

Datenschutzinformationsblatt

Allgemeine Informationen zum Unternehmen:

Diese Datenschutzinformation gilt für unsere gesamte Unternehmensgruppe. Hierzu gehören die folgenden Firmen:

Kay Meyer FM-Consultants & CAD-Services e.K.
Geschäftsinhaber: Kay Meyer

FM-Connect.com Network GmbH Geschäftsführer:
Kay Meyer

CAD-Consortium.com GmbH
Geschäftsführer: Kay Meyer

FM-Workshops.com Akademie GmbH
Geschäftsführer: Kay Meyer

Alle Unternehmen haben ihren Sitz:
Am Altenfelsdeich 16
25371 Seestermühe

Im Folgenden sprechen wir von der Kay Meyer Unternehmensgruppe und meinen mit dieser Bezeichnung alle oben genannten Firmen.

Wie erreichen sie uns?

Sie erreichen uns postalisch unter der oben angegebenen Anschrift und wie folgt:

Telefon: 04125 / 398 99 23 Email:
info@kaymeyer.de

Wer ist bei uns verantwortlich für den Datenschutz?

Verantwortliche Stelle für die Kay Meyer Unternehmensgruppe gemäß Art. 4 Ziffer 7 DSGVO und nach § 3 Abs. 7 BDSG ist die:

Kay Meyer FM-Consultants & CAD-Services e.K.
Geschäftsinhaber: Kay Meyer
Am Altenfelsdeich 16 25371
Seestermühe

Wir haben einen Datenschutzbeauftragten bestellt:

Tobias Lange

Externer Datenschutzbeauftragter

Tegelsberg 53, 22399 Hamburg

www.externer-datenschutzbeauftragterhamburg.eu

info@dsb-hh.com

Wir nehmen den Schutz Ihrer Daten sehr ernst, speichern und verarbeiten diese nur nach den gesetzlichen Bestimmungen.

Personenbezogene Daten:

Wir speichern nur folgende personenbezogenen Daten: Vorname, Name, E-Mailadresse und Telefonnummern.

Die personenbezogenen Merkmale können mit Firma, Anschrift der Firma, Funktion oder Abteilung der betroffenen Person verknüpft sein.

Bei Nutzung unsere Website wird ihre IP-Adresse erhoben.

Wir speichern und verarbeiten hierüber hinaus keine personenbezogenen Daten, insbesondere keine sensiblen Daten.

Rechtsgrundlagen und Zweck der Speicherung und Verarbeitung Ihrer Daten:

Soweit Daten nicht auf gesetzlicher Verpflichtung, zum Zwecke der Erbringung einer vertraglich vereinbarten Leistung oder vorvertraglich, zur Anbahnung oder Aufnahme einer Geschäftsbeziehung, erhoben und verarbeitet werden, erheben wir personenbezogene Daten nur wie nachstehend:

Wir speichern personenbezogene Daten nur aufgrund einer von ihnen rechtswirksam erteilten Einwilligung. Die Speicherung und Verarbeitung erfolgt nur zum Zweck der Kontaktaufnahme und Zusendung für Informationen zu unseren Seminarangeboten in Ihrer Region sowie zu Neuerungen im Facility Marketing.

Wir sammeln ausdrücklich keine Daten aus öffentlich zugänglichen Quellen und kaufen keine Daten von Dritten.

Bei Besuch unsere Website erheben wir Ihre IP auf Grundlage eines berechtigten Interesses nach Art. 6 DSGVO lit. f.) in anonymisiert Form zu Zwecken des sicheren Betriebens unserer Website und zu Marketingzwecken. Wir setzen rechtskonform Marketingmittel auf unserer Webseite ein. Näheres zur Datenerhebung auf unserer Website entnehmen sie bitte der Datenschutzerklärung auf unsere Webseite.

Wir erheben und verarbeiten personenbezogene Daten zu keinem anderen Zweck, insbesondere führen wir diese nicht mit anderen Daten zusammen (Profiling) oder übermitteln Ihre Daten an Dritte.

