ComMusic – Frank Wieczorek e.K.

Leitfaden zur Umsetzung der Datenschutzgrundverordnung in der ComMusic-Software

Ein Leitfaden für die Vereine zur Umsetzung der DSGVO bei der Anwendung der ComMusic-Software

27.04.2018

Inhalt

Leitfaden zur Umsetzung der EU-Datenschutzgrundverordnung (DSGVO) im Verein mit der ComMusic-Software

In diesem Leitfaden finden Sie alle nötigen Schritte zur Umsetzung der DSGVO in Ihrem Verein. Trotz größter Sorgfalt ist es möglich, dass nachträgliche Änderungen oder spezielle Details keine Beachtung fanden.

1) Haftungsausschlusserklärung

Dieses Dokument enthält Angaben, die nur zu Informationszwecken gedacht sind. Diese stellen weder eine Rechtsberatung dar, noch erhebt die vorliegende Zusammenstellung einen Anspruch auf Vollständigkeit.

Verbindlich ist immer der entsprechende Gesetzestext. Bitte haben Sie Verständnis dafür, dass ComMusic keine Haftung für die Richtigkeit der folgenden Angaben übernehmen kann.

2) Pflichten des Administrators

2.1) Nutzerverwaltung

Der Administrator des Vereins ist für die Einrichtung der Nutzerkonten verantwortlich. Laut der DSGVO muss nachvollziehbar sein, wer welche Änderungen an Daten durchgeführt hat. Deshalb benötigt jeder Nutzer des Vereins ein eigenes Nutzerkonto mit Passwort. Mehrere Nutzer die denselben Zugang zum Programm benutzen, stehen im Widerspruch zur DSGVO. Jeder Nutzer darf außerdem nur Zugriff auf die Daten bekommen, die er für die Erfüllung seiner Aufgaben benötigt. Wie genau Konten eingerichtet werden, finden Sie in der Hilfe oder unter

https://www.commusic.de/hilfe/module_2_6_5.html

2.2) Sicherung der Vereinsdaten

Der Verein muss sich gegen den Verlust seiner Daten absichern und ist für Sicherungen (Backups) selbst verantwortlich. Es wird explizit darauf hingewiesen, dass Datensicherungen zusätzlich auf einer anderen Hardware (USB-Stick, separate Festplatte, Laptop usw.) gespeichert werden sollten. Die Datensicherungen finden Sie im Backupverzeichnis, das Sie im Menü „Einstellungen“ unter „Verzeichnisse ändern“ anpassen können.

Hat der Verein einen Serververtrag, werden die vom Programm auf dem Server angelegten Backups automatisch jeden Tag auf mehreren verschiedenen Systemen an verschiedenen Standorten verschlüsselt gesichert. Siehe technisch organisatorische Maßnahmen.

https://www.commusic.de/dokumente/tom.pdf

Wie Sie eine Datensicherung vom Server laden, ist im folgenden Hilfeartikel beschrieben

https://www.commusic.de/hilfe/module_2_2_1_4.html

2.3) DSGVO-konformes Arbeiten im Serverbetrieb und lokal

Mit der ComMusic-Software kann lokal oder, falls ein Serverplatzvertrag abgeschlossen wurde, im Serverbetrieb gearbeitet werden. Alle relevanten Dateien, wie Datenbank, Datensicherung, Ehrungs-, Melde- und Lehrgangsdateien, sowie Dokumente und sonstige Dateien, die für den Serverbetrieb eines Vereins notwendig sind, werden nach aktuellem Stand der Technik auf dem Server verschlüsselt gespeichert. Im Fall

einer Kommunikation mit dem übergeordneten Verband findet die Übertragung ebenfalls genauso sicher verschlüsselt statt. Ein DSGVO-konformes Arbeiten ist hier problemlos möglich.

