

# MARC MASSELIER

## Datensicherheitserklärung

### Lesbarkeit

Im Interesse einer besseren Lesbarkeit werden Texte geschlechtsneutral formuliert und diese gelten auch für eine Mehrzahl von Personen.

### Datensicherheitserklärung

Diese Datensicherheitserklärung gilt für alle Geschäftsbereiche der MARC MASSELIER | Treuhand & Informatik, nachfolgend "MTI" genannt.

Sollten sich zwischen dieser Datensicherheitserklärung und den sonst anwendbaren Vertrags- oder Geschäftsbedingungen der irgendwelche Widersprüche ergeben, so haben die Bestimmungen dieser Datensicherheitserklärung Vorrang.

### Kundeninformation

Die wenigsten Unternehmer wissen um die Risiken der digitalen Welt: Angriffe durch Hacker sind eher die Ausnahme; unzureichende Datensicherung auf veralteten Medien, vernachlässigter Virenschutz bei E-Mails, ungeschützte Online-Verbindungen und fehlende Mitarbeiterüberwachung führen häufiger zu Schäden an Unternehmen. Wir kümmern uns proaktiv um die Einhaltung der Datenschutzbestimmungen in allen Bereichen.

### Hightech Datacenter – Software as a Service (SaaS) – Cloud System

MTI bietet Ihnen ein einzigartiges Paket von Programmen, welche Ihnen ermöglichen, leicht und einfach mit den Business Softwares und den damit verbundenen Programmen zu arbeiten.

### Wie ist das möglich?

MTI stellt Ihnen Ihren Arbeitsplatz in der Cloud zur Verfügung. Alles funktioniert online - Sie nutzen die Programme über eine Internetverbindung auf günstiger monatlicher Mietbasis. Damit haben Sie weltweit Zugriff auf Ihre Software. Sie haben stets die aktuelle Version der Software zur Verfügung - Update-Kosten gibt es nicht.

Wir sorgen dafür, dass Sie genügend Serverkapazität und Rechenleistung zur Verfügung haben. Die Serveranlagen werden in zwei hochverfügbaren Datenzentren in der Schweiz betrieben. Diese Datenzentren befinden sich in 2 örtlich getrennten, geheimen Festungsanlagen der Schweizer Armee im Berner Oberland. Ein Datenzentrum profitiert von einem militärischen EMP Schutz und das andere Zentrum von einem natürlichen unterirdischen Kühlwassersee.

### Folgende weitere Sicherheitsaspekte können wir Ihnen auch noch bieten

- Hochleistungs-Server;
- Leistungsfähige Storage Systeme, redundante Router und Firewalls;
- Stromversorgung mit Diesel und USV;
- Umfassender Brandschutz;
- Redundante Klimatisierung;
- Zutritt über Vereinzelnungs- oder Materialschleuse;
- 24 x 7h Video- und Laser-Monitoring;
- 24 x 7h Monitoring Operations-Center;
- 5-fach redundante Einführung von fünf Carriers - leistungsfähiges Breitbandnetz;
- Getrennte Rohr- und Streckenführung;
- FINMA compliant (reviewed);
- Tier Level 3 TIA-942 Uptime Institute.

Marc Masselier  
Treuhand & Informatik  
Himmenreichstrasse 29  
CH-8570 Weinfelden

 +41 77 482 06 42  
 marc@masselier.ch  
 www.masselier.ch

Geschäftsführer Marc Masselier  
UID Register Nr. CHE-469.286.914  
MWST Nr. CHE-469.286.914 MWST

# MARC MASSELIER

## **Datensicherheit**

Die Daten werden auf unserem Backup-System gesichert. Ihre Daten werden redundant synchron gespiegelt. Jeden Tag wird eine komplette Sicherung in das zweite Datacenter gemacht.

## **Download der Daten immer möglich**

Mit unserer Software haben Sie die Fäden selbst in der Hand. Sie machen sich nicht abhängig! Sie können die Daten auf Ihrem lokalen Computer sichern. Hierdurch können Sie Ihre eigene Datensicherungspolitik weiterverfolgen.

