ANLAGE 2:

VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG GEMÄß ART. 28 DSGVO

Definitionen, Präambel

„Hauptvertag" ist der Vertrag, zu dem vorliegende Vereinbarung zur Auftragsverarbeitung eine Anlage bildet oder der auf die Geltung der vorliegenden Vereinbarung zur Auftragsverarbeitung verweist.

„Auftragnehmer" im Sinne dieser Vereinbarung ist die **MORGEN & MORGEN GmbH, Elisabethenstraße 20, 65428 Rüsselsheim**.

„Auftraggeber" ist der Kunde, mit dem der Auftragnehmer den Hauptvertrag schließt.

Diese Vereinbarung regelt und konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im Hauptvertrag vereinbarten Auftragsverarbeitung ergeben und regelt die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers.

Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung i. S. d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)avv

Gegenstand und Dauer der Auftragsverarbeitung ergeben sich aus dem Hauptvertrag.

Die Art der Daten, Verarbeitungszwecke und Kategorien betroffener Personen ergeben sich aus Anlage 1 „Art der Daten, Verarbeitungszwecke und Kategorien betroffener Personen".

Anwendungsbereich und Verantwortlichkeit

Der Auftraggeber ist im Rahmen dieses Vertrags für die Einhaltung der gesetzlichen Regelungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung, allein verantwortlich.

Die Verarbeitung der Daten erfolgt ausschließlich auf Basis des Hauptvertrages und der Weisungen des Auftraggebers. Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die keinen Datenschutzbezug haben, werden als Antrag auf Leistungsänderung behandelt, sofern sie nicht vom vertraglichen Leistungsumfang abgedeckt sind. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

Pflichten des Auftragnehmers

Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrags und der Weisungen des Auftraggebers verarbeiten, außer es liegt anderer gesetzlicher Erlaubnistatbestand vor.

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung so lange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DSGVO erfüllt sind.

Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO, insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO, herzustellen. Dazu können auch genehmigte Verhaltensregeln gemäß Art. 40 DSGVO oder genehmigte Zertifizierungsverfahren gemäß Art. 42 DSGVO vorgelegt werden. Kann der Auftragnehmer keine Zertifizierungen bzw. genehmigten Verhaltensregeln vorlegen, kann durch den Auftraggeber oder einen Beauftragten ein Audit durchgeführt werden.

Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft hierzu die in Anlage 2 dargestellten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers im Sinne des Art. 32 DSGVO. Änderungen der in Anlage 2 vereinbarten technischen und organisatorischen Maßnahmen bleiben dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, nach Anmeldung und unter Berücksichtigung einer angemessenen Vorlaufzeit (mindestens 72 Zeitstunden, werktäglich) durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem direkten Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich vorstehender Absatz entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn die Aufsichtsbehörde einer gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß sanktionsbewehrt ist.

Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu mit dem Auftraggeber ab.

Der Auftragnehmer informiert den Auftraggeber unverzüglich über Verstöße gegen datenschutzrechtliche Vorschriften durch ihn, eingesetzte Mitarbeiter oder sonstige Dritte, sofern und soweit der Auftraggeber von der Datenverarbeitung als Verantwortlicher gemäß Art. 4 Abs. 7 DSGVO betroffen ist.

Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.

Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten und in notwendigem Umfang bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

Der Auftragnehmer stellt sicher, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrags fort.

Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrags anfallende Datenschutzfragen. Ansprechpartner beim Auftragnehmer ist:

Datenschutz Pöllinger GmbH
Gisela Pöllinger
Dresdner Str. 38
92318 Neumarkt
+49 9181 2705770
E-Mail: kontakt@datenschutz-poellinger.de

Bei einem Wechsel des Datenschutzbeauftragten informiert der Auftragnehmer den Auftraggeber und teilt schriftlich die geänderten Kontaktdaten mit.

Der Auftragnehmer gewährleistet, den Pflichten nach Art. 32 Abs. 1 lit. d DSGVO zu entsprechen und ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

Im Falle eines berechtigen Löschungsverlangens des Auftraggebers, d.h. die verlangte Löschung vom Weisungsrahmen umfasst ist, löscht der Auftragnehmer die gegenständlichen Daten. 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, sofern nicht im Vertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen, sofern und soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Der Auftragnehmer verzichtet auf ein eventuelles Zurückbehaltungsrecht, sofern und soweit keine ihn bindenden gesetzlichen Verpflichtungen entgegenstehen.

