Überblick der Umsetzung der EU-Datenschutzgrundverordnung in Mitgliedsvereinen des Salzburger Blasmusikverbandes mit Fokus auf die Mitgliederdatenverwaltung

Version 19. 3. 2018

1 Einleitung

Alle Mitgliedsvereine des Salzburger Blasmusikverbandes benutzen zur Verwaltung ihrer Mitglieder die vernetzte Internet-Applikation **MuSys**.

Seitens des Salzburger Blasmusikverbandes wurden umfangreiche Maßnahmen ergriffen, damit dabei die Handhabung der personenbezogenen Daten gesetzeskonform, besonders im Hinblick auf die EU-Datenschutz Grundverordnung (DSGVO) vonstattengeht.

Dazu stehen Beschreibungen der Strukturen und Abläufe und Formulare zur Handhabung verschiedener Situationen zur Verfügung. Das gesamte Dokumentationsmaterial hierzu ist unter folgender Internetadresse abrufbar:

https://www.blasmusik-verband.at/datenschutz

Sämtliche dort zur Verfügung gestellte Materialien unterliegen einem Beschluss des Landesvorstandes des Salzburger Blasmusikverbandes und sind somit auch für die Mitgliedsvereine bindend.

In diesem Dokument wird im Besonderen auf die Mitgliederdatenverwaltung eingegangen. Es wird darauf hingewiesen, dass entsprechende Datenschutzmaßnahmen auch für die Handhabung von personenbezogenen Daten in anderen Bereichen (auch für analoge Datendarstellungen) anzuwenden sind!

Detaillierte Beschreibungen über die Datenanwendung und Datenweitergaben sind in folgenden mitgeltenden Dokumenten zu finden:

Dokumente: **Datenschutz-Salzburger Blasmusikverband**
Datenschutz-Österreichischer-Blasmusikverband
Datenschutzbestätigung-AKM-2013

2 Verantwortlichkeiten auf Musikvereinsebene

Die Letztverantwortung für die Erfassung und Handhabung der notwendigen Mitgliederdaten eines Musikvereins liegt beim Leitungsorgan (Obmann/Obfrau). Zur operativen Durchführung kann ein eigener Funktionär (z.B. EDV-Referent oder Schriftführer) eingesetzt werden oder vom Leitungsorgan eine oder mehrere Personen mit entsprechender technischer Ausstattung (Computer, Internetanbindung) delegiert werden.

3 Datenschutzrelevante Prozesse im Musikverein

3.1 Zugangsberechtigungen

Zum Zugriff auf die Daten eines Bereichs wurde dem Leitungsorgan jeweils eine Zugangsberechtigung vergeben, die übermittelt wurde. Mit diesem können Eingaben/Änderungen durchgeführt bzw. Daten eingesehen und ausgewertet werden. Mit dieser Berechtigung können weitere Zugangsberechtigungen erstellt werden, eingeschränkt (nur bestimmte Funktionalität) oder auch nicht.

Bei Anlage und Weitergabe einer neuen Zugangsberechtigung sind neue zugriffsberechtigte Personen auf die Aspekte des Datenschutzes hinzuweisen. **Nicht mehr benötigte Zugangsberechtigungen sind ehestmöglich wieder zu deaktivieren bzw. zu löschen.**

Es wird empfohlen, für alle Personen, die Zugang zu personenbezogenen Daten haben, sie auf die Aspekte des Datenschutzes zu unterweisen und eine Verpflichtung unterzeichnen zu lassen und im Verein abzulegen:

Formular: **Datenschutz-Verpflichtung**

3.2 Erfassung von Personenstammdaten

Üblicherweise werden bei Aufnahme eines neuen Mitglieds in den Verein personenbezogene Daten erfasst, oder auch später aktualisiert.

