**Bei dem nachfolgenden Dokument handelt es sich nur um ein Muster. Ob und inwieweit die Inhalte des Dokuments auf die jeweiligen datenschutzrechtlichen Pflichten des MUSIKVEREINS passen, kann vom Autor ohne weitere Kenntnis der Sachlage nicht eingeschätzt werden. Der Autor übernimmt weder eine Garantie für die Korrektheit der Inhalte noch für individuelle die Anwendbarkeit für die vom MUSIKVEREIN vorgesehenen datenschutzrechtlichen Prozesse.**

Technische und organisatorische Maßnahmen des Auftragnehmers gemäß Art. 25 DS-GVO

**Hinweis** (kann nach vollständiger Angabe der Maßnahmen gelöscht werden)**:** Bitte geben Sie nachfolgend jeweils die getroffenen technischen und organisatorischen Maßnahmen an. Als Unterstützung sind hier bestimmte typische Begriffe als Hilfe und Veranschaulichung angeführt.

Bei einzelnen Maßnahmen kann eine stichwortartige Benennung oder auch nur ein Wort (z.B. „Alarmanlage“) ausreichend sein. Bei anderen Maßnahmen sollte jedoch regelmäßig eine kurze Beschreibung erfolgen, die eine Bewertung durch den Auftraggeber ermöglicht (Beispiel: Im Falle einer Videoüberwachung als Maßnahme der Zutrittskontrolle wäre es erforderlich, zu beschreiben, ob z.B. nur die Eingangstür oder auch andere Gebäudeteile überwacht werden und ob eine Aufzeichnung der Aufnahmen erfolgt). Auch bei einer Maßnahme wie einer „Passwortvergabe“ ist konkret aufzuführen, ob es eine Mindestpasswortlänge und –komplexität gibt und wie Passwortlänge und Komplexität ausgestaltet sind. Außerdem wäre zudem anzugeben, ob die Mindestpasswortlänge und –komplexität technisch erzwungen wird.

# Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

# Zutrittskontrolle

*Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.*

Typische Maßnahmen (nur Stichworte) sind z.B.:

* Alarmanlage
* Absicherung von Gebäudeschächten
* Automatisches Zugangskontrollsystem
* Chipkarten-/Transponder-Schließsystem
* Schließsystem mit Codesperre
* Manuelles Schließsystem
* Biometrische Zugangssperren
* Videoüberwachung der Zugänge
* Lichtschranken / Bewegungsmelder
* Sicherheitsschlösser
* Schlüsselregelung (Schlüsselausgabe etc.)
* Personenkontrolle beim Pförtner / Empfang
* Protokollierung der Besucher
* Sorgfältige Auswahl von Reinigungspersonal
* Sorgfältige Auswahl von Wachpersonal
* Tragepflicht von Berechtigungsausweisen

# Zugangskontrolle

*Maßnahmen, die geeignet sind* *zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.*

Typische Maßnahmen (nur Stichworte) sind z.B.:

* Zuordnung von Benutzerrechten
* Erstellen von Benutzerprofilen
* Passwortvergabe
* Authentifikation mit biometrischen Verfahren
* Authentifikation mit Benutzername / Passwort
* Zuordnung von Benutzerprofilen zu IT-Systemen
* Gehäuseverriegelungen
* Einsatz von VPN-Technologie
* Sperren von externen Schnittstellen (USB etc.)
* Sicherheitsschlösser
* Schlüsselregelung (Schlüsselausgabe etc.)
* Verschlüsselung von mobilen Datenträgern
* Verschlüsselung von Smartphone-Inhalten
* Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
* Einsatz von Anti-Viren-Software
* Verschlüsselung von Datenträgern in Laptops / Notebooks
* Einsatz einer Hardware-Firewall
* Einsatz einer Software-Firewall

# Zugriffskontrolle

*Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.*

Typische Maßnahmen (nur Stichworte) sind z.B.:

* Erstellen eines Berechtigungskonzepts (Need to know-Prinzip)
* Verwaltung der Rechte durch Systemadministrator
* Anzahl der Administratoren auf das „Notwendigste“ reduziert
* Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
* Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
* Sichere Aufbewahrung von Datenträgern
* physische Löschung von Datenträgern vor Wiederverwendung
* ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
* Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
* Protokollierung der Vernichtung
* Verschlüsselung von Datenträgern

# Trennungskontrolle

*Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.*

Typische Maßnahmen (nur Stichworte) sind z.B.:

* physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
* Logische Mandantentrennung (softwareseitig)
* Erstellung eines Berechtigungskonzepts
* Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
* Versehen der Datensätze mit Zweckattributen/Datenfeldern
* Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
* Festlegung von Datenbankrechten
* Trennung von Produktiv- und Testsystem

# Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

# Weitergabekontrolle

*Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.*

Typische Maßnahmen (nur Stichworte) sind z.B.:

* Einrichtungen von Standleitungen bzw. VPN-Tunneln
* Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
* E-Mail-Verschlüsselung
* Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
* Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
* Beim physischen Transport: sichere Transportbehälter/-verpackungen
* Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen

# Eingabekontrolle

*Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.*

Typische Maßnahmen (nur Stichworte) sind z.B.:

* Protokollierung der Eingabe, Änderung und Löschung von Daten
* Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
* Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
* Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
* Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

# Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

# Verfügbarkeitskontrolle

*Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.*

Typische Maßnahmen (nur Stichworte) sind z.B.:

* Unterbrechungsfreie Stromversorgung (USV)
* Klimaanlage in Serverräumen
* Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
* Schutzsteckdosenleisten in Serverräumen
* Feuer- und Rauchmeldeanlagen
* Feuerlöschgeräte in Serverräumen
* Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
* Erstellen eines Backup- & Recoverykonzepts
* Testen von Datenwiederherstellung
* Erstellen eines Notfallplans
* Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
* Serverräume nicht unter sanitären Anlagen
* In Hochwassergebieten: Serverräume über der Wassergrenze

# Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

# Datenschutz-Managementsystem

*Ein System, welches an zentraler Stelle den gesamten Datenschutzprozess steuert und abbildet*

# Incident-Response-Management

*Maßnahmen zum Umgang mit Störungen und bei Datenverlust*

# Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

*Maßnahme, die eine aktive Reduzierung der zu erfassenden Daten ermöglichen. Bei Auswahlfelder ist immer eine benutzerfreundliche Voreinstellung zu wählen.*

# Auftragskontrolle

*Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.*

Typische Maßnahmen (nur Stichworte) sind z.B.:

* Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
* vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
* schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG
* Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)
* Auftragnehmer hat Datenschutzbeauftragten bestellt
* Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
* Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
* laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
* Vertragsstrafen bei Verstößen