Auftrag zur Datenverarbeitung gemäß Art. 28 DS GVO

VEREINBARUNG

zwischen

Verein: _____

Straße: _____

Ort: _____

- nachstehend Auftraggeber genannt -

und

Musikbund von Ober und Niederbayern
Sandstraße 31
80335 München

- nachstehend Auftragnehmer genannt -

1. Gegenstand und Dauer des Auftrages

1.1 Gegenstand des Auftrags

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

- Verwaltung der Vereins- und Mitgliederdaten in der MON-Verwaltungssoftware
- Abschluss von Rahmenverträgen (z.B. GEMA, Versicherung, Künstlersozialkasse)
- Beantragung von staatlichen Zuschüssen (z.B. Wissenschaftsministerium)
- Abwicklung von Junior- und Musikerleistungsabzeichenprüfungen
- Abwicklung von Ehrungen
- Berechnung von Mitgliedsbeiträgen

1.2 Dauer des Auftrags

Der Auftrag wird unbefristet erteilt.

2. Auftragsinhalte

2.1 Umfang, Art und Zweck

Verwaltung der Vereins- und Mitgliederdaten in der MON-Verwaltungssoftware, Abschluss von Rahmenverträgen und Auswertung zur Beantragung von Zuschüssen und Erstellung der Beitragsrechnungen. Dafür ist auch eine Weitergabe von Daten an Dachverbände (z.B. Bayerischer Blasmusikverband und Bundesvereinigung deutscher Musikverbände) notwendig.

Die Verarbeitung sowie Nutzung der Daten durch den Auftragnehmer findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland statt. Jede Verlagerung der Datenverarbeitung oder Nutzung in ein Drittland bedarf der Zustimmung des Auftraggebers und darf nur erfolgen, sofern die Vorgaben in Art 44 zutreffen.

2.2 Art der Daten

Gegenstand der Speicherung, Verarbeitung und Nutzung personenbezogener Daten sind folgende Datenarten und Kategorien: Sämtliche Vereins- und Mitgliederdaten, die mit der Vereinsverwaltungssoftware gespeichert und genutzt werden.

2.3 Kreis der Betroffenen

Betroffen sind durch die Speicherung, Verarbeitung und Nutzung sämtliche in der Vereinssoftware angelegten Vereine und deren Mitglieder

3. Technisch-organisatorische Maßnahmen

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.
Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen. Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.
Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

Die zu treffenden

3.1 nicht auftragsspezifischen Maßnahmen betreffen die Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, das Trennungsgebot […].
Siehe hierzu Anlage: „Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen“

3.2 auftragsspezifischen Maßnahmen betreffen die Art des Datenaustausches, Bereitstellung der Daten, Art und Umstände der Datenverarbeitung, Datenhaltung, Umstände beim Output und Datenversand […].
Siehe hierzu Anlage; „Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen“

Zur regelmäßigen Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen hat der Auftragnehmer mit Florian Bauer (florian.bauer@mon-online.de) einen IT-Sicherheitsbeauftragten ernannt.

4. Berichtigung, Löschung und Sperrung

Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Unterauftragsverhältnisse

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Für die Programmier- und Wartungsarbeiten hat der Auftragnehmer einen Vertrag zur Auftragsdatenverarbeitung mit der Fa. edvhauck GmbH abgeschlossen.
Für die Auftragsdatenverarbeitung durch die MON-Bezirksverbände wurden ebenfalls Verträge zur Auftragsdatenverarbeitung geschlossen.

Der Auftragnehmer darf weitere Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

6. Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

7. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer ist verpflichtet, dem Auftraggeber umgehend und vollumfänglich Meldung zu erstatten, wenn es durch ihn oder eine bei ihm beschäftigte Person Verstöße gegen den Datenschutz gab bzw. dem Auftragnehmer solche zur Kenntnis gelangten.

