung von Datenträgern, andere Unregelmäßigkeiten bei der Erhebung, Verarbeitung oder Nutzung der Daten – bekannt werden. Auch begründete Verdachtsfälle sind mitzuteilen. Die Mitteilung hat mindestens die Angaben nach Art. 33 Abs. 3 DS-GVO zu enthalten.

Ebenso informiert der Auftragnehmer unverzüglich den Auftraggeber bei Verstößen seitens des Auftragnehmers oder der bei ihm beschäftigten Personen gegen die in diesem Vertrag getroffenen Festlegungen.

Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

11 Sicherheitsvorfälle durch Schadprogramme

Ein „Angriff" auf die bei der TopM eingesetzten System- oder Netzwerkkomponenten durch Schadprogramme (Computervirus, Junkware, Malware, Evilware, oder ähnlichem) wird als Sicherheitsvorfall bezeichnet. Die TopM wird geeignete Methoden und Systeme (Virenscanner, Firewalls, etc.) einsetzen um derartige Angriffe frühzeitig zu erkennen und in der Folge auch reagieren zu können.

Die TopM wird bei jedem Sicherheitsfall prüfen, ob die Systeme des Auftraggebers betroffen sind und den Auftraggeber gegebenenfalls sofort informieren und innerhalb der Arbeitszeiten der TopM an einer Problemlösung arbeiten.

Im Falle der Beschäftigung von Unterauftragnehmern (s. nachfolgendes Kapitel „Unterauftragsverhältnisse") wird die TopM die Unterauftragnehmer zu gleichen Maßnahmen verpflichten.

TopM Software GmbH
Albert-Einstein-Straße 1 – 1a
D-86399 Bobingen
Telefon: 0 82 34 / 96 52-0
Telefax: 0 82 34 / 96 52-49
www.topm.de

12 Unterauftragsverhältnisse

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind nur solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Leistungen gem. Wartungsvertrag beziehen, entweder durch Erbringung der ganzen oder einer Teilleistung der im Wartungsvertrag vereinbarten Leistung.

Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/ Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Die Pflicht des Auftragnehmers, auch bei ausgelagerten Nebenleistungen die Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers sicherzustellen, bleibt unberührt.

Die Beauftragung von Subunternehmen ist nur nach vorheriger schriftlicher Zustimmung des Auftraggebers zulässig. Der Auftragnehmer wird in einem solchen Fall vertraglich sicherstellen, dass die vereinbarten Regelungen auch gegenüber dem jeweiligen Subunternehmen gelten. Außerdem trägt der Auftragnehmer Sorge, dass dieselben Datenschutzstandards im Subunternehmen eingehalten werden. Auf Verlangen des Auftraggebers hat der Auftragnehmer Einsicht in die relevanten Vereinbarungen zwischen Auftragnehmer und Subunternehmern zu gewähren.

Die Rechte des Auftraggebers müssen auch gegenüber Subunternehmern wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem in diesem Vertrag festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.

13 Kontrollrechte des Auftraggebers

Der Auftragnehmer gestattet dem Datenschutzbeauftragten oder einem anderen Beauftragten des Auftraggebers, die Einhaltung der Datenschutzbestimmungen in seinen Betriebs- oder Geschäftsräumen zu überprüfen. Die Durchführung der Überprüfungen ist rechtzeitig zwischen Auftraggeber und Auftragnehmer abzustimmen. Sie haben ohne vermeidbare Störungen des Geschäftsbetriebs und zu Geschäftszeiten des Auftragnehmers zu erfolgen. Der Auftraggeber hat das Recht sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen wobei zwischen zwei Kontrollen jeweils ein im Hinblick auf Art und Umfang der verarbeiteten Daten ein angemessener Zeitraum liegen muss. Die Parteien sind sich darüber einig, dass „angemessen" in diesem Sinne ein

TopM Software GmbH
Albert-Einstein-Straße 1 – 1a
D-86399 Bobingen
Telefon: 0 82 34 / 96 52-0
Telefax: 0 82 34 / 96 52-49
www.topm.de

Zeitraum von wenigstens zwölf Monaten ist. Die Ergebnisse der Überprüfung werden dokumentiert.