Das Gesetz sieht vor, dass eine Person, deren Daten verarbeitet werden sollen, explizit die Zustimmung dazu erteilen muss. Ansonsten ist die Verarbeitung nicht erlaubt, es sei denn die Datenverarbeitung basiert auf einer anderen vertraglichen Regelung, wie die Mitgliedschaft in einem Verein. Bei Datenerfassung ist die betroffene Person über die Dateninhalte, mögliche Verarbeitungsschritte, die geplanten Datenweitergaben und über die Rechte der Betroffenen transparent zu informieren.

Es wird empfohlen von betroffenen Personen eine schriftliche Einwilligungserklärung einzuholen. Bei Personen unter 14 Jahren ist diese Zustimmung seitens eines Erziehungsberechtigten notwendig. Das folgende Formular kann dazu verwendet werden. Es enthält auch alle notwendigen Informationen, die bei Datenverarbeitung weitergegeben werden sollten:

Formular: **Betroffener-Zustimmungserklärung**

Für Personen, deren Daten vor Inkrafttreten der DSGVO am 25. Mai 2018 erfasst wurden ist dies nicht zwingend notwendig, wenn sie zuvor (auch mündlich) über die Vorgänge informiert wurden. Es wird aber empfohlen solche Einwilligungserklärungen auch von solchen Personen nachzuholen.

3.3 Datenweitergabe und andere Datenanwendungen

Alle Datenweitergaben aus der Mitgliederverwaltung heraus sind sehr eingeschränkt und klar definiert (siehe aufgelistete Dokumente unter Abschnitt 1).

Werden seitens des Musikvereines darüber hinaus personenbezogene an weitere Empfänger weitergegeben oder auch andere Datenanwendungen verwendet, so wird die Dokumentation dieser Schritte dringend empfohlen:

Formular: **Personendaten-Verarbeitung-Liste**

Es wird darauf hingewiesen, dass Veröffentlichungen von Daten auch Weitergaben darstellen, die der Zustimmung der Betroffenen bedürfen. Für das Anzeigen von Kontaktdaten (von Funktionären) auf Homepages ist eine gesonderte Autorisierung der Betroffenen einzuholen (in der Anwendung MuSys kann bei jeder Person genau gesteuert werden, welche Kontaktdaten auf der Homepage des Salzburger Blasmusikverbandes angezeigt werden). Laut Gesetz ist eine

mündliche Zustimmung ausreichend. Eine schriftliche Zustimmungserklärung wird jedoch empfohlen.

Auf ähnliche Sorgfalt bei der Veröffentlichung personenbezogener Daten wird für andere Vorgänge, wie Namenslisten auf Konzertprogrammen oder diverse Berichte in Medien, hingewiesen.

3.4 Sicherstellung der Rechte Betroffener

3.4.1 Anfrage um Auskunft

Im Falle einer Auskunftsanfrage einer betroffenen Person hat der Verantwortliche für die Datenverarbeitung gemäß DSGVO binnen einer Frist eines Monats die Antwort zu übermitteln.

Es wird die Verwendung des folgenden Formulars empfohlen, welches gemeinsam mit einem Ausdruck des Personendatenstammblattes aus MuSys übermittelt wird. Bei Verwendung weiterer Datenanwendungen oder Ablage analoger Datenbestände sind diese ebenfalls zu berichten:

Formular: **Betroffener-Auskunftserteilung**

3.4.2 Anfrage auf Datenberichtigung, auf Datenlöschung oder Einschränkung der Datenverarbeitung

Im Falle einer Anfrage auf Datenberichtigung, auf Datenlöschung oder auf Einschränkung der Datenverarbeitung ist das gemäß DSGVO binnen Frist eines Monats zu erledigen.

Es wird die Verwendung des folgenden Formulars empfohlen, welches auch entsprechende Hinweise auf detaillierte notwendige Maßnahmen enthält. Es wird zusätzlich empfohlen in solchen Anfragefällen den Landesverband zu kontaktieren!

Formular: **Betroffener-Rechteumsetzung**

3.4.3 Anfrage auf Übertragung der Daten

Ein Betroffener hat das Recht seine Daten in einem maschinenlesbaren allgemeinen Format übertragen zu lassen.

