

ComMusic – Frank Wiczorek e.K.

# **Sicherheitsmechanismen im Serverbetrieb**

Beschreibung der technischen Maßnahmen zum Datenschutz für die Produkte im Serverbetrieb

Stand 18.04.2018

# ComMusic-Sicherheitsmechanismen im Serverbetrieb

Dieses Dokument beschreibt die Maßnahmen der Firma ComMusic – Frank Wieczorek e.K. zur Umsetzung des Datenschutzes im Serverbetrieb gemäß der EU Datenschutz Grundverordnung (DSGVO).

Wie Sie diese Maßnahmen richtig nutzen und Ihren Verein lokal und im Serverbetrieb absichern, finden Sie im Hilfeartikel „Leitfaden für Vereine zur DSGVO“.

## 1) SERVER STANDORT

Die Server von ComMusic stehen in einem Rechenzentrum der Strato AG in Deutschland. Zu den Sicherheitsmechanismen von Strato gibt es weitere Informationen unter folgendem Link:

<https://www.strato.de/sicherheit/>

Die Server sind nur eingeschränkt über das Internet erreichbar und zwar ausschließlich wie folgt:

- ComMusic-Software (verschlüsselt RSA2048, AES-256)
- mit Zertifikaten abgesichertes, verschlüsseltes VPN (nur für geschulte Mitarbeiter von ComMusic)
- Login bei Webanwendung und WOM - per EV-SSL-Zertifikat gesichert und verschlüsselt
- weitere Kommunikation mit SSL-Zertifikat gesichert und verschlüsselt

## 2) ZUGRIFFSSCHUTZ

Für jeden Verein existiert eine eigene Access-Datenbank auf einem der Server. Alle Daten des Vereins - die Datenbank selbst, sowie Ehrungs- und Meldedateien, Reporterdokumente und Protokolle - liegen mit AES-256 verschlüsselt auf dem Server. Bei Bedarf werden die Daten entschlüsselt und anschließend wieder verschlüsselt. Der Schlüssel dafür liegt nur auf dem Server in einem abgesicherten Bereich und wird permanent auf unberechtigte Zugriffe überwacht.

Die Verbindung zwischen Software und Server wird über einen Handshake mit RSA-2048 hergestellt und ist ebenfalls mit AES-256 verschlüsselt. Alle Nutzerpassworte sind „gesalzen“ und mit SHA-512 gehasht.

Zugriff auf die Vereinsdatenbank und die dazugehörigen Dateien und Dokumente bekommen nur Mitglieder, die der Administrator des Vereins dazu ermächtigt hat. Der Administrator wird bei Vertragsabschluss von einer vertretungsberechtigten Person des Vereins festgelegt. Innerhalb des ComMusic-Programms gibt es einen weiteren Zugriffsschutz, den der Administrator bis auf Register Ebene mit individuellen Zugriffsrechten versehen kann.

Über diese Absicherung des Servers, der Daten des Vereins auf dem Server, der Kommunikation mit dem Server und der Zugriffsrechte innerhalb der Vereinsdatenbank sind die Daten der Vereine sicher vor dem unbefugten Zugriff von Dritten auf dem Server geschützt.

## 3) SICHERUNG

Die Server werden automatisch jeden Tag auf mehreren verschiedenen Systemen an verschiedenen Standorten verschlüsselt gesichert.

Nutzer mit einem Premium- oder einem Verbandsserververtrag können sich täglich eine verschlüsselte Datensicherung an ein oder mehrere E-Mail-Adressen zusenden lassen. Diese wird bei Änderungen am Datenbestand automatisch nachts versendet. Damit kann im Verein ein zusätzliches eigenes Sicherungskonzept über mehrere Generationen aufgebaut werden.

Zudem besteht für alle Anwender die Möglichkeit, jederzeit manuelle Datensicherungen anzulegen.

#### 4) PERFORMANCE, REDUNDANZ UND SKALIERBARKEIT

Da es sich bei den Servern von ComMusic um ein System von mehreren, unabhängigen Servern handelt, können die Benutzer auf die einzelnen Server verteilt werden. Das System ist dabei so flexibel aufgebaut, dass es jederzeit um weitere Server erweitert werden kann. Dadurch können die Server auch regelmäßig erneuert und aktualisiert werden.

Die einzelnen Server sind jeweils mit gespiegelten Festplatten (RAID 1) ausgerüstet, um Datenverlust beim Ausfall einer Festplatte zu vermeiden.

Durch dieses Konzept wird sichergestellt, dass jeder Benutzer ausreichend Ressourcen zur Verfügung hat. Bei Ausfall einer Festplatte kann ohne Datenverlust weitergearbeitet werden und selbst beim Komplettausfall eines Servers kann ein anderer dessen Aufgaben übernehmen.

#### 5) ÜBERWACHUNG

##### 5.1) Ausfallsicherheit

Alle Server werden ständig (1 x pro Minute) von zwei verschiedenen Standorten auf ihre Verfügbarkeit überprüft.

##### 5.2) Unberechtigte Zugriffe

Unberechtigte Zugriffe, also solche, die die Rechte eines Nutzer überschreiten oder von der ComMusic-Software ausgehen, werden vom System automatisch protokolliert. Die betroffene IP-Adresse wird danach für einen bestimmten Zeitraum gesperrt. Diese Maßnahme dient vor allem zum Schutz vor noch unbekanntem Sicherheitslücken.

Es wird sowohl bei Nichterreichbarkeit als auch bei unberechtigten Zugriffen das Serviceteam sofort per E-Mail benachrichtigt. Dadurch werden eventuelle Ausfälle, Instabilitäten und Angriffe sofort erkannt und es können innerhalb kürzester Zeit Gegenmaßnahmen ergriffen werden.

##### 5.3) Protokollierung

Alle Produkte von ComMusic protokollieren die Eingaben von Nutzern und schreiben Nutzernamen, Datum, Uhrzeit und die vorgenommenen Änderungen, Löschungen, Neuaufnahmen, sowie An- und Abmeldung eines Nutzers in die Logdatei des Vereins. Dieses Protokoll kann in den Anwendungen aufgerufen und angezeigt werden.