Ihre Rechte:

Soweit Sie betroffene Person i.S.d. Art. 4 Nr. 1 DSGVO sind, haben Sie bezüglich der Verarbeitung Ihrer personenbezogenen Daten die nachstehenden Rechte:

Nach Art. 15 DSGVO haben Sie das Recht von der verantwortlichen Stelle eine Bestätigung darüber zu verlangen, ob personenbezogene Daten verarbeitet werden, und unentgeltliche Auskunft über die zu Ihrer Person gespeicherten personenbezogenen Daten zu erhalten.

Nach Art. 16 DSGVO haben Sie das Recht, die unverzügliche Berichtigung unrichtiger personenbezogener Daten zu verlangen. Zudem haben Sie das Recht, im Hinblick auf die Verarbeitung, die Vervollständigung unvollständiger personenbezogener Daten zu verlangen.

Nach Art. 17 DSGVO haben Sie das Recht, von der verantwortlichen Stelle zu verlangen, dass Ihre personenbezogenen Daten unverzüglich gelöscht werden, sofern einer der in Art. 17 DSGVO genannten Gründe vorliegt und soweit die Verarbeitung nicht weiter erforderlich ist.

Nach Art. 18 DSGVO haben Sie das Recht, die Einschränkung der Verarbeitung zu verlangen, wenn eine der in Art. 18 DSGVO genannten Voraussetzungen vorliegt.

Nach Art. 20 DSGVO haben Sie das Recht, Ihre personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und Sie haben das Recht, soweit in Art. 20 DSGVO nicht eingeschränkt, diese Daten einem anderen Verantwortlichen ohne Behinderung durch uns zu übermitteln.

Sie haben das Recht, eine erteilte Einwilligung zur Verarbeitung personenbezogener Daten jederzeit zu widerrufen. Der Widerruf entfacht nur Wirkung für die Zukunft. Den Widerruf richten Sie bitte an die oben angegebene verantwortliche Stelle.

Nach Art. 21 DSGVO haben Sie das Recht, jederzeit gegen die Verarbeitung ihrer personenbezogenen Daten Widerspruch einzulegen. Liegen die Voraussetzungen für einen wirksamen Widerspruch vor, darf eine Verarbeitung der personenbezogenen Daten nicht mehr erfolgen.

Sie haben, neben anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsmitteln, das Recht auf Beschwerde bei einer zuständigen Aufsichtsbehörde, wenn Sie der Auffassung sind, dass die Verarbeitung Ihrer personenbezogenen Daten gegen die Vorgaben der DSGVO verstößt. Die Beschwerde kann Online auf der Website der Aufsichtsbehörde erfolgen. Zuständige Aufsichtsbehörde wäre:

Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein
Holstenstraße 98
24103 Kiel
Tel.: 0431 / 988 1200 Fax: 0431 / 988
1223 E-Mail:
mail@datenschutzzentrum.de
<https://datenschutzzentrum.de>

Wie lange werden Ihre Daten gespeichert?

Personenbezogene Daten werden gelöscht, sobald deren Speicherung für die Erfüllung des ursprünglichen Zwecks nicht mehr erforderlich ist und keine gesetzlichen Aufbewahrungsfristen mehr bestehen.

Sofern Aufbewahrungsfristen bestehen, richtet sich die Speicherung personenbezogener Daten nach den gesetzlichen Aufbewahrungsfristen. Nach Ablauf der

gesetzlichen Fristen werden die entsprechenden Daten gelöscht. Beim Bestehen von Aufbewahrungsfristen, soweit ein Zweck zur Verarbeitung der Daten nicht mehr vorliegt, erfolgt eine Einschränkung der Verarbeitung der personenbezogenen Daten bis zur Löschung.

Unsere Technischen und Organisatorischen Maßnahmen (TOMs):

Nach Artikel 32 DSGVO treffen wir im angemessenen Verhältnis der Schutzbedürftigkeit Ihrer Daten technische und organisatorische Maßnahmen zur Sicherheit ihrer Daten.

Hierzu zählen verschiedene Maßnahmen in den Kategorien:

- Vertraulichkeit
- Integrität
- Verfügbarkeit und Belastbarkeit
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

1. Vertraulichkeit

Zutrittskontrolle:

Nur berechtigte Personen haben Zutritt zu unseren Geschäftsräumen. Wir setzen ferner Sicherheitsschlösser und Alarmanlagen ein. Der Zutritt zu unseren Geschäftsräumen wird aufgezeichnet und überwacht. Dieses schließt auch Besucher und Mitarbeiter dritter Unternehmen ein. Der Zutritt zu unseren Server-Räumen ist zusätzlich beschränkt und darf nur von besonders berechtigten Mitarbeitern erfolgen.