8. Weisungsbefugnis des Auftraggebers

Der Datenumgang erfolgt ausschließlich im Rahmen der hier getroffenen Vereinbarungen und entsprechend der Weisung des Auftraggebers. Unabhängig von dieser Vereinbarung behält sich der Auftraggeber ein umfassendes Weisungsrecht vor. Veränderungen bezüglich des Gegenstandes und der Verarbeitungsverfahren bedürfen der einvernehmlichen Abstimmung. Vertreter des Auftraggebers ist der jeweilige im Vereinsregister eingetragene Vorsitzende bzw. sein Stellvertreter.

Weisungen des Auftraggebers werden dem Auftragnehmer stets in schriftlicher Form erteilt (E-Mail, Fax, Brief usw.). Mündliche Weisungen werden umgehend verschriftlicht. Es bedarf der umgehenden Mitteilung durch den Auftragnehmer, wenn dieser annimmt, dass die erfolgte Weisung gegen datenschutzrechtliche Bestimmungen verstößt.

Der Auftragnehmer verwendet die Daten zu keinem anderen Zweck und ist auch nicht zur Weitergabe von Daten, die Gegenstand dieses Auftrages sind, an Dritte berechtigt.

9. Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.
Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.
Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz Herr Otto Steinberger (datenschutz@mon-online.de) bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

10. Löschung von Daten

Ist der Auftrag erledigt bzw. endet das Mitgliedschaftsverhältnis im MON, hat der Auftragnehmer sämtliche Daten zu löschen, sofern es keine anderweitigen Aufbewahrungspflichten gibt, z.B.

- 5 Jahre Nachweispflicht gegenüber dem Freistaat Bayern bzw. dem Bayerischen Obersten Rechnungshof hinsichtlich der Zuschussgewährung
- 10 Jahre buchhalterische Aufbewahrungspflicht.

Ein entsprechendes Protokoll ist dem Auftraggeber auf Wunsch auszuhändigen.

11. Sonstiges / Salvatorische Klausel

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Ort, Datum: _____

_____

[Unterschrift Auftraggeber]

Ort, Datum: _____

_____

[Unterschrift Auftragnehmer]

Anlage: Dokumentation Datenschutz und Datensicherheit durch Technik & Organisation

Allgemein:
Aktueller Virenscanner/Sicherheitssoftware
Automatische Updates im Betriebssystem
Automatische Updates des Browsers
Permanente Datensicherung und Versionenverlauf über Dropbox
Alle Server (auch Cloudspeicher) auf Servern in EU
Papieraktenvernichtung mit Shredder
Regelmäßige Schulungen der haupt- und ehrenamtlichen Mitglieder
Verschlüsselung der LapTops, die im Einsatz außerhalb der Geschäftsstelle sind
Personalakten befinden sich in einem Tresor

Software zur Mitgliederverwaltung:
Abgeschichtete Rechte in der Mitgliederverwaltung / Individuelle Zugangsdaten und damit verbundene Rechte / Jeder sieht nur, was er bruahct (Minimalprinzip)
Zugriff nur über Remotedesktop (keine Homepage)
Zweistufige Anmeldung (Remote-Desktop / Software)
Klare Trennung von Daten und Anwendung (Client-Server-Model; SQL-Datenbank und Software)
Kein Zugriff auf das Server-Datensystem, sondern ausschließlich auf die MON-Software
Kein Zugriff für externe Auswerter oder Firmen, die nicht speziell berechtigt sind
Laufend verbesserte, nach eigenen Vorgaben programmierte Software
Zugriff-gesichert durch Hardware- und Software-Firewall
Datensicherungkonzept, um Datenverlust zu durch technische Schäden zu vermeiden
Speicherung der Daten auf eigenen Servern
Regelmäßige Wartungsintervalle, in dem alle Sicherheitspatches installiert werden
Server auf dem Stand der Technik
Datensicherheitsbeauftragter überwacht die Prozesse