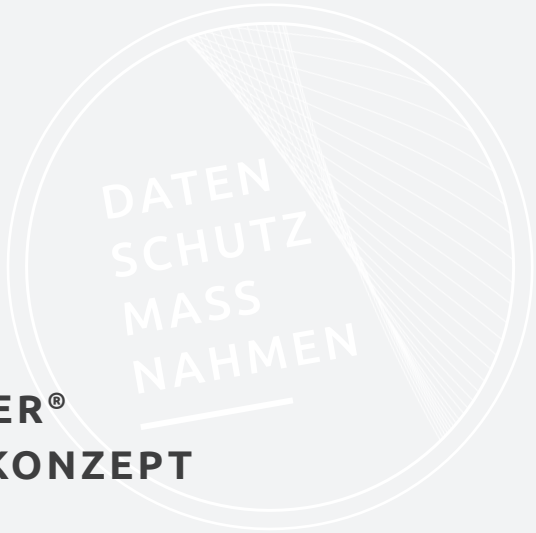


KUNDENMEISTER®
DATENSICHERHEITSKONZEPT

DATENSCHUTZMASSNAHMEN

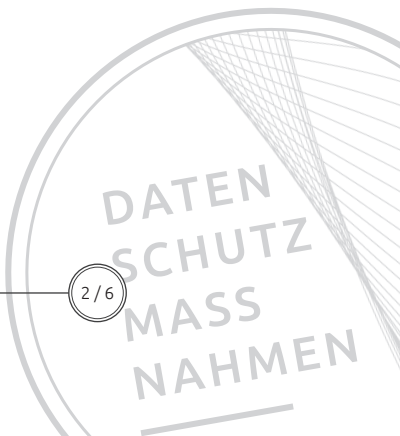
KundenMeister®

KundenMeister
Koerbler GmbH
Hofweg 1 | A-8430 Leitring
Tel.: +43 (0)3452 214 214
Fax: +43 720 555 204
office@kundenmeister.com | www.kundenmeister.com

Sehr geehrte Damen und Herren,

Die Sicherheit unserer CRM Software KundenMeister und speziell Ihrer Daten ist uns ein zentrales Anliegen!

Dieses Datensicherheitskonzept beinhaltet alle Maßnahmen, die wir zum Schutz Ihrer Daten innerhalb unseres Systems bzw. unseres Unternehmens durchführen.



1. Zutrittskontrolle

Folgende Maßnahmen gewährleisten, dass Unbefugte nicht in der Lage sind, sich physisch den Datenverarbeitungsanlagen (Unternehmen und Rechenzentrum), mit denen personenbezogene Daten verarbeitet bzw. gespeichert werden, nähern zu können.

a. Zutrittskontrolle zum Rechenzentrum

- Ausschließlich befugte Personen haben Zutritt mittels eines Kartensystems. Die Inhaber von Zugangskarten sind durch Lichtbildausweis identifiziert. Jeder Zutritt wird im Logsystem protokolliert.
- Der gesamte Serverraum ist mit Videoüberwachung (pro Gang eine Kamera) ausgestattet. Die Videodaten werden in der der ÖBB-Zentrale in Wien aufgezeichnet, es kann daher durch einen Diebstahl der Kameras nicht zu Datenverlust kommen.

b. Zutrittskontrolle zu den Büroräumlichkeiten der Koerbler GmbH

- Zutritt zu den Büroräumen haben grundsätzlich nur Mitarbeiter von Körbler.
- Gäste müssen sich am Empfang anmelden und dürfen sich nicht unbegleitet im Büro bewegen.
- Zutritt zu den Betriebsräumen ist nur mit einem Sicherheitsschlüssel möglich.
- Türe, Tore und Fenster sind außerhalb der Betriebszeiten fest verschlossen.

2. Zugangskontrolle

Mit folgenden Maßnahmen gewährleistet die Körbler GmbH, dass Unbefugte nicht in der Lage sind, vorhandene Datenverarbeitungssysteme und technische Lösungen zu nutzen.

- Der elektronische Zugang zu Systemen über Netzwerk ist durch Firewalls und VPNs geschützt.
- Die administrativen Zugangsdaten zu den jeweiligen Serversystemen sind nur den Administratoren bekannt.
- Jeder Nutzer erhält einen personalisierten, passwortgeschützten Account.
- Das Passwort ist in regelmäßigem Abstand zu ändern und muss eine Kombination aus Buchstaben und Ziffern beinhalten. Dabei können die letzten 5 Passwörter nicht wiederverwendet werden. Dies ist in der Sicherheitsrichtlinie Passwort-Policy dokumentiert.
- Pro Benutzer wird eine individuelle Benutzererkennung vergeben.
- Passwörter können individuell vom Benutzer festgelegt werden.
- Passwörter müssen aus mindestens 8 Zeichen bestehen und mindestens ein Sonderzeichen und/oder eine Zahl enthalten.

3. Zugriffskontrolle

Nachstehende Maßnahmen gewährleisten, dass Befugte ausschließlich dann auf Kundendaten zugreifen, wenn der Kunde eine Anfrage beim Kundensupport gestellt hat oder der Datenzugriff erforderlich ist, um die Services bereitzustellen oder Service- bzw. technische Probleme zu vermeiden oder zu behandeln.

