BITTE BEACHTEN:
Dieser Auftrag zur Verarbeitung personenbezogener Daten ist unterschrieben an die aufgeführte Adresse der MORGEN & MORGEN GmbH zu senden. Eine Ausführung erhalten Sie von MORGEN & MORGEN unterschrieben zurück.

Auftrag zur Verarbeitung personenbezogener Daten gemäß § 11 Bundesdatenschutzgesetz (BDSG)

Hiermit beauftrage ich die

MORGEN & MORGEN GmbH
Wickerer Weg 13 –15
65719 Hofheim

zur Datenverarbeitung gemäß „Ergänzende Bedingungen Auftragsdatenverarbeitung“ und der „Anlage Ergänzende Bedingungen Auftragsdatenverarbeitung“ (Allgemeine technische und organisatorische Maßnahmen nach § 9 BDSG und Anlage zu § 9 Satz 1 BDSG).

Ich nehme einverständlich zur Kenntnis, dass ein wirksamer Auftragsdatenverarbeitungsvertrag zwischen mir und der MORGEN & MORGEN GmbH nur unter diesen Bedingungen zustande kommt.

Firma / Name

Straße / Hausnummer

PLZ/Ort

Ort, Datum

Unterschrift / Stempel

Ort, Datum **(MORGEN & MORGEN GmbH)**

Unterschrift / Stempel **(MORGEN & MORGEN GmbH)**

Ergänzende Bedingungen Auftragsdatenverarbeitung
MORGEN & MORGEN GmbH smartKundenrechner

1. Allgemeines

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien aus dem Hauptvertrag, dem M&M smartKundenrechner Lizenzvertrag, sofern im Rahmen der Leistungserbringung (nach den Allgemeinen Geschäftsbedingungen der MORGEN & MORGEN GmbH für M&M smartKundenrechner und mit geltenden Dokumenten) eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch M&M für den Kunden im Sinne des § 11 BDSG erfolgt. Der Auftraggeber wird im folgenden Kunde, der Auftragnehmer M&M genannt.

2. Gegenstand und Dauer des Auftrags

1. Gegenstand des Auftrags zum Umgang mit personenbezogenen Daten ist die Nutzung des Online-Versicherungsvergleichsprogramms M&M smartKundenrechner für Interessenten des Kunden durch Einbindung des M&M smartKundenrechner in die Website des Kunden sowie Bereitstellung einer Webservice Infrastruktur für die Übermittlung der Daten des Interessenten an den Kunden.

2. Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der abgeschlossenen Leistungsvereinbarung M&M smartKundenrechner.

3. Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen

1. Zweck der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten ist:

Der Kunde bezieht von M&M das Online-Versicherungsvergleichsprogramm M&M smartKundenrechner. Dieses bindet der Kunde in seine Website ein, damit Interessenten über die aufgerufene Website des Kunden Versicherungsvergleichsberechnungen vornehmen können. Bei Interesse haben diese Interessenten die Möglichkeit, durch Eingabe ihrer personenbezogenen Daten in das Kontaktformular des M&M smartKundenrechner eine Kontaktaufnahme anzufordern. M&M sendet die Anfrage des Interessenten per E-Mail als verschlüsseltes PDF-Dokument an die E-Mailadresse des Kunden, das er mit seinem Passwort öffnen kann. Diese Funktionalitäten werden auf Serversystemen von M&M automatisch durchgeführt. Der gesamte Datentransfer erfolgt jeweils in verschlüsselter Form.

2. Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

3. Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten können folgende Datenarten / -kategorien sein:

Personenstammdaten, Kommunikationsdaten (z.B. Telefon, E-Mail), Daten zu Produkt bzw. Vertragsinteresse.

4. Kreis der Betroffenen

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen kann folgende Personenkategorien umfassen:

Interessenten / potentielle Versicherungsnehmer / Endkunden (ggfs. deren Familienange-hörige oder begünstigte Freunde), die sich an den Kunden wenden, um sich von diesem über die Auswahl eines Versicherungsproduktes beraten zu lassen.

4. Technisch-organisatorische Maßnahmen nach § 9 BDSG und Anlage zu § 9 Satz 1 BDSG (siehe „Anlage zu Ergänzende Bedingungen Auftragsdatenverarbeitung“)

1. Der Kunde ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

2. Für die auftragsgemäße Bearbeitung personenbezogener Daten nutzt M&M folgende Ein-richtung:

Bereitstellung der Hostinginfrastruktur durch Verizon Deutschland GmbH für M&M smartKundenrechner.

3. Die als Anlage beigefügte Beschreibung der technischen und organisatorischen Maßnah-men entsprechend der Anlage zu § 9 BDSG, “Anlage zu Ergänzende Bedingungen Auftragsdatenverarbeitung“, wird als verbindlich festgelegt.

4. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es M&M gestattet, alternative adäquate Maßnahmen umzusetzen, wenn das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. M&M hat auf Anforderung die Angaben nach § 4g Abs. 2 Satz 1 BDSG dem Kunden zur Verfügung zu stellen.

