Datenschutz - die Mindestsicherheitsmaßnahmen

Für die Mitgliedsvereine im Südtiroler Theaterverband

1. Allgemeines
Das vorliegende **Promemoria** beinhaltet u.a. die Mindestsicherheitsmaßnahmen zum Datenschutz, die von allen Mitgliedsbühnen im Südtiroler Theaterverband einzuhalten sind: Wer die Mindestsicherheitsmaßnahmen nicht einhält, kann strafrechtlich belangt werden.

Es muss vorausgeschickt werden, dass die Mitgliedsbühnen im Südtiroler Theaterverband als eigenständige Vereine und Organisationen gegründet sind und daher für die Einhaltung aller gesetzlichen Bestimmungen[1] -auch jener zum Datenschutz - eigenverantwortlich sind.

Des Weiteren wird vorausgeschickt, dass die Mitgliedsbühnen keine sensiblen Daten benötigen, bzw. verarbeiten sollen, damit die zusätzlichen (restriktiven) Auflagen, welche nur die sensiblen Daten betreffen, nicht einhalten müssen.

2. Begriffsbestimmung
a) **Als personenbezogene Daten gelten** alle Informationen über natürliche (physische) und juristische Personen (gewerbliche und nicht gewerbliche Körperschaften).

b) **Unter der Verarbeitung personenbezogener Daten versteht** man alle, mit oder ohne Hilfe der EDV durchgeführte Arbeitsvorgänge, betreffend:

- das Erheben der Daten,
- das Speichern und Aufbewahren der Daten,
- das Modifizieren und Verändern der Daten,
- die Benützung der Daten,
- die Bereitstellung oder Weitergabe der Daten,
- das Löschen und Vernichten der Daten.

c) **Als sensible Daten sind jene eingestuft**, welche über die rassische und ethnische Herkunft, die religiöse, philosophische oder andere Weltanschauung, die politische Meinung, die Zugehörigkeit zu Parteien und Gewerkschaften die Mitgliedschaft bei einer Partei, Gewerkschaft, Vereinigung oder Organisation mit religiöser, philosophischer, politischer oder gewerkschaftlicher Ausrichtung, die Gesundheit oder das Sexualleben Aufschluss geben können.
Vorausgeschickt, dass die Mitgliedsbühnen keine sensiblen Daten verarbeiten, werden die restriktiven Auflagen betreffend die sensiblen Daten an dieser Stelle nicht näher erläutert.

3. Einholen und Verarbeiten der Daten
Zunächst sei vorausgeschickt, dass Daten, die vor dem 08. 05.1997 gesammelt wurden, frei verwendet werden können.
Für alle nach diesem Datum eingeholten Daten empfiehlt es sich, Informationen zu den Rechten im Zusammenhang mit dem Datenschutz und Zustimmung zur Bearbeitung der Daten schriftlich einzuholen. Am besten ist es, wenn dies im Zuge der Mitgliederneuaufnahme oder bei Anmeldung zu Kursen, veranstaltet von den einzelnen Theatervereinen (vgl. beiliegenden Vordruck A) geschieht.
Zu buchhalterischen Notwendigkeiten können Daten auch ohne Information zu Datenschutz und Einholen von Zustimmungserklärungen bearbeitet werden, ebenso zu allen anderen von Gesetzes wegen vorgeschriebenen Zwecken.

---

[1] Gesetzesvertretendes Dekret vom 30. Juni 2003, Nr. 196.

4. Zustimmung zur Weitergabe von Daten

Vereine und Bühnen, welche die gesammelten Daten an Dritte (z.B. an andere Bühnen, an Weiterbildungsorganisationen, auch im Ausland) weitergeben oder veröffentlichen wollen, müssen die Zustimmung dafür eigens einholen.