Dieser Prozess wird in der Anwendung MuSys insofern unterstützt, indem man das Personendatenstammblatt der Person im PDF-Format ausgibt und diese Datei weitertransportiert.

3.5 Meldepflicht bei Datenschutzverletzungen

Wird eine Datenschutzverletzung festgestellt (Datenverlust, unberechtigter Zugriff, Datenveränderung, Datenzerstörung, etc.) so sieht die DSGVO eine verpflichtende Meldung an die Aufsichtsbehörde vor.

Der Verantwortliche hat schnellstmöglich geeignete Maßnahmen in die Wege zu leiten. Die Meldung an die Aufsichtsbehörde muss möglichst binnen 72 Stunden nachdem dem Verantwortlichen die Verletzung bekannt wurde, erfolgen. Bei Verzögerung ist dies zu begründen. Zusätzlich ist eine Benachrichtigung der betroffenen Person(en) vorgesehen. Es wird die gesamte Abhandlung laut folgendem Formular empfohlen:

Formular: **Datenschutzverletzung-Abhandlung**

4 Sicherheit

Der Salzburger Blasmusikverband trifft für die Serveranwendung technische und organisatorische Sicherheitsmaßnahmen, um die personenbezogenen Daten gegen unbeabsichtigte oder unrechtmäßige Löschung, Veränderung oder gegen Verlust und gegen unberechtigten Zugriff zu schützen. Dabei werden Mittel nach dem aktuellen technischen Stand und gemäß der wirtschaftlichen Vertretbarkeit eingesetzt um das Datenmaterial zu schützen.

Es wird sehr stark empfohlen auf eine entsprechende **Sicherheit des Arbeitsplatzes (Vereins-arbeitsplatz)** zu sorgen, damit auf diesem Wege keine unberechtigten Datenzugriffe oder gar Datenveränderungen zustande kommen können.

Folgende Richtlinien sollen dabei mitbeachtet werden:

- Verwendung sicherer Kennwörter (mindestens 8 Zeichen, gemischt Groß-/Kleinschreibung, Ziffern, Sonderzeichen
- Geschützte Datenzugänge, auch physisch (versperrte Räume)
- Regelmäßige Datensicherungen durchführen (Ablage an anderen geschützten Orten)
- Administrative Vorgänge protokollieren und nicht jeden Benutzer Administratorrechte zugestehen
- Betriebssystem und Software aktuell halten (laufend Updates einspielen)
- Virenschutz, Firewall und andere Sicherheitssoftware aktuell halten
- Richtlinien für Email, private Verwendung usw. definieren (Erkennen von Phishing-Mails, SPAM etc.: Benutzer dafür sensibilisieren)
- Auch Papierdokumente sorgfältig verwahren, handhaben und bei Bedarf sorgfältig vernichten
- Keine Besucher auf Vereinscomputer zulassen
- Nur personenbezogene Daten ansehen, wenn unbedingt notwendig
- Keine unkontrollierte Speicherung von personenbezogenen Daten (z.B. auf USB-Sticks)
- Übermittlung von Daten nur verschlüsselt und bei genau definierten Zwecken (Bestätigung vom Empfänger notwendig)

5 Weitere Hinweise

Es wird darauf hingewiesen, dass die Anwender der Softwarelösung, sowie auch die Verantwortlichen des jeweiligen Bereiches (Obleute) für eine unrechtmäßige Weitergabe von personenbezogenen Daten haftbar gemacht werden können.

Datenanwendungen sind Arbeitsabläufe und ihre Daten und keine Computerprogramme, das bedeutet, dass personenbezogene Daten für einen gewissen Zweck verarbeitet werden. D.h., dass alle Maßnahmen laut DSGVO nicht nur für elektronische Daten gelten, sondern für sämtliche Unterlagen, die personenbezogene Daten enthalten. Daher ist darauf hinzuweisen, dass die Sorgfalts- und Geheimhaltungspflicht im Umgang mit personenbezogenen Daten ebenso außerhalb der Anwendung MuSys zu beachten ist (z.B. für ausgedruckte Datensätze oder andere Personenlisten).