Der Auftragnehmer darf die Ausübung des Kontrollrechts von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen.

Sollten der TopM durch derartige Überprüfungen interne oder externe Kosten entstehen, so ist die TopM berechtigt diese dem Auftraggeber in Rechnung zu stellen. Die Höhe der abzurechnenden Kosten orientiert sich dabei an den jeweils aktuellen Stundensätzen gem. TopM-Preisliste.

14 Regelungen zur Wahrung der Rechte von Betroffenen

Für die Wahrung der Rechte von Betroffenen im Zusammenhang mit dieser Auftragsverarbeitung ist allein der Auftraggeber verantwortlich. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten.

Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

Der Auftragnehmer wird die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken (sperren).

15 Weisungsbefugnis des Auftraggebers

Die weisungsbefugten Personen seitens des Auftraggebers ergeben sich aus den „Anfrageberechtigten Personen" aus dem Wartungsvertrag. Seitens des Auftragnehmers ist jeder Mitarbeiter der TopM zur Annahme dieser Weisungen befugt.

Eine Weisung im Sinne dieses Vertrags ist eine einseitige Anordnung des Auftraggebers gegenüber dem Auftragnehmer, welche auf einen bestimmten Umgang mit personenbezogenen Daten bei der Auftragsverarbeitung gerichtet ist.

Der Auftragnehmer verpflichtet sich, personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers zu erheben, zu verarbeiten oder zu nutzen. Die entsprechenden Weisungen bedürfen grundsätzlich der Schriftform.

TopM Software GmbH
Albert-Einstein-Straße 1 – 1a
D-86399 Bobingen
Telefon: 0 82 34 / 96 52-0
Telefax: 0 82 34 / 96 52-49
www.topm.de

16 Rückgabe und Löschung der Daten bei Beendigung des Auftrages

Nach Beendigung der Tätigkeit des Auftragnehmers werden alle Datenträger, die sich im Besitz des Auftragnehmers befinden und personenbezogenen Daten des Auftraggebers enthalten, unverzüglich an den Auftraggeber übergeben. Weiterhin werden die beim Auftragnehmer gespeicherten Kopien der Daten gelöscht.

Die Modalitäten des Transports der Daten (einschließlich Übergabe und Abholung) oder ggf. einer Datenfernübertragung werden am Ende der Tätigkeit mit dem Auftraggeber abgestimmt und protokolliert.

Von obiger Löschung ausgenommen sind Daten, die in einer revisionssicheren Datenbank gespeichert wurden und damit nicht mehr löschbar sind. Die TopM wird diese Daten auch nach Beendigung der Tätigkeit im Sinne dieser Vereinbarung gegen unbefugten Zugriff und Missbrauch schützen.

Der Auftragnehmer wird seine Tätigkeit nur nach ausdrücklicher Aufforderung durch den Auftraggeber beenden. Diese Aufforderung ist in schriftlicher Form mit Bezug auf diese Vereinbarung an die Geschäftsleitung der TopM zu richten.

17 Haftung und Mitwirkungspflicht

Der Auftragnehmer haftet gegenüber dem Auftraggeber für alle Schäden, die durch vorsätzliche oder fahrlässige Verletzung dieser Vereinbarung entstehen. Resultieren aus der Erhebung, Verarbeitung oder Nutzung der Daten Ansprüche Dritter gegen den Auftraggeber, wird der Auftragnehmer alle Informationen zur Verfügung stellen, die der Auftraggeber aufgrund seiner Beweislast benötigt.

TopM Software GmbH
Albert-Einstein-Straße 1 – 1a
D-86399 Bobingen
Telefon: 0 82 34 / 96 52-0
Telefax: 0 82 34 / 96 52-49
www.topm.de

18 Schlussbestimmungen

Zu dieser Vereinbarung bestehen keine Nebenabreden die den Datenschutz betreffen.

Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebs- und Geschäftsgeheimnissen sowie Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages hinaus vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

Es gilt deutsches Recht. Gerichtsstand und Erfüllungsort aller Leistungen aus diesem Vertrag ist Bobingen.

Bei etwaigen Widersprüchen gehen Regelungen dieses Vertrags den Regelungen des separat abgeschlossenen Wartungsvertrags vor.

Die Aufhebung, sowie Änderungen und Ergänzungen dieser Vereinbarung müssen schriftlich festgehalten werden. Mündliche Vereinbarungen, auch die mündliche Vereinbarung über die Aufhebung der Schriftform, sind nichtig.

Sollte eine der Bestimmungen dieser Vereinbarung ganz oder teilweise rechtsunwirksam sein oder werden, so wird die Gültigkeit der übrigen Bestimmungen dadurch nicht berührt. In einem solchen Fall ist die Vereinbarung vielmehr ihrem Sinne gemäß zur Durchführung zu bringen.

Bobingen, 08.05.2018

.....

Uwe R. Iltgen,
TopM Software GmbH
Geschäftsführer

Dietmannsried, 24.05.2018

Ort, Datum

Unterschrift des Auftraggebers

TopM Software GmbH
Albert-Einstein-Straße 1 – 1a
D-86399 Bobingen
Telefon: 0 82 34 / 96 52-0
Telefax: 0 82 34 / 96 52-49
www.topm.de

Technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten

Stand 01.05.2018

TopM Software GmbH

Bobingen, 01.05.2018

TopM Software GmbH
Albert-Einstein-Straße 1 - 1a
D-86399 Bobingen
Telefon: 0 82 34 / 96 52-0
Telefax: 0 82 34 / 96 52-49
www.topm.de

Inhaltsverzeichnis

TopM Software GmbH
Albert-Einstein-Straße 1 – 1a
D-86399 Bobingen
Telefon: 0 82 34 / 96 52-0
Telefax: 0 82 34 / 96 52-49
www.topm.de

1 Allgemeines

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen die durch die TopM eingesetzt werden um den Schutz personenbezogener Daten sicherzustellen.

2 Getroffene Maßnahmen

Die TopM hat in den folgenden Bereichen nach DSGVO Maßnahmen getroffen um den Datenschutz sicherzustellen:

2.1 Verschlüsselung

- Alle Daten die auf einem mobilen Endgerät (z.B. Notebooks) oder Datenträger (z.B. USB-Sticks) die Geschäftsräume der TopM verlassen werden verschlüsselt gespeichert.
- Die Übertragung der Daten zwischen ASP-Server und ASP-Client erfolgt verschlüsselt.
- Die Übertragung zwischen der TopM mobile2-App und den Hostingservern der TopM erfolgt SSL-verschlüsselt.
- VPN-Verbindungen zwischen mobilen Geräten und den Serversystemen der TopM finden verschlüsselt statt

2.2 Gewährleistung der Vertraulichkeit

- Die TopM setzt ein elektronisches Transponder-Schließsystem mit mitarbeiterbezogenen Zutrittsberechtigungen ein.
- Besucher erhalten erst nach Türöffnung durch den Empfang Zutritt zu den Räumlichkeiten der TopM.
- Alle Räume in denen sich Datenträger mit personenbezogenen Daten befinden werden via Schließsystem verschlossen. Für den Serverraum und das Personalbüro gibt es gesonderte Schließberechtigungen.
- Der Zugriff innerhalb des Systems wird durch ein Rechtesystem geregelt, so dass über Nutzerprofile sichergestellt ist, dass jeder Mitarbeiter der TopM nur die zur Durchführung seiner Aufgaben erforderlichen Daten einsehen kann
- Kundendaten werden in getrennten Datenbeständen geführt.
- Der Zugriff auf die personenbezogenen Daten wird durch gesonderte Anmeldung via personifiziertem Benutzername und Kennwort geschützt.
- Es werden Mindestanforderungen an Passwörter gesetzt (Mindestlänge, Sonderzeichen, Zahlen)