Im Lokalbetrieb kann die Verwaltung nur nach den Richtlinien der DSGVO durchgeführt werden, wenn eine Person die Datenverarbeitung allein durchführt. Warum das so ist und was unternommen werden muss, um DSGVO-konform zu arbeiten, ist im Folgenden erläutert.

a) Format der Datenbank

Es wird eine Microsoft Access 11.0 (2003) Datenbank (.mdb) verwendet. Verschlüsselt ist sie mit dem Administratorpasswort per RC4. Da einerseits das Verfahren unsicher ist und MS Access andererseits das Passwort im Dateiheader verschleiert ablegt, muss der Verein im Umgang mit der Datenbank besondere Vorsicht walten lassen.

Der Administrator darf als einziger Nutzer lokal arbeiten, da sich andere Nutzer über den Zugriff auf die Datenbank das Administratorkennwort erschleichen könnten und nicht mehr gewährleistet werden kann, dass ausschließlich Änderungen vom Administrator durchgeführt wurden (s.o. „2.1 Nutzerverwaltung“: Eindeutigkeit der Nutzer).

Nur der Administrator darf Zugriff auf den Bereich der lokalen Festplatte haben, in dem die Datenbank liegt.

b) Format der Datenaustauschdateien

Für den Fall das mehrere Nutzer lokal mit der Software arbeiten, bietet ComMusic die Möglichkeit die Daten per Datenaustausch zu synchronisieren. Die Datenaustauschdateien sind wie die Datenbank verschleiert.

Aus diesen Gründen ist ein Arbeiten mit Datenaustausch unter Berücksichtigung der DSGVO nicht mehr möglich. Mehrere Nutzer können nur auf einem Serverplatz DSGVO-konform arbeiten.

c) Format der Sicherungen

Die Datensicherungen sind ohne Passwort verschlüsselt und können von jedem Nutzer mit der Software entschlüsselt werden. Sie gelten deshalb nur als verschleiert und müssen vor dem Zugriff Unbefugter geschützt werden.

Im Serverbetrieb darf nur der Administrator die Berechtigung haben, Datensicherungen herunterzuladen und zu erstellen, da sich sonst andere Nutzer ebenfalls das Administratorkennwort aus der enthaltenen Datenbank erschleichen könnten und die Eindeutigkeit des Nutzers nicht mehr gegeben ist.

Die Datensicherungen auf den Servern sind mit AES-256 verschlüsselt.

d) Format der Ehrungs-, Melde- und Lehrgangsdateien

Die Ehrungs-, Melde- und Lehrgangsdateien sind lokal nur verschleiert und müssen wie die Sicherungen vor unberechtigtem Zugriff geschützt werden.

Im Serverbetrieb werden die Dateien mit AES-256 verschlüsselt gespeichert und nur der Verein und der adressierte Verband haben Zugriff darauf.

2.4) Informieren bei Datenpanne

Der Verein hat die Pflicht, die Aufsichtsbehörde zu informieren, wenn eine Verletzung der Sicherheit der personenbezogenen Daten stattfand, die dazu geführt hat, dass die Daten verändert, offengelegt oder vernichtet wurden bzw. verloren gegangen sind.

Die betroffenen Mitglieder müssen unterrichtet werden, wenn laut DSGVO „voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten“ für sie besteht und die Daten nicht durch technisch organisatorische Maßnahmen so gesichert waren, dass ein Missbrauch mit hoher Wahrscheinlichkeit ausgeschlossen werden kann.

2.5) Vertrag zur Auftragsverarbeitung

Der Verein muss mit jedem Dritten, der personenbezogene Daten der Mitglieder verarbeitet einen Vertrag zur Auftragsverarbeitung abschließen.

Falls der Verein einen Serververtrag hat oder die Meldung, Anträge oder Lehrgangsanmeldungen über den Server an seinen Verband schickt, muss ein Vertrag zur Auftragsdatenverarbeitung mit der Firma ComMusic - Frank Wieczorek e.K geschlossen werden. Der Vertrag zur Auftragsdatenverarbeitung kann in der Software unter „Sicherheit“ und „Auftragsverarbeitungsvertrag“ elektronisch abgeschlossen werden.