Zugangs- und Zugriffskontrolle:

Zum Schutz des Zugangs zu personenbezogenen Daten verwenden wir eine technische Verschlüsselung der Datenträger. Bei Fernzugriff auf personenbezogene Daten, verwenden wir VPN Technik. Unsere Server sind ferner mit einer Firewall und mit Anti-Viren Software gesichert, die Gehäuse sind verschlossen und der Zugang zum BIOS ist durch ein separates Passwort gesichert.

Ein Log-In/Zugriff auf personenbezogene Daten kann nur über einen Benutzernamen und Passwort

erfolgen. Wir vergeben und verwalten Benutzerberechtigungen nach dem Minimalprinzip und überwachen diese Fortlaufend.

Unsere Server werden durch Dritte verwaltet. Diese Dienstleister sitzen in Deutschland und sind mit einem AVV (Auftragsverwaltungsvertrag) auf den Schutz der Daten nach DSGVO verpflichtet.

Wir haben umfassende betriebliche Richtlinien zur sicheren Datenverarbeitung erarbeitet, auf welche unsere Mitarbeiter geschult sind. Wir haben unsere Mitarbeiter auf den Datenschutz nach DSGVO und BDSG schriftlich verpflichtet.

Alle Zugriffe auf, Änderungen und Neuanlagen von personenbezogenen Daten werden protokolliert.

Wir vernichten Datenträger und personenbezogene Daten in Papierform durch ein hierfür zertifiziertes Unternehmen, welche durch einen AVV (Auftragsverwaltungsvertrag) nach DSGVO verpflichtet ist. In Einzelfällen Schreddern wir Papier nach DIN 66399 mit mindestens Sicherheitsstufe P4.

Trennungskontrolle:

Wir trennen Kategorien von Daten durch Zugriffsberechtigungen, Datenbankmerkmale, Datenbankrechte und, bei Erfordernis, auf physikalischen Datenträgern.

Pseudo- und Anonymisierung von Daten:

In Abwägung der Verhältnismäßigkeit zum Aufwand und der Schutzbedürftigkeit der von uns erhobenen personenbezogenen Merkmale nehmen wir, zusätzlich zur Verschlüsselung der Daten, keine zusätzliche Pseudo- und Anonymisierung vor.

2. Integrität

Weitergabekontrolle:

Wir weisen nochmals daraufhin, dass wir grundsätzlich keine Daten weitergeben, veräußern oder außerhalb unserer Unternehmensgruppe verarbeiten, soweit gesetzliche oder vertraglich vereinbarte Bestimmungen nicht anderes verlangen.

In seltenen Fällen werden einzelne Datensätze an Mitarbeiter im Außendienst übermittelt bzw. diesen der Zugriff hierauf erlaubt. Wir Nutzen hierfür VPN-Technik, Verschlüsselung wie SSL etc., insbesondere in der E-Mailkommunikation, als auch Signaturverfahren und andere technische Standards. Alle Zugriffe werden protokolliert.

Soweit Daten physikalisch bewegt werden, erfolgt dieses in sicheren Transportbehältern unter besonderer Sorgfalt.

Unsere Mitarbeiter werden auf den Datenschutz regelmäßig geschult und die Übermittlung von Daten erfolgt unter Abwägung der Schutzbedürftigkeit der Daten mit geeigneten Mitteln, die in einem betriebsinternen Leitfaden festgelegt sind. In diesen Regeln finden sich auch eindeutige Anweisungen zum Zeitraum der Speicherung und zur Löschung.

Eingangskontrolle:

Alle bei uns eingehenden neuen Daten, sowie Änderungen und Löschungen, werden technisch verarbeitet. Die entsprechenden Protokolle werden regelmäßig überprüft.