TopM Software GmbH
Albert-Einstein-Straße 1 – 1a
D-86399 Bobingen
Telefon: 0 82 34 / 96 52-0
Telefax: 0 82 34 / 96 52-49
www.topm.de

- Es werden Firewalls eingesetzt um den ein- und ausgehenden Datenverkehr zu regeln und kontrollieren.
- Es werden aktuelle Virenscanner mit aktuellen Definitionen eingesetzt.
- Betriebssystemupdates-/patches werden regelmäßig und zeitnah eingespielt.
- Alle Mitarbeiter der TopM werden schriftlich zur Wahrung des Datenschutzes verpflichtet
- Es existieren Arbeitsanweisungen zur Löschung und Entsorgung von Datenträgern und Papierunterlagen.
- Bei Auftragsdatenverarbeitung werden die vereinbarten Regelungen strikt eingehalten
- Für die Zugänge zu Kundensystemen werden täglich wechselnde Passwörter erzeugt.
- Für die Zugänge zu den Hostingservern werden personalisierte und täglich wechselnde Passwörter erzeugt.

2.3 Gewährleistung der Integrität

- VPN-Verbindungen zwischen mobilen Geräten und den Serversystemen der TopM
- Verbindungen zum Webserver der TopM sind SSL-Verschlüsselt
- Die Übertragung der Daten zwischen ASP-Server und ASP-Client erfolgt verschlüsselt.
- Die Übertragung zwischen der TopM mobile2-App und den Hostingservern der TopM erfolgt SSL-verschlüsselt.

2.4 Gewährleistung der Verfügbarkeit und Belastbarkeit

- Die Hostingserver werden in einem ISO/IEC 27001-zertifizierten Rechenzentrum betrieben.
- Alle Produktivsysteme setzen ein RAID 1 zur Spiegelung der Daten ein.
- Es finden mehrfache, regelmäßige Datensicherungen aller Produktivdaten auf unterschiedliche Backupserver statt.
- Die Hostingdaten werden mehrfach innerhalb des Rechenzentrums gespiegelt und zusätzlich auf örtlich getrennte Backupserver kopiert.
- Alle Produktivsysteme werden durch USVs gestützt.
- Die Serverräume lokal und im Rechenzetrum sind klimatisiert.
- Es findet ein permanentes Monitoring der Hostingserver statt.
- Es findet regelmäßig eine Revision der IT-Infrastruktur nach entsprechender Arbeitsanweisung statt

TopM Software GmbH
Albert-Einstein-Straße 1 – 1a
D-86399 Bobingen
Telefon: 0 82 34 / 96 52-0
Telefax: 0 82 34 / 96 52-49
www.topm.de

- Es werden Notfallserver für die Hostingserver eingesetzt.

2.5 Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

- Es existieren Notfallpläne für die Umschaltung auf Backupsysteme.

2.6 Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

- Regelmäßige Überprüfung der technischen und organisatorischen Maßnahmen.
- Es findet regelmäßig eine Revision der IT-Infrastruktur nach entsprechender Arbeitsanweisung statt.
- Bestellung eines externen Datenschutzbeauftragten.
- Mitarbeiter werden auf Vertraulichkeit/Datengeheimnis verpflichtet.
- Die Datenschutzfolgenabschätzung wird bei Bedarf durchgeführt.
- Die Firewalllogs werden anlassbezogen überprüft und evaluiert.

2.7 Datenschutz durch Technikgestaltung

- In den Softwareprodukten der TopM können User-Interfaces durch den Konfigurator flexibel gestaltet werden. So können Pflichtfelder vorgegeben oder nicht benötigte Felder ausgeblendet werden.

TopM Software GmbH
Albert-Einstein-Straße 1 – 1a
D-86399 Bobingen
Telefon: 0 82 34 / 96 52-0
Telefax: 0 82 34 / 96 52-49
www.topm.de