Pflichten des Auftraggebers

Der Auftraggeber ist für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer, sowie für die Rechtmäßigkeit der Datenverarbeitung in seinem Verantwortungsbereich allein verantwortlich und hat entsprechend seiner Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO und Art. 24 Abs. 1 DSGVO zu genügen.

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

Der Auftraggeber benennt dem Auftragnehmer einen Ansprechpartner für im Rahmen des Vertrags anfallende Datenschutzfragen nebst dessen Kontaktdaten (Anschrift, Telefonnummer, E-Mail-Adresse).

Anfragen betroffener Personen

Macht eine Person gegenüber dem Auftragnehmer ein Betroffenenrecht gemäß Artt. 12 ff. DSGVO (z.B. zur Berichtigung, Löschung oder Auskunft) geltend, leitet der Auftragnehmer die Anfrage unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im in notwendigen und angemessenen Umfang.

Subunternehmer (weitere Auftragsverarbeiter)

Der Einsatz von Subunternehmern durch den Auftragnehmer bedarf der vorherigen Zustimmung des Auftraggebers. Über den geplanten Einsatz eines Subunternehmers hat der Auftragnehmer den Auftraggeber rechtzeitig vorab und schriftlich zu informieren. Die Zustimmung zur Untervergabe gilt als erteilt, wenn der Auftraggeber nicht innerhalb von 6 (sechs) Wochen, beginnend mit Zugang der Information in vorstehendem Sinne, dem Einsatz des betreffenden Subunternehmers widerspricht. Ein solcher Widerspruch ist nur aus berechtigten Gründen zulässig, wie z. B. nicht ausreichende Zuverlässigkeit des Subunternehmers.

Widerspricht der Auftraggeber dem Einsatz eines vom Auftragnehmer gewünschten Subunternehmers, so ist der Auftragnehmer berechtigt, den Hauptvertrag ohne Einhaltung einer Kündigungsfrist und mit sofortiger Wirkung zu kündigen.

Setzt der Auftragnehmer berechtigt Subunternehmer ein, so erstreckt er seine datenschutzrechtlichen Pflichten aus diesem Vertrag auf den Subunternehmer. Hierbei steht es dem Auftragnehmer frei, auch an Subunternehmer zu vergeben, die das notwendige, angemessene Schutzniveau im Sinne Art. 32 Abs. 1 DSGVO durch andere technische und organisatorische Maßnahmen sicherstellen als in Anlage 2 zur vorliegender Vereinbarung zur Auftragsverarbeitung beschrieben, soweit sie das dort vereinbarte Schutzniveau nicht unterschreiten.

Der Auftragnehmer wird insbesondere durch geeignete Vertragsgestaltung sicherstellen, dass der Auftraggeber das Weisungsrecht und die vereinbarten Kontrollrechte auch unmittelbar gegenüber Subunternehmern ausüben kann.

Der Auftraggeber ist berechtigt, vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt des mit dem Subunternehmer geschlossenen Vertrags (ohne vergütungsbezogene Angaben) und die Umsetzung der datenschutzrechtlich relevanten Verpflichtungen des Subunternehmens zu erhalten, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen.

Der Auftraggeber stimmt bereits hiermit und nach Maßgabe der Regelungen dieser Ziffer 6 dem Einsatz der nachfolgend genannten Subunternehmer zu:

Firma Unterauftragnehmer	Anschrift	Leistung
PlusServer GmbH	Welserstraße 14 51149 Köln	Bereitstellung der Hostinginfrastruktur durch PlusServer GmbH, zur Speicherung der Daten aus dem online Vergleichsprogramm M&M Office und Backup.
insign GmbH	Am Bäckeranger 2 85417 Marzling	Bereitstellung von Webservices und Softwarekomponenten für die Verarbeitung der elektronischen Unterschrift des Kunden zum Zwecke der Einbettung der elektronischen Signatur inklusive biometrischer Daten in das Antrags-PDF für die Antragstellung. Das Antrags-PDF wird an den M&M Webservice rückübermittelt, zum Zwecke der Antragseinreichung von Krankenversicherungs-/ Lebens- und Altersvorsorgeprodukten für Kunden des Kunden (Verbraucher).