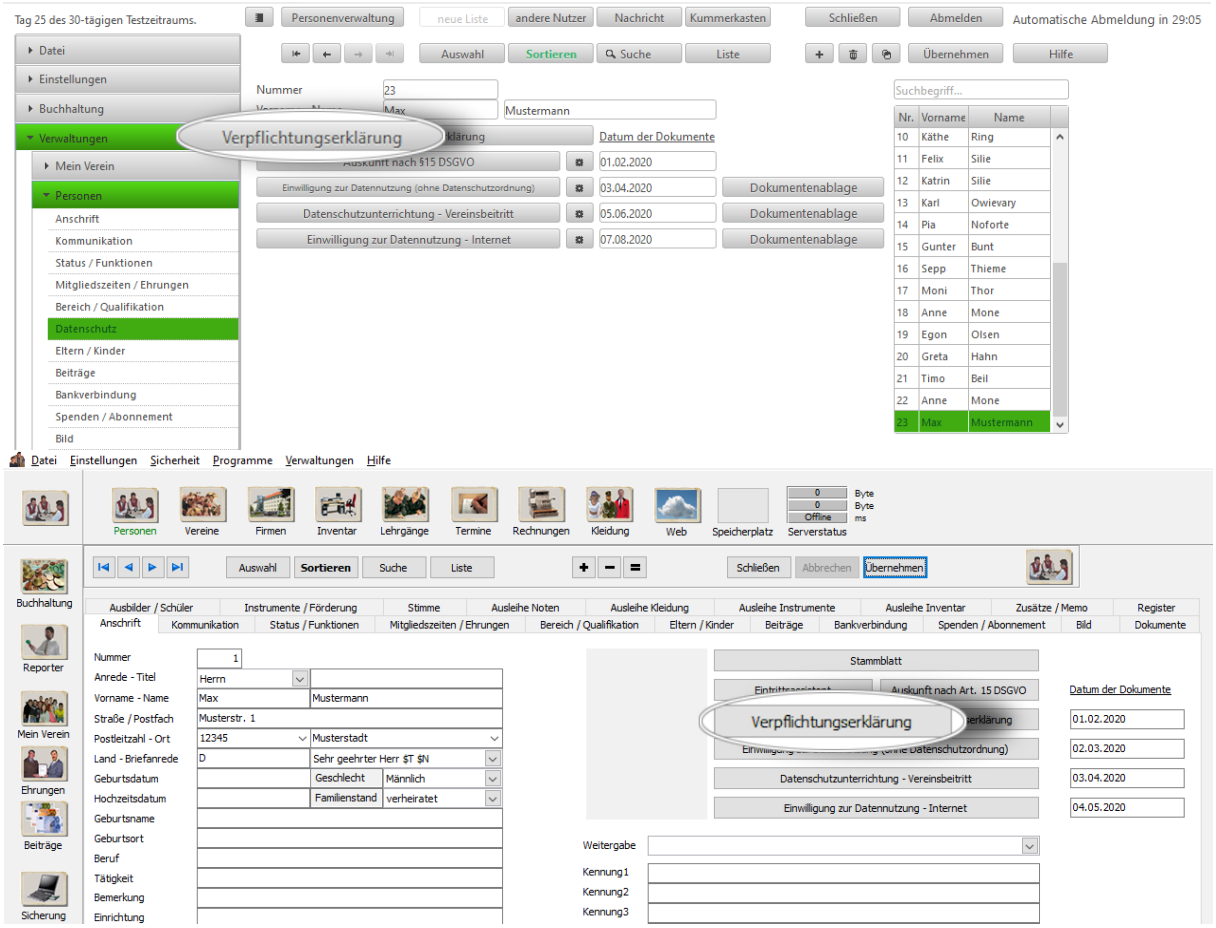
2.6) Verfahrensverzeichnis

Im Verein muss laut DSGVO ein Verfahrensverzeichnis geführt werden, in dem jede Verarbeitung von persönlichen Daten aufgeführt ist. Auch die mit der ComMusic-Software durchgeführten Tätigkeiten sind darin aufzuführen.