- Zu Kundensystemen erhalten nur die Administratoren Zugriff, die den Kunden betreuen.
- Individuelle Zuweisung von Rechten pro Benutzer.
- Zugriff auf Systeme mit Kundendaten haben nur ausgewählte Mitarbeiter, die einen solchen Zugriff für Ihre Tätigkeit zwingend benötigen.

4. Weitergabekontrolle

Folgende Maßnahmen stellen sicher, dass personenbezogene Daten nicht an Unbefugte weitergegeben und ausschließlich verschlüsselt übertragen werden.

- Außer zum Zwecke der Datensicherung erfolgt die Weitergabe personenbezogener Daten nur auf explizite Anweisung durch den Kunden (schriftlicher Change-Request oder Auftrag).
- Die Daten sind durch Firewalls und Virenschutzsysteme vor dem Zugriff von außen, sowie Manipulationen, geschützt.
- Alle Mitarbeiter sind zur Verschwiegenheit und zur Einhaltung des Datengeheimnisses verpflichtet.
- Zugriffe auf Daten im Rechenzentrum erfolgen ausschließlich über verschlüsselte Verbindungen.

5. Eingabekontrolle

Nachstehende Maßnahmen garantieren, dass nachträglich geprüft werden kann, wer und wann personenbezogene Daten im KundenMeister eingegeben, verändert oder entfernt hat.

- Zur Gewährleistung der Eingabekontrolle sind Protokollierungs- und Protokollauswertungssysteme integriert.
- Das Nachverfolgen von Dateneingaben wird, wo technisch möglich, durch das etablierte Logging-Verfahren gewährleistet. Somit ist es jederzeit nachvollziehbar welche User Daten eingegeben haben.
- Jede Eingabe oder Änderung von Kundendaten wird protokolliert.
- Jede Administratortätigkeit (z.B. Anlegen oder Löschen von Benutzern, Änderungen der Benutzerrechte) wird protokolliert (Syslog).

6. Auftragskontrolle

Folgende Maßnahmen gewährleisten, dass die Datenverarbeitung nur entsprechend den Weisungen des Auftraggebers durchgeführt wird.

- Alle Mitarbeiter werden regelmäßig zum Datenschutz geschult.
- Arbeitsanweisung werden in Schrift- oder Textform dokumentiert.

7. Verfügbarkeitskontrolle

Nachstehende Maßnahmen stellen den Schutz personenbezogener Daten sicher.

- Alle Systeme, die im Zusammenhang mit der Verarbeitung von personenbezogenen Daten genutzt werden, werden im Rahmen des Backup-Dienstes regelmäßig gesichert und die Konsistenz der Sicherung wird geprüft.
- Brand- und Rauchüberwachung: Das Rechenzentrum ist mit einem Brandfrüherkennungssystem ausgestattet. Bei Rauch- und Hitzeentwicklung wird sofort in der Zentrale Alarm ausgelöst. Sofern notwendig, wird auch die automatische Löschanlage aktiviert.
- Brandlöschanlage: Das Rechenzentrum ist mit einer automatischen Gaslöschanlage ausgestattet. Die Flutung mit Stickgas zerstört keine Computerhardware und ist somit auf Schadenvermeidung optimiert.
- Alle Systeme sind mit unterbrechungsfreier Stromversorgung ausgestattet. Diese Systeme stellen auch einen Überspannungsschutz dar. Das Rechenzentrum wird in einem stabilen und redundanten Stromnetz betrieben.

8. Trennungskontrolle

Folgende Maßnahmen garantieren die getrennte Verarbeitung von Daten.

- Daten welche zu unterschiedlichen Zwecken erhoben wurden, werden getrennt voneinander verarbeitet.

9. Datensicherung und Löschung

a. Ort der Datensicherung

Unser Serverstandort befindet sich in Österreich im Rechenzentrum der eww ITandTEL.

eww ag

Stelzhamerstraße 27
4600 Wels
T.: 07242 493-0
F.: 07242 493-138
info@eww.at

Vorteile unseres Rechenzentrums:

- 24x7 Erreichbarkeit
- Redundante High-Speed Glasfaseranbindung
- providerunabhängig
- Hochverfügbare Stromanbindung (99,9%)
- Redundante USV-Anlage mit Batterie und Generator
- Energieeffizientes, redundantes Klimakonzept
- Brandfrühesterkennung und Brandlöschanlage
- Überwachung durch Netzwerk-Management und Building-Management-System
- Protokolliertes Zutritts-System
- Zertifizierung nach ISO/IEC 27001
- Green IT: umweltschonend und sparsam

b. Dauer der Datensicherung

Wir erstellen für unsere Kunden sechs Wochen lang tägliche Datensicherungen. D.h. die letzten 42 Tage werden täglich für Sie gesichert. Eine Wiederherstellung der Daten ist nach dem Fair-use-Prinzip möglich, was bedeutet, dass wir prinzipiell nichts für eine Wiederherstellung verlangen.

c. Dauer der Datenlöschung

Eine von Ihnen beantragte Löschung wird im Regelfall innerhalb von 2 Werktagen durchgeführt.

Zudem ist es möglich einzelne Datensätze zu löschen, jedoch müssen wir Sie darauf hinweisen, dass das Löschen einzelner Datensätze, sofern nicht genau definiert was zu löschen ist, Kosten verursacht, die wir gegenüber unseren Kunden geltend machen müssen.

Wenn eine Wiederherstellung von Daten notwendig sein sollte, wird darauf geachtet, dass gelöschte Daten nicht wiederhergestellt werden.