Die 10 Grundregeln des Datenschutzes für die tägliche Arbeit

Jeder, der mit Daten umgeht, ist verantwortlich dafür, daß die Ihm anvertrauten personenbezogenen Daten nur für den Zweck der Aufgabenstellung verarbeitet bzw. genutzt werden.
Damit Sie im Umgang mit personenbezogenen Daten auf der sicheren Seite sind, müssen Sie sich an folgende 10 Regeln halten:

1. Passwort

Zu jedem Benutzername gehört ein Passwort. Dieses Passwort muss zwingend den internen Richtlinien für ein sicheres Passwort entsprechen.
Das Passwort darf nur Ihnen bekannt sein. Halten Sie sich stets an die Devise, ein Passwort darf auf gar keinen Fall aufgeschrieben werden, sonder muss im Gedächtnis behalten werden.

2. Umgang mit personenbezogenen Daten

Da Sie für den korrekten Umgang mit personenbezogenen Daten verantwortlich sind, müssen Sie darauf achten, daß Sie immer nur mit denjenigen personenbezogenen Daten in Berührung kommen, welche Sie zwingend für Ihre Tätigkeit benötigen.

3. Speicherung von personenbezogenen Daten

Festplatten von PCs stellen ein Sicherheitsrisiko bzgl. der Verfügbarkeit, Speicherung und des Schutzes dar. Deshalb müssen Sie darauf achten, dass Sie personenbezogene Daten auf dem Server abspeichern.

4. Konfigurationen

Ihre PCs sind alle konfiguriert und mit entsprechenden Sicherheitsprogrammen ausgestattet. Sie dürfen zu keiner Zeit die Voreinstellungen verändern und unter keinen Umständen selbständig in die Hard- und Software-Konfiguration eingreifen.

5. Datentransport

Bei der Versendung von Daten, gleich ob per E-Mail oder durch ein Transportunternehmen, müssen Sie darauf achten, dass diese sicher bei dem entsprechenden Empfänger ankommen. Dies kann zum Einen durch eine verschlüsselte Versendung, zum Anderen durch ein zuverlässiges Transportunternehmen und einer zuverlässigen Verpackung der zu versendenden Daten gewährleistet werden.

6. Schließen und Sichern

Jedesmal wenn Sie Ihren Arbeitsplatz verlassen, z.B. Mittagspause, Meeting etc. müssen die Räumlichkeiten abgeschlossen und ihr PC durch die Aktivierung des Kennwortschutzes gesichert werden. Nur so ist sichergestellt, dass Unbefugte keinen Einblick in personenbezogene bzw. sonstige Daten erhalten.

Bei längerer Abwesenheit ist es ratsam, sich ganz von den Systemen abzumelden, um z.B. Systemarbeiten nicht zu behindern.
Diese Vorgaben gelten nicht nur in den Vereinsräumlichkeiten, sondern auch bei Homeoffice-Tätigkeit.

7. Verschluss von Daten

Personenbezogene und andere sensible Daten, egal ob auf dem Computerbildschirm, auf Datenträger oder in Papierform, müssen, sofern Sie daran nicht unmittelbar arbeiten, unter Verschluss gehalten werden. Dies wird zum Beispiel dadurch erreicht, dass die Computerbildschirme so aufgestellt werden, dass Dritte keine Einsichtmöglichkeit auf den Bildschirm haben. Daten auf Datenträgern und bei Daten in Papierform dürfen nicht offen auf dem Schreibtisch oder sonst irgendwo herum liegen, sondern in einem verschließbaren Schrank unter Verschluss gehalten werden.

8. Aufbewahrungs- und Löschungsfristen

Personenbezogenen Daten müssen laut Gesetz eine bestimmte Dauer aufbewahrt bzw. nach einer bestimmten Dauer gelöscht werden. Sie müssen darauf achten, dass Sie die vom Verein vorgegebenen und festgesetzte Aufbewahrungs- bzw. Löschungsfristen beachten.

9. Vernichtung von Akten und Datenträgern

Nicht mehr benötigte Datenträger und Listenausdrucke müssen datenschutzgerecht vernichtet bzw. entsorgt werden, damit eine missbräuchliche Verwendung der Daten ausgeschlossen ist. Dokumente mit personenbezogenen Daten und Datenträger gehören selbstverständlich nicht in einen gewöhnlichen Papierkorb. Die Vernichtung muss zwingend den internen Richtlinien für eine sichere Vernichtung entsprechen.

10. Schlüssel

Schlüssel für Büroräumlichkeiten, für Aktenschränke etc. dürfen nicht offen herumliegen. Sie müssen darauf achten, dass eine strikte Trennung zwischen den Schlüsseln für geschäftliche Zwecke und für private Zwecke erfolgt.

Fazit: Gehen Sie mit den personenbezogenen Daten in der Art und Weise um, wie Sie es sich wünschen würden, wie man mit Ihren eigenen personenbezogenen Daten umgehen sollte!