3) Pflichten aller Nutzer (inkl. Administrator)

3.1) Belehrung zum Datenschutz

Jeder Nutzer der Vereinsverwaltung muss eine Datenschutzbelehrung erhalten und unterschreiben. Dazu gibt es in der Personenverwaltung den Schalter [Verpflichtungserklärung] – im Vereinsprogramm unter Windows befindet er sich im Register „Anschrift“ bzw. in der Webanwendung im Register „Datenschutz“. Damit kann für jede Person im Verein ein entsprechendes Formular gedruckt werden. Die Vorlage für dieses Formular kann im Reporter ggf. an die Bedürfnisse des Vereins angepasst werden.



In der Personenverwaltung ist ein Dokument für die Belehrung zum Datenschutz vorbereitet

3.2) Grundsätze des Datenschutzes

Jeder Nutzer der Vereinsverwaltung muss sich bei der Verarbeitung von personenbezogenen Daten an die Grundsätze des Datenschutzes halten:

a) Rechtmäßigkeit

Daten dürfen nur rechtmäßig d.h. mit Einverständnis des Mitglieds erhoben werden. Es muss für jedes Vereinsmitglied nachvollziehbar sein, wie seine Daten verarbeitet werden.

b) Zweckbindung

Die personenbezogenen Daten dürfen nur so verarbeitet werden, wie es dem Zweck des Vereins entspricht und wie es dem Mitglied in der Satzung oder in einer Einverständniserklärung (s.u. „4.1 Einverständnis“) mitgeteilt wurde.

c) Datenminimierung

Daten dürfen nur in einem dem Zweck entsprechenden Umfang erhoben und verarbeitet werden. Wenn ein Verein beispielsweise die Bankdaten von Mitgliedern gespeichert hat, ohne diese für einen Beitragseinzug oder sonstige Geldtransfers zu nutzen, dann dienen diese Daten keinem Zweck und müssen gelöscht werden.

d) Richtigkeit und aktueller Stand

Mitglieder haben einen Anspruch darauf, dass ihre Daten korrekt und auf aktuellem Stand gespeichert und verarbeitet werden. Der Verein ist deshalb verpflichtet Aktualisierungen und Korrekturen unverzüglich durchzuführen.

4) Mit allen betroffenen Mitgliedern

4.1) Einverständnis

a) Datenschutzerklärung und Datenerhebung

Jedes Mitglied (bzw. eine erziehungsberechtigte Person) muss die Datenschutzordnung des Vereins, sowie sein eigenes Widerrufsrecht nachweislich zur Kenntnis nehmen und der Erhebung und Verarbeitung seiner Daten zustimmen. Das kann beim Abschluss des Mitgliedsvertrages geschehen, wenn die Datenschutzordnung des Vereins Teil der Vereinsatzung ist. Andernfalls muss eine gesonderte Einverständniserklärung abgeschlossen werden. Hierfür steht in Vereinssoftware, Webanwendung und im Verein24 light ein Dokument in der Personenverwaltung im Reiter „Anschrift“ als Schalter [Einwilligung zur Datennutzung (ohne Datenschutzordnung)] zur Verfügung.

Es ist stellenweise üblich Daten besonderer Kategorie, Ernährungsgewohnheiten/-unverträglichkeiten, Krankheiten und Allergien im Rahmen von Schulungen oder Lehrgängen zu verarbeiten, die in diese Kategorie fallen. Hierauf sollte schon beim Erstellen der Datenschutzordnung bzw. der Einverständniserklärung geachtet werden.

