Anhang 2 - Technische und organisatorische Maßnahmen von ComMusic nach DSGVO (Art. 28 Abs. 3)

1) Vertraulichkeit (Art. 32 Abs. 1 Buchst. b) DSGVO)

1.1) Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren:

- Manuelles Schließsystem
- Videoüberwachung der Räumlichkeiten außerhalb der Betriebszeiten
- Server und wichtige NAS-Geräte befinden sich in einem Datentresor
- Alle integrierten Festplatten und Daten auf NAS-Geräten sind verschlüsselt
- Reinigungspersonal hat nur Zutritt zu Räumlichkeiten, wenn ein Mitarbeiter der Firma ComMusic anwesend ist
- Begleitung von Besuchern und Fremdpersonal

1.2) Zugangskontrolle

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

- Zuordnung von Benutzerrechten
- Zugangsschutz - Authentifikation mit Benutzername und Passwort
- strenge Passwortrichtlinie
- Datenträger der NAS sind AES-256 verschlüsselt
- Automatische und manuelle Zugangssperren
- USB- und CD-Boot auf den PCs gesperrt
- BIOS Passwörter gesetzt
- Einsatz von Anti-Viren-Software
- Getrennte Netzwerke (WLAN, LAN, IoT, VPN)

1.3) Zugriffskontrolle

Maßnahmen, die geeignet sind, zu 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:

- Umsetzung der Zugriffsbeschränkungen
- Benutzerverwaltung mit mehrstufigem Zugriffsberechtigungssystem
- Der Zugriff auf die Datenbanken und Verzeichnisstrukturen wird von den Servern protokolliert
- Unberechtigter Zugriff wird automatisch gemeldet
- Nutzer, die auf Daten zugreifen, zu denen Sie keine Berechtigung haben, werden automatisch gesperrt

1.4) Trennungskontrolle

Maßnahmen, die geeignet sind zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Logische Mandantentrennung (softwareseitig), jeder Kunde hat seine eigene Datenbank
- Erstellung eines Berechtigungskonzepts
- Festlegung von Datenbankrechten

2) **Integrität (Art. 32 Abs. 1 Buchst. b) DSGVO)**

2.1) Weitergabekontrolle

Maßnahmen, die geeignet sind, zu 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 einer Übermittlung personenbezogener Daten durch Einrichtung zur Datenübertragung vorgesehen ist:

- Zugriff auf Server ausschließlich per VPN-Tunnel
- Zugriff auf Datenbanken per Software RSA2048/AES-256-Verschlüsselt
- Passworte werden gesalzen und sind SHA-512 gehasht
- Zugriff über Webseite erfolgt SSL-Verschlüsselt mit erweiterten Zertifikaten

2.2) Eingabekontrolle

Maßnahmen, die geeignet sind, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Eingaben, Änderungen und Löschvorgänge von Benutzern werden mit dem betroffenen Datensatz und der Nutzerkennung protokolliert

3) **Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 Buchst. b) DSGVO)**

3.1) Verfügbarkeitskontrolle

Maßnahmen, die geeignet sind, zu gewährleisten, dass personenbezogene Daten gegen zufällige oder mutwillige Zerstörung oder Verlust geschützt sind:

- Server laufen mit RAID 1 System aus 2 Festplatten
- Festplatten-Status wird kontrolliert
- Datensicherungen werden auf alle Server gespiegelt
- Datensicherungen sind zusätzlich am Standort der Firma ComMusic auf einem RAID 1 System aus 4 Festplatten gesichert
- Server werden 1x je Minute von 2 Standorten auf Erreichbarkeit überprüft
- Server stehen im Rechenzentrum der Strato AG
- folgende Maßnahmen wurden durch die Strato AG getroffen:
    - Vorhandensein und Umsetzung eines Konzeptes zur Durchführung von regelmäßigen Datensicherungen
    - Vorhandensein und regelmäßige Prüfung von Notstromaggregaten und Überspannungsschutzeinrichtungen
    - Überwachung der Betriebsparameter von Rechenzentren
    - Vorhandensein eines Notfallkonzeptes
    - Regelungen zur Aufnahme eines Krisen bzw. Notfallmanagements

3.2) Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 Buchst. c DSGVO)

Maßnahmen, die geeignet sind, zu gewährleisten, dass die Wiederherstellbarkeit sichergestellt ist:

- Unsere Backupsysteme sind so aufgebaut, dass eine Wiederherstellung beschädigter oder defekter Systeme innerhalb kurzer Zeit möglich ist.

4) Verfahren zur regelmäßigen eigenen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 Buchst. d) DSGVO; Art. 25 Abs. 1 DSGVO)

4.1) Datenschutz-Management

Die Firma ComMusic betreibt ein eigenes Datenschutzmanagementsystem (DSMS), in das alle Mitarbeiter und die Geschäftsführung einbezogen sind.

Das Datenschutz-Management wird einmal jährlich und bei Bedarf auch zusätzlich überprüft. Bedarf kann durch eine Gesetzesänderung, neue technische Anforderungen oder den Eintritt eines Datenschutz-Vorfalls entstehen.

4.2) Incident-Response-Management (Vorfallreaktionsplan)

Für Hardwareausfälle und Datenpannen existiert ein Vorfallreaktionsplan, nach dem datenschutzkonform gehandelt werden kann.

4.3) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Bei allen Produkten von ComMusic werden datenschutzfreundliche Voreinstellungen („privacy-by-default“) verwendet.

4.4) Auftragskontrolle

Maßnahmen, die geeignet sind, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- Verpflichtung der Mitarbeiter von ComMusic auf das Datengeheimnis
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Weisungen werden nur durch weisungsbefugte Personen entgegengenommen
- Ob eine Person weisungsbefugt ist, wird bei Anfragen und Aufträgen überprüft
- Änderungen an den Befugnissen werden vorab geprüft und sind in den AGB geregelt