Datensicherheitskonzept nach DSGVO/BDSG für Verantwortliche im Sinne DSGVO, Vorstandsmitglieder und Funktionsträger des Dance Club Markdorf e.V.

(Stand 20.04.2018)

Daten, die im Rahmen einer Vereinstätigkeit erhoben, verarbeitet oder genutzt werden, werden im Folgenden „Daten“ genannt. Verantwortliche im Sinne DSGVO werden nachfolgend „Verantwortliche“ genannt.

Jeder Verantwortliche des Vereins ist verpflichtet, durch geeignete und angemessene technische und organisatorische Maßnahmen dafür zu sorgen, dass Daten unbefugten Dritten weder auf den von ihm benutzten noch fremden Rechnern oder sonstigen DV-Systemen zugänglich sind, insbesondere auch nicht Familienangehörigen oder Besuchern. Dies gilt auch und gerade, soweit die Vereinstätigkeit in den eigenen häuslichen Räumlichkeiten durchgeführt wird.

1.) Standardmaßnahmen

Nachfolgende, etablierte IT-Standardmaßnahmen sind zu einzuhalten, um die Daten effektiv zu schützen.

- Aktuelles Betriebssystem verwenden. (Im Zweifelsfall einen IT-Sachkundigen zu Rate ziehen)
- Automatische Updates im Betriebssystem aktivieren (insbesondere Sicherheitsupdates)
- Separaten Benutzer mit separatem Passwort für die Vereinstätigkeiten einrichten
- Automatische Updates des Browsers aktivieren (insbesondere Sicherheitsupdates)
- Backups regelmäßig, z.B. einmal monatlich auf externen crypto USB-Stick mit automatischer Verschlüsselung, siehe Kapitel 2.)
- Aktueller Virenscanner/Sicherheitssoftware

2.) Externe, beziehungsweise leicht bewegliche Datenträger und Dateisysteme

- Externe, leicht bewegliche Datenträger beziehungsweise Dateisysteme, wie z.B. USB-Sticks/Festplatten oder CD/DVD/BD-ROM, auf denen Daten gespeichert sind, sind gemäß einem
  - AES (Advanced Encryption Standard), beziehungsweise einem
  - FIPS 197 (Federal Information Processing Standard)

  zu verschlüsseln und damit sicher vor dem unbefugten Zugriff Dritter zu schützen. Insbesondere auch vor Familienangehörigen oder Besuchern, soweit die Vereinstätigkeit in den eigenen häuslichen Räumlichkeiten durchgeführt wird.
- Dazu bieten sich sogenannte ‚crypto‘ USB-Sticks mit automatischer Verschlüsselung, oder verschlüsselte virtuelle Laufwerke (Multiplatform Open Source Software: „VeraCrypt“, „TrueCrypt 7.1a“) an.
- Beendet ein Verantwortlicher seine Tätigkeit für den Verein, so ist von dessen Nachfolger oder vom Vereinsvorsitzenden ein neuer Schlüssel hierfür zu generieren.

3.) Transport der Daten, Schutz vor Verlust oder Diebstahl von externen, leicht beweglichen Datenträgern

- Daten, sind ausschließlich auf einem verschlüsselten Datenträger zu transportieren. Siehe dazu Kapitel 2.).
- Daten dürfen zwischen den Verantwortlichen ausschließlich auf verschlüsselten Datenträgern (Kapitel 2.) oder verschlüsselt (Kapitel 2.) per E-Mail oder file share ausgetauscht werden.

4.) Vernichtung von elektronischen Daten

- Ein einfaches Löschen von ganzen Dateien oder Verzeichnissen reicht nicht aus. Daten oder Verzeichnisse sind durch einen sogenannten „Datei-Shredder“ zu vernichten, die Daten mindestens nach einem der Verfahren
  - Gutmann, US Dod 522022-M, PseudorandomData

  sicher unbrauchbar machen.
  Dazu bietet sich verschiedene Open Source Software, zum Beispiel „Eraser“ an.

5.) Papieraktenvernichtung

- Papierakten sind mit einem Standard-Shredder oder durch thermische Behandlung (zu Asche verbrennen) zu vernichten.

6.) Inkrafttreten

Dieses Datensicherheitskonzept tritt ab dem 20.04.2018 in Kraft