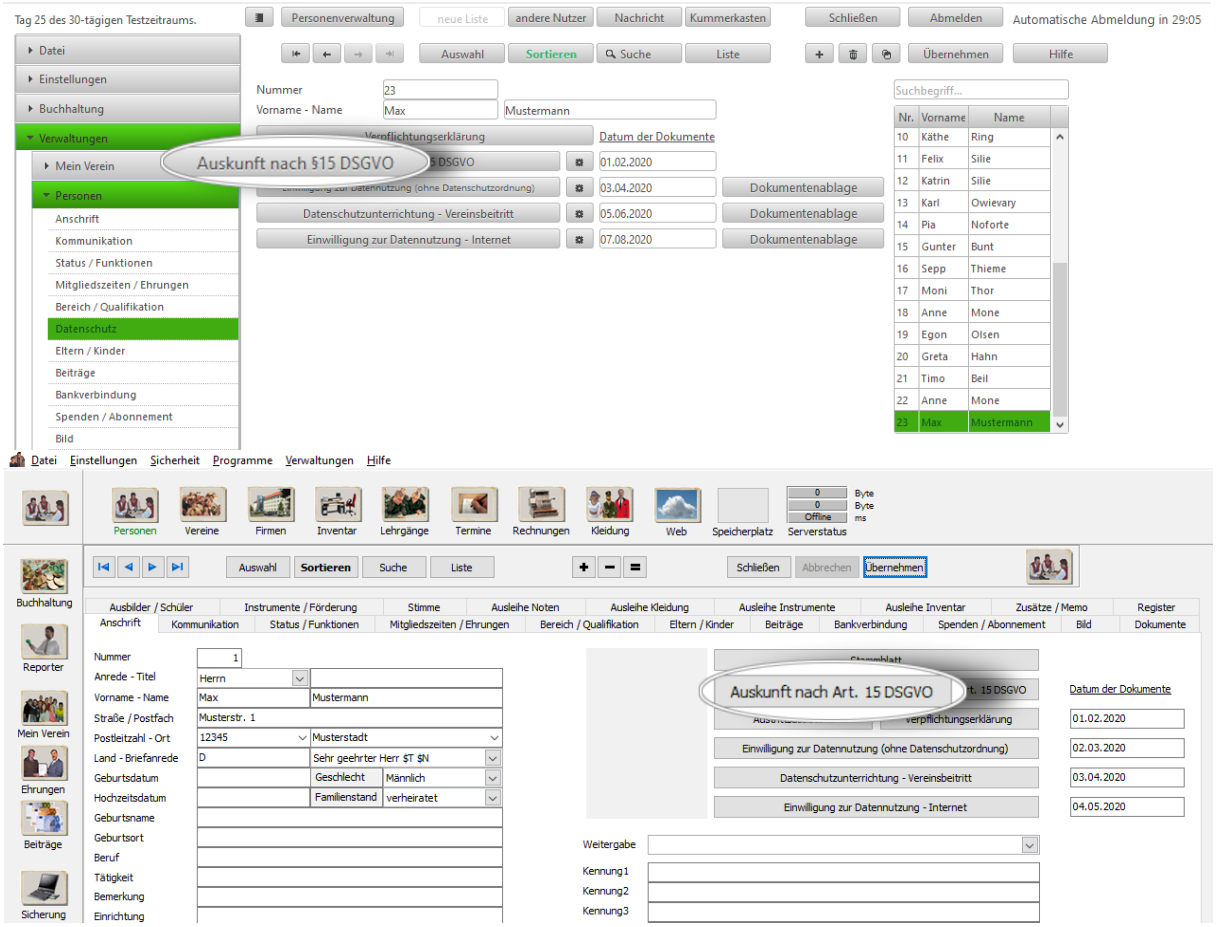
Bei Erhebung der Daten müssen dem Mitglied genaue Kontaktdaten vom Verantwortlichen, dessen Vertreters und ggf. des Datenschutzbeauftragten des Vereins genannt werden.

b) Weitergabe von Bildern (an Verband/Zeitungen/Homepage etc.)