Lieferanten des Auftragnehmers, deren Leistungen sich nicht unmittelbar auf die Erbringung der Hauptleistungen beziehen (z.B. Telekommunikation, Post-/Transportdienstleistungen, Entsorgung, Facility Management...) sind keine Subunternehmer im Sinne dieser Vereinbarung zur Auftragsverarbeitung.

Sonderkündigungsrecht

Der Auftraggeber kann Verträge mit dem Auftragnehmer jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers oder dessen Subunternehmer gegen Datenschutzvorschriften oder eine Bestimmung dieses Vertrages vorliegt.

Ein schwerwiegender Verstoß liegt insbesondere dann vor, wenn der Auftragnehmer oder dessen Subunternehmer, die vereinbarten technischen und organisatorischen Maßnahmen, in erheblichem Maße nicht erfüllen oder nicht erfüllt haben oder Kontrollrechten des Auftraggebers nicht genügen. Bei sonstigen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

Haftung und Schadensersatz

Der Auftragnehmer haftet nach den gesetzlichen Bestimmungen.

Schlussbestimmungen

Die Regelungen dieser Vereinbarung zur Auftragsverarbeitung gehen den sonstigen Regelungen des Hauptvertrags vor.

Es gilt das Recht der Bundesrepublik Deutschland.

ANLAGE 1:

ART DER DATEN, VERARBEITUNGSZWECKE UND KATEGORIEN BETROFFENER PERSONEN

Art der Daten

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

- Personenstammdaten, insbesondere
  - Vor- und Nachnamen
  - E-Mail-Adressen
  - Telefonnummern
  - Anschriften
  - Arbeitsort
- Benutzernamen, Passwörter
- Ansprechpartner
- Bankverbindungsdaten (Kontonummer, Bankleitzahl, IBAN, BIC, Kontoinhaber)
- Kundendaten des Auftraggebers, insbesondere
  - Vor- und Nachnamen
  - Anschriften
  - E-Mail-Adressen
  - Telefonnummern
- Gesundheitsdaten
- Vertragsabrechnungs- und Zahlungsdaten,
- biometrische Informationen für die elektronische Signatur.

Verarbeitungszwecke

Art und Zweck der Verarbeitung sind

- die Durchführung des Vertragsverhältnisses
- die Bearbeitung von Support- und Wartungsanfragen des Auftraggebers
- die Bearbeitung von Entwicklungsanfragen des Auftraggebers
- die Identifikation berechtigter Supportanfragen
- die laufende Kommunikation mit dem Auftraggeber in Projekten bzw. im Rahmen der Durchführung von Vertragsverhältnissen
- die Durchführung von Software-Tests
- die Kontrolle der vertrags- und bestimmungsgemäßen Nutzung von Services und Produkten

Kategorien betroffener Personen

Betroffene sind

- der Auftraggeber
- die Interessenten, potentiellen Versicherungsnehmer und Endkunden des Auftraggebers
- ggfs. deren Familienangehörige
- sonstige Dritte, die sich an den Auftraggeber wenden, um sich von diesem über die Auswahl eines Versicherungsproduktes beraten zu lassen
- Mitarbeiter (mit und ohne Arbeitnehmerstatus) des Auftraggebers.
- Lieferanten des Auftraggebers
- Mitarbeiter von Lieferanten des Auftraggebers
- Sonstige Geschäftspartner des Auftraggebers und deren Mitarbeiter

ANLAGE 2:

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

1. Vertraulichkeit (Art. 32 Abs. 1b DS-GVO)

Zutrittskontrolle

Ein unbefugter Zutritt 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; Die Büroräume sind alarmgesichert;
→ Es existiert ein Zugangskontrollsystem in dem die zutrittsberechtigten Mitarbeiter mit unterschiedlichen Berechtigungen festgelegt sind;
→ Es bestehen Regelungen für Fremdpersonal, Reinigungspersonal und Besucher; Die Begleitung von Gästen ist in einer Richtlinie geregelt
→ Zutritt zu Serverraum und Archiv ist nur ausgewählten berechtigten Personen gestattet
→ Server befinden sich in abschließbaren Serverschränken
→ Datenträger werden unter Verschluss gehalten

Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.
Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

→ Die unbefugte Nutzung von IT-Systemen wird verhindert durch eine UserID, Passwortvergabe und Zugangsbeschränkung via RSA SecurID Token (teilweise);
→ Passwörter sind nur dem Nutzer bekannt;
→ Firewalls mit unterschiedlichen Sicherheitszonen. Trennung von Netzwerk-Segmenten (z.B. LAN, DMZ, VPN) mit entsprechendem Regelwerk.
→ Einsatz von RSA SecurID-Tokens für VPN-Zugriffe.
→ Virenscanner verschiedener Hersteller, SPAM-Filter.