## **So schützen wir Ihre Daten vor unbefugtem Zugriff - Benutzername und Passwortabfrage**

Jeder Nutzer erhält Zugangsdaten bestehend aus Benutzernamen und Passwort welche von uns definiert und fixiert werden. Sämtliche Zugriffe auf sind nach dem Mandantenprinzip voneinander getrennt, damit ein Kunde nicht Zugang zu Fremddaten erhält. Jeder Nutzer ist vertraglich verpflichtet, die Geheimhaltung der Zugangsdaten sicherzustellen.

Bitte beachten Sie den korrekten Umgang mit Ihren Zugangsdaten. Halten Sie Ihre Zugangsdaten unbedingt geheim und teilen Sie diese niemandem mit! Merken Sie sich Ihr Kennwort gut. Falls Sie sich Ihr Kennwort doch notieren, sorgen Sie dafür, dass niemand Zugang zu diesen Papieren hat. Speichern Sie Ihr Kennwort nicht auf dem Computer. Bei der Eingabe des Kennwortes sollten Sie sicherstellen, dass Ihre Eingaben nicht von Unbefugten beobachtet werden. Falls Sie vermuten, dass ein Unbefugter Ihre Zugangsdaten kennt, melden Sie uns dies umgehend, dass wir Ihre Anmeldedaten sofort ändern können. Melden Sie sich an Ihrem Computer ab oder sperren Sie diesen, wenn Sie Ihren Arbeitsplatz verlassen.

## **Secure Socket Layer (SSL) – 128 Bit Verschlüsselung (HTTPS)**

Diese Methode verschlüsselt sämtlichen Datenverkehr zwischen Kundenbrowser und Server-System. Der Aufruf der Internetseite sollte unbedingt mit einem SSL-fähigen Browser erfolgen (alle neueren Browser). Die Verschlüsselung erfolgt automatisch, wenn Sie `https://...` anstatt nur `http://...` eingeben. Das "s" hinter dem http bewirkt die verschlüsselte Verbindung! Bitte auf die Gültigkeit des ausgestellten Zertifikats achten. Doppelklicken Sie auf das geschlossene Schloss - Sie erhalten Informationen über das Zertifikat.

## **Interner Datenzugriff**

Die Mitarbeiter der MTI sind vertraglich verpflichtet, das Datenschutzgeheimnis zu wahren. Eine Weitergabe dieser Daten an Dritte erfolgt nur, wenn dies für die Vertragserfüllung notwendig ist. Solche Dritte sind ebenfalls von der MTI durch Vereinbarungen zur Beachtung des Datenschutzes der Nutzer verpflichtet. Mitarbeiter von MTI können Informationen über den Kunden und dessen Datenbestände zum Zwecke der Behebung von Störungen oder der Bearbeitung von Supportanfragen einsehen.

## **Ihre Datenschutzverpflichtung: Informations- und Aufklärungspflichten gegenüber Ihren Kunden**

Wir weisen darauf hin, dass Sie als Nutzer unserer Software gegenüber Ihren Kunden die Datenschutzgesetze der Schweiz zu beachten haben. Im Rahmen des Nutzungsverhältnisses unserer Software verwalten Sie individuelle und personenbezogene Daten auf unseren Servern. Sie sind deshalb verpflichtet datenschutzrechtliche Bestimmungen einzuhalten. In speziellen Fällen kann dadurch auch eine Informations- und Aufklärungspflicht gegenüber bestehen. Je nach Art der verwalteten Daten kann ein Einverständnis der Personen erforderlich sein, deren Daten verwaltet werden. Exemplarisch seien an dieser Stelle nur Ärzte oder Anwälte genannt, die beim Umgang mit ihren Patientenbeziehungsweise Mandantendaten aufgrund der Schweigepflicht besonders strengen Anforderungen unterliegen.