Für die Weitergabe von Bildern in Ehrungsanträgen an den Verband, die (Verbands-)Zeitung oder für die vereinseigene Homepage ist eine gesonderte Einverständniserklärung des Mitglieds nötig. Dies kann nicht über die Datenschutzordnung des Vereins geregelt werden. Im Reiter „Anschrift“ der Personenverwaltung steht hierfür ebenfalls ein Dokument unter [Einwilligung zur Datennutzung - Internet] bereit.

4.2) Auskunftsrecht

Jedes Vereinsmitglied hat das Recht zu erfahren, welche Daten von ihm erfasst sind, wie sie verarbeitet und an wen sie weitergegeben werden. Die Auskunft muss unverzüglich – maximal einen Monat nach Antrag auf Auskunft – und kostenlos erfolgen.



Zur Auskunft nach Artikel 15 DSGVO gibt es ein Dokument mit allen persönlichen Daten eines Mitglieds

Zweck und Rechtsgrundlage der Verarbeitung müssen dem Mitglied offengelegt werden. Hier ist die „Verwaltung der Vereinsmitglieder“ zu nennen, ggf. die Pflicht im Verband (aktive) Mitglieder zu melden – auch um einen Versicherungsschutz zu sichern - die Verwaltung von Instrumenten, Kleidung, Noten und Inventar, das von Mitgliedern ausgeliehen wird, sowie der Bankeinzug von Beiträgen.

Wie lange die persönlichen Daten gespeichert werden, muss ebenfalls mitgeteilt werden. Das ist üblicherweise auf die Dauer der Mitgliedschaft beschränkt. Falls jedoch Rechnungen mit den persönlichen Daten des Mitglieds geschrieben wurden, verlängert sich der Zeitraum um 10 Jahre für die Rechnungsdaten nach der letzten Rechnung, da Rechnungen 10 Jahre für das Finanzamt aufgehoben werden müssen.

4.3) Recht auf Berichtigung

Mitglieder haben ein Recht darauf, dass Fehler in ihren Daten berichtigt und Änderungen unverzüglich übernommen werden.

4.4) Belehrung über Rechte

Jedes Mitglied muss darüber belehrt werden, dass es Auskunft über seine persönlichen Daten beim Verein verlangen darf, Anspruch auf die Berichtigung von Fehlern hat, die Einwilligung zur Nutzung seiner persönlichen Daten jederzeit widerrufen darf, die Daten auf Wunsch zu einem anderen Verein übertragen werden müssen und die Löschung der Daten verlangt werden kann.

4.5) Folgen der Nichtbereitstellung

Ein aktives Mitglied kann im Regelfall nur im Verein verbleiben bzw. beitreten, wenn es der Nutzung seiner Daten zustimmt. Falls das Mitglied nicht zustimmt oder widerruft, kann der Verein es nicht mehr verwalten, keine Beiträge einziehen, keine Ehrungen beantragen und Ausgeliehenes nicht eintragen. Außerdem kann das Mitglied nicht mehr an den Verband gemeldet werden und damit keinen Versicherungsschutz oder Förderung erhalten.

4.6) Protokollierung des Einverständnisses und der zur Kenntnisnahme

Das Einverständnis des Mitglieds und die zur Kenntnisnahme seiner Rechte muss festgehalten werden. Es gibt dazu entsprechende Vorlagen für die auszufüllenden Dokumente in der Personenverwaltung im Reiter „Anschrift“, falls die Datenschutzordnung nicht Teil der Vereinssatzung ist.

4.7) Erfasste Daten laut BDMV-Meldestandard

Im Rahmen der Meldung werden bestimmte Daten aus der ComMusic-Software an den übergeordneten Verband gemeldet. Eine genaue Liste aller übermittelten Informationen finden Sie hier:

https://www.commusic.de/hilfe/module_2_5_1.html