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;
→ Organisatorische und technische Berechtigungsbewilligungen sind getrennt Für die Wiederherstellung von Backups besteht ein verbindliches Verfahren
→ Bei Programmentwicklungen erfolgt eine Trennung in ein Test- und ein Produktivsystem

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 Auftragnehmer werden getrennt von Auftraggeberdaten verarbeitet

Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

Im Rahmen der Verarbeitung von personenbezogenen Daten kommen verschiedene Verschlüsselungsmechanismen (z.B. SSL- Verschlüsselung bei Übertragung, externer Zugriff per VPN) zum Einsatz.

Pseudonymisierung
Bei Supporttickets können die personenbezogenen Daten, die der LN an M&M schickt, nicht pseudonymisiert werden.

2. Integrität (Art. 32 Abs. 1 b DS-GVO)

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 die Vertraulichkeit verpflichtet;
- → Backups auf Sicherungsbänder werden ausschließlich verschlüsselt erstellt (Auftragnehmer)
- → Der Datentransport erfolgt verschlüsselt.

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: Benutzerberechtigungen

- → sind festgelegt;
- → Berechtigungen sind differenziert nach Systemen/Datenbanken und nach Lesen/Ändern/Löschen;
- → Aufbewahrungsfristen für Backups sind festgelegt

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1b DS-GVO)

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen. Maßnahmen zur Datensicherung (physikalisch / logisch):

- → Storagesysteme sind grundsätzlich redundant ausgelegt (RAID5, RAID-DP oder RAID1);
- → Es besteht ein Backup- und Recoverkonzept;
- → Es besteht eine USV-Anlage
- → Sicherheitssysteme wie Firewall, Virenscanner und SPAM-Filter sind im Einsatz.

4. Verfahren zur regelmäßigen Überprüfung

Bewertung und Evaluierung (Art. 32 Abs. 1d DS-GVO; Art. 25 Abs. 1 DS-GVO) Datenschutz-Management;

- → Verarbeitung personenbezogener Daten gemäß Art. 5 DSGVO, Verzeichnis der Verarbeitungstätigkeit gemäß Art. 30 DSGVO
- → Verantwortliche und der Auftragsverarbeiter haben geeignete technische und organisatorische Maßnahmen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung von personenbezogenen Daten gemäß der Datenschutz-Grundverordnung, Art. 32 DSGVO, erfolgt.
- → M&M Office ist vom TÜV Rheinland auf Datenschutz und Datensicherheit zertifiziert. Diese Zertifizierung besteht durchgehend seit 2013
- → Es besteht ein Datenschutzmanagement Konzept

Incident-Response-Management (Art.33 Abs. 1 DS-GVO);

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Auftragnehmer diese unverzüglich dem Verantwortlichen. Er unterstützt ihn bei der Erfüllung seiner Pflichten aus Art. 33 DS-GVO, indem er im Rahmen seiner Möglichkeiten Informationen gem. Art. 33 Abs. 3 DS-GVO weitergibt, die der Verantwortliche für die Meldung bei der Aufsichtsbehörde benötigt.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);

Es werden nur Daten erfasst, verarbeitet und weitergegeben werden, wie für die Nutzung erforderlich sind. Der Auftraggeber als der Nutzer von M&M Office hat die Wahlfreiheit welche personenbezogenen Daten er in M&M Office eingeben möchte.

Auftragskontrolle

- → Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, Nennung des Dienstleisters, Vorabüberzeugungspflicht,
- → Verpflichtung der Mitarbeiter zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DS-GVO)
- → Beim Einsatz von Subunternehmern werden schriftliche Vereinbarungen zur Auftragsdatenverarbeitung geschlossen, die eingesetzten Subunternehmer sind dem Auftraggeber abschließend benannt