Unsere Mitarbeiter sind individuell für den Zugriff auf unsere EDV berechtigt und auf den richtigen Umgang mit unseren EDV-Lösungen eingehend geschult. Jede Eingabe, Änderung oder Löschung von Daten kann individuell nachverfolgt werden.

3. Verfügbarkeit und Belastbarkeit:

Verfügbarkeitskontrolle:

Unsere Serverräume sind nach den allgemeinen Standards überwacht und gesichert, insbesondere durch Alarm- und Brandschutzmaßnahmen.

Wir erstellen regelmäßige Datensicherungen nach den allgemein gültigen Standards für Backups. Die korrekte Erstellung von Backups wird durch entsprechend hierfür benannter Mitarbeiter kontrolliert und die Datenwiederherstellung aus Backups regelmäßig getestet.

Für eine externe Sicherung greifen wir auf

Drittanbieter zurück, welche durch ordentlichen AVV (Auftragsverarbeitungsvertrag) verpflichtet sind und entsprechende Zertifizierungen aufweisen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutzmaßnahmen:

Wir führen eine zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz in einem Intranet mit Zugriffsmöglichkeit für alle Mitarbeiter nach Bedarf / Berechtigung.

Für das Datenschutzmanagement haben wir einen externen Datenschutzbeauftragten beauftragt, der, auch unter der Hilfe von Datenschutz-Software, die Einhaltung der Vorschriften nach DSGVO und BDSG überwacht, dokumentiert und ggf. modifiziert.

Wir kommen den Informationspflichten nach Artikel 13 und 14 DSGVO nach. Soweit Folgenabschätzungen oder weitere Einhaltungen von Pflichten nach DSGVO erforderlich sind, wird unser externer Datenschutzbeauftragter dieses entsprechend umsetzen.

Wir überprüfen mindestens jährlich die Wirksamkeit aller technischen und organisatorischen Maßnahmen. Wir schulen und sensibilisieren unsere Mitarbeiter mindestens jährlich auf Datenschutz.

Ein betrieblicher Leitfaden mit einem Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden.

Incident-Response-Management:

Wir setzen technisch ein und aktualisieren regelmäßig: Firewall, Spamfilter, Virens Scanner und weitere Schutzmaßnahmen.

Wir haben einen betrieblichen Leitfaden zum Umgang mit relevanten Sicherheitsvorfällen, insbesondere zur Erkennung, Meldung und Dokumentation solcher Fälle.

Sicherheitsvorfälle werden umgehend dem Datenschutzbeauftragten und dem betrieblich Verantwortlichen gemeldet.

Datenschutzfreundliche Voreinstellungen:

Es werden von uns nicht mehr personenbezogene Daten erhoben und verarbeitet, als minimal, zur Ausübung des Zwecks, erforderlich sind.

Wir haben technische Maßnahmen geschaffen, mit welchen Betroffene auf einfachste Weise einen Widerruf ausüben oder ihre weiteren Rechte nach der DSGVO geltend machen können.

Auftragskontrolle:

Wir wählen unsere Auftragnehmer, Subunternehmer und Dienstleister sorgfältig aus. Je nach Art und Umfang der Tätigkeit dritter Unternehmen überprüfen wir deren Datenschutzmaßnahmen oder lassen uns entsprechende Bestätigungen über die Umsetzung technischer und organisatorischer Maßnahmen bescheinigen.

Wir schließen mit allen Auftragnehmern, Subunternehmern und Dienstleistern entsprechend notwendige Vereinbarung nach den Vorschriften der DSGVO und dem BDSG, zum Beispiel AVVs (Auftragsverarbeitungsverträge), Geheimhaltungsverpflichtungen etc.

Soweit erforderlich vereinbaren wir mit unseren Auftragnehmern, Subunternehmern und Dienstleistern das Recht auf Wahrnehmung von Kontrollrechten und ggf. auch Weisungsrechte.

Sie haben weitere Fragen zum Datenschutz in der Kay Meyer Unternehmensgruppe?

Datenschutz ist uns ein besonders wichtiges Anliegen. Sollten Sie weitere Fragen hierzu haben, die wir mit unserem Informationsblatt nicht klären konnten, zögern Sie nicht den Kontakt zu uns aufzunehmen. Wir erörtern mit Ihnen sehr gerne Ihr Anliegen.