5. Berichtigung, Sperrung und Löschung von Daten

Der Kunde ist verantwortlich für die Einhaltung der Rechte der Betroffenen, wie Berichtigung, Löschung und Sperrung von Daten, die ihm gegenüber geltend gemacht werden können. Für den M&M smartKundenrechner gilt, dass keinerlei Daten gespeichert werden. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Kunden weiterleiten.

6. Kontrollen und sonstige Pflichten seitens M&M

M&M hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags nach § 11 Abs. 4 BDSG folgende Pflichten:

1. Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten, der seine Tätigkeit gemäß §§ 4f, 4g BDSG ausüben kann.

M&M stellt sicher, dass die mit der Verarbeitung der Daten des Kunden befassten Mitarbeiter entsprechend § 5 BDSG verpflichtet und in die Schutzbestimmungen des BDSG eingewiesen worden sind.

2. Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend § 9 BDSG und Anlage.

Die unverzügliche Information des Kunden über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach § 38 BDSG. Dies gilt auch, soweit eine zuständige Behörde nach §§ 43, 44 BDSG bei M&M ermittelt.

3. Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch M&M im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.

Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Kunden. Hierzu kann M&M auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit vorlegen.

7. Unterauftragsverhältnisse

1. Der Kunde ist damit einverstanden, dass M&M zur Erfüllung seiner vertraglich vereinbarten Leistungen, andere qualifizierte Unternehmen zur Leistungserfüllung heranzieht bzw. mit Leistungen unterbeauftragt.

2. Zurzeit ist folgender Subunternehmer mit der Verarbeitung von personenbezogenen Daten beschäftigt: - Verizon Deutschland GmbH, Sebrathweg 20, 44149 Dortmund -

Bereitstellung der Hostinginfrastruktur durch Verizon Deutschland GmbH.

3. Erteilt M&M Aufträge an Unterauftragnehmer, so obliegt es allein M&M, seine Pflichten aus dem Vertrag dem Unterauftragnehmer zu übertragen. Satz 1 gilt insbesondere für Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages. Einen Wechsel der Unterauftragnehmer wird M&M dem Kunden schriftlich anzeigen.

4. Sofern M&M andere Unternehmen mit Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt, wie zum Beispiel Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern verpflichtet sich M&M zur Gewährleistung des Schutzes und der Sicherheit der Daten des Kunden. Sofern Nebenleistungen datenschutzrechtlich als (Unter-)Auftragsdatenverarbeitungen einzustufen sind, schließt M&M mit den eingesetzten Unternehmen angemessene vertragliche Vereinbarungen nach § 11 BDSG.

8. Kontrollpflichten und -rechte des Kunden

1. Im Hinblick auf die Kontrollverpflichtungen des Kunden nach § 11 Abs. 2 Satz 4 BDSG vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt M&M sicher, dass sich der Kunde von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierfür kann der Kunde Selbstauskünfte bei M&M einholen. M&M kann außerdem Testate oder Zertifikate unabhängiger Prüfunternehmen oder des be-trieblichen Datenschutzbeauftragen vorlegen.

2. Sofern der Kunde auf eigene Kosten eine Vor-Ort-Prüfung bei M&M oder einem von M&M eingesetzten Dienstleister durchführen möchte, muss diese in der Regel mit angemessener Frist angekündigt werden. Zum Schutz der Daten und Rechte anderer Kunden und Betroffener dürfen Vor-Ort-Prüfungen nur von zur Berufsverschwiegenheit verpflichteten, fachkundigen Prüfern oder Prüfunternehmen durchgeführt werden.Bei der Durchführung der Prüfung ist auf den Geschäftsbetrieb von M&M Rücksicht zu nehmen. Entsteht durch die Prüfung Mehraufwand für M&M ist dieser durch den Kunden gesondert zu vergüten.

3. Der Kunde hat M&M unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

9. Mitteilung bei Verstößen

M&M erstattet dem Kunden eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Kunden oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.

Dem Kunden obliegen die aus § 42a BDSG resultierenden Informationspflichten.

10. Weisungsbefugnis und Verantwortung des Kunden

1. Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarung und nach Weisung des Kunden (vgl. § 11 Abs. 3 Satz 1 BDSG).

2. Erteilt der Kunde zusätzliche Weisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründenden Kosten vom Kunden zu tragen. M&M ist berechtigt bei Weisungen des Kunden, deren Umsetzung für M&M nicht oder nur mit unverhältnismäßig hohem Mehraufwand möglich ist, den Vertrag zu kündigen.

Zusätzliche Weisungen bedürfen der Schriftform.

3. Der Kunde ist für die Beurteilung der Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten sowie für die Wahrung der Rechte der Betroffenen verantwortlich. Er hat dafür Sorge zu tragen, dass die gesetzlich vorgeschriebenen Anforderungen erfüllt werden, wie z.B. die Einholung von Einwilligungserklärungen seiner Kunden, wenn er deren Daten verarbeiten lässt, insbesondere wenn der Kunde besondere Arten personenbezogener Daten i.S.d. § 3 Abs. 9 BDS, wie z.B. Gesundheitsdaten verarbeiten lässt.