5. Datensicherung /Zugangskotrolle und Archivierung

Grundsätzlich gilt, dass personenbezogene Daten in allen Phasen, d.h. von der Erhebung bis hin zum Löschen immer mit größter Sorgfalt zu behandeln sind. Insbesondere gilt, dass bei rein händischer Datenbearbeitung:

- Daten und Kopien in abschließbaren Fächern (Schließfächern) aufzubewahren sind.
- Die Mitarbeiter schriftlich anzuweisen sind, wie mit den Daten verfahren werden darf/muss (z.B. überholte Karteikarten im Reißwolf vernichten; Schrank mit Karteikarten bei Verlassen des Arbeitsplatzes abschließen) und wer von den Mitarbeitern wofür zuständig ist, ggf. über das Definieren von Rollenbildern. Die Anweisungen sind periodisch, mindestens einmal im Jahr, auf ihre Gültigkeit und Richtigkeit hin zu überprüfen und auf den neuesten Stand zu bringen.
- Unterlagen, welche personenbezogene Daten enthalten (Mitgliederkarteien und –listen) in verschließbaren Schränken/Räumen aufzubewahren sind;

Bei EDV-unterstützter Bearbeitung, gilt zusätzlich:

- PCs, auf welchen personenbezogene Daten gespeichert sind, müssen mit Passwort geschützt sein. Das Passwort selbst muss von Person zu Person unterschiedlich sein und jedenfalls mindestens acht Zeichen lang sein (lässt der Rechner diese Anzahl von Zeichen nicht zu, so ist jedenfalls die maximale Zeichenanzahl auszuschöpfen). Die Passwörter dürfen weder weitergegeben noch in irgendeiner Art verwahrt werden, die es Unbefugten leicht macht, darauf zuzugreifen. Als Passwort dürfen keine Zeichenfolgen verwendet werden, die leicht erraten oder ermittelt werden können. Das zum erstmaligen Gebrauch zugewiesene Passwort ist nach besagtem erstmaligem Gebrauch abzuändern, und anschließend spätestens sechsmonatlich. Alte Passwörter dürfen nicht an andere Mitarbeiter weitergegeben oder von diesen als „neues" Passwort verwendet werden. Von diesen Vorgaben sind Mitarbeiter schriftlich zu informieren. Ebenso sind die Mitarbeiter schriftlich anzuweisen, den Computer am Arbeitsplatz nicht unbeaufsichtigt zu lassen bzw., bei Abwesenheit, in einer Weise zu sperren, dass ein Zugriff nur unter erneuter Eingabe des Passwortes möglich ist. Wird ein Passwort mehr als sechs Monate lang nicht genutzt oder scheidet ein Mitarbeiter aus dem Betrieb aus, verfallen die entsprechenden Passwörter. Für den Fall längerer Abwesenheit eines Mitarbeiters (z.B. Urlaub, Krankheit, Mutterschaft) muss gewährleistet werden, dass die normalerweise nur ihm zugänglichen Daten anderen Berechtigten einsichtig werden (z.B. durch Umleiten des Mailverkehrs, durch Freigabe von Ordnern bzw. durch Hinterlegen/Mitteilen des Passwortes an den Systemadministrator oder eine andere vorab als berechtigt definierte Person);
- in Schriftform, Profile zu den Zugriffsrechten der verschiedenen Mitarbeiter bzw. Gruppen von Mitarbeitern zu definieren sind, diese anschließend mindestens jährlich zu überprüfen und auf den neuesten Stand zu bringen sind;
- die Computer, besonders wenn mit Internet-Anschluss versehen, durch geeignete Maßnahmen (Firewall, Antivirenprogramm usw.) abzusichern sind, wobei die Schutzmechanismen mindestens sechsmonatlich auf den neuesten Stand zu bringen sind;
- auf zu entsorgende Datenträger (Disketten usw.) vorher alle Daten gelöscht werden müssen;
- die gespeicherten Daten müssen mindestens einmal wöchentlich auf andere Datenträger (Bandlaufwerk, CD, Disketten o.ä.) gesichert werden.

6. Überwachung der Sicherheitsmaßnahmen durch den Verantwortlichen

Der Verantwortliche für den Datenschutz ist jedem Verein – sofern nicht eine gewisse Person mit Vorstandsbeschluss damit beauftragt wird – der/die Vorsitzende. Diese/r ist auch dafür verantwortlich, Sorge zu tragen, dass nur Befugte zu den Daten Zugang haben.

So braucht beispielsweise der Kassier für die Erledigung seines institutionellen Auftrages natürlich alle Adressen der Mitglieder, um die Zahlungsaufforderung zuzuschicken.

vom Vorstand genehmigt

Datum und Unterschrift

11.08.2006