11. Löschung von Daten und Rückgabe von Datenträgern

Für das M&M Softwareprogramm M&M smartKundenrechner gilt:

Die seitens der Interessenten des Kunden eingegebenen personenbezogenen Daten in das Kontaktaufnahmeformular des M&M smartKundenrechner werden von M&M per E-Mail als verschlüsseltes PDF-Dokument an die E-Mailadresse des Kunden übermittelt. Eine Speicherung der E-Mail bzw. des Kontaktaufnahmeformulars bzw. der seitens des Interessenten aufgerufenen Berechnungen finden seitens M&M nicht statt.

Nach Vertragsende wird der Zugang des Kunden zum M&M smartKundenrechner gelöscht.

12. Sonstiges

1. Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeite-ten Daten und der zugehörigen Datenträger ausgeschlossen.

2. Für Nebenabreden ist die Schriftform erforderlich.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Die Vertragsparteien werden in einem solchen Fall die unwirksame Bestimmung durch eine gesetzeskonforme Regelung ersetzen. Dasselbe gilt für unerkannte Regelungslücken.

Anlage zu Ergänzende Bedingungen Auftragsdatenverarbeitung MORGEN & MORGEN GmbH smartKundenrechner

Allgemeine technische und organisatorische Maßnahmen nach § 9 BDSG und Anlage zu § 9 Satz 1 BDSG

1. Allgemeines

Der Kunde und M&M haben im Rahmen der Leistungserbringung (nach M&M smartKundenrechner AGB und mitgeltenden Dokumenten), die Geltung der „Ergänzenden Bedingungen Auftragsdatenverarbeitung“ vereinbart.

Diese „Anlage zu Ergänzende Bedingungen Auftragsdatenverarbeitung“ mit der Darstellung der technischen und organisatorischen Maßnahmen seitens des Auftragnehmers – M&M –, wird vom Kunden und M&M als verbindlich festgelegt.

2. Technische und organisatorische Maßnahmen

2.1. Zutrittskontrolle

Ein unbefugter Zutritt zu DV-Anlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

- Zutritt zum Gebäude und zu den Büroräumen ist nur mit Magnetkarte/Chipkarte oder Sicherheitsschlüssel möglich;
- Werksschutz;
- Überwachungseinrichtungen;
- Es existiert ein Zugangskontrollsystem in dem die zutrittsberechtigten Mitarbeiter mit unterschiedlichen Berechtigungen festgelegt sind;
- Pförtnerdienst (7*24 Std);
- Es bestehen Regelungen für Fremdpersonal, Reinigungspersonal und Besucher;
- Die Begleitung von Gästen ist in einer Richtlinie geregelt;
- Es sind Sicherheitsbereiche/-zonen (z.B. für Server, Großrechner, Archiv) festgelegt;
- RZ-Zutritt ist gesichert, innenliegend im Kellergeschoß, dadurch hermetisch abgerie-gelt;
- Server befinden sich in abschließbaren Serverschränken.

2.2. Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

Technische (Kennwort-/Passwortschutz) und organisatorische (Benutzerstammsatz) Maß-nahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- UserID;
- Passwortvergabe ;
- Jeder Berechtigte verfügt über ein eigenes nur ihm bekanntes Passwort;
- Der Zugriff erfolgt ausschließlich über verschlüsselte Verbindungen.

2.3. Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

- In den IT-Systemen sind Berechtigungen festgelegt;
- Berechtigungen sind abgestuft;
- Bei Programmentwicklungen erfolgt eine Trennung in ein Test- und ein Produktiv-system.

2.4. Weitergabekontrolle

Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

- Alle Mitarbeiter, die Umgang mit personenbezogenen Daten haben, sind auf das Datengeheimnis verpflichtet;
- Interessentendaten werden per E-Mail als verschlüsseltes PDF-Dokument an den Kunden versandt und können nur mit dem Passwort des Kunden geöffnet werden;
- Es werden keine Daten des Interessenten gespeichert.

2.5. Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

- Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind, ist für das Produkt nicht relevant, es werden keinerlei Daten des Interessenten gespeichert.

2.6. Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.

Maßnahmen (technisch/organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auf-traggeber und Auftragnehmer:

- Mitarbeiter sind auf das Datengeheimnis verpflichtet;
- Beim Einsatz von Subunternehmern werden schriftliche Vereinbarungen zur Auf-tragsdatenverarbeitung geschlossen.

2.7. Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

- Maßnahmen zur Datensicherung (physikalisch/logisch) entfallen, da keine Daten des Interessenten gespeichert werden.

2.8. Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- Daten von M&M werden getrennt von Kundendaten verarbeitet, im Übrigen werden keine Daten des Interessenten gespeichert.