Technische und Organisatorische Maßnahmen im Datenschutz

FC Stöckach e.V.

Version 1.0

September 2018

Dokumenteneinstufung: intern

Autoren	Kontaktdaten
Michael Pfundt	info@fc-stoeckach.de

Version	Datum	Änderungsverlauf	Autor
1.0	September 2018	Erstellung	MP

Dokumentenklassifikation: - intern -

Inhaltsverzeichnis

Präambel

Die technischen und organisatorischen Maßnahmen (TOM) dienen zum Schutz der Mitgliederdaten und dem Einhalten der DSGVO. Sie sind jeder Person die für den FC Stöckach mit personenbezogenen Daten umgeht zur Kenntnis zu geben. Die Einhaltung der Maßnahmen ist ein wesentlicher Baustein zur Sicherheit der Daten.

Die TOM sind als Anlage zur Geschäftsanweisung Datenschutz zu verstehen.

Erster Teil: Allgemeine Regelungen

1 Zweck und Aufbau des Dokumentes

Die TOM beschreiben die mindestens notwendigen Vorkehrungen, die beim Umgang mit personenbezogenen Daten für den FC Stöckach zu treffen sind. Bei ihrer Festlegung wurde auf ein angemessenes Verhältnis von Sicherheit zu Machbarkeit geachtet.

2 Geltungsbereich und Verantwortung

Der Geltungsbereich des Dokumentes umfasst die Verarbeitung personenbezogener Daten durch alle im Namen des Vereins handelnden Personen.

Vorliegendes Dokument ist allen diesen Personen, die potentiell mit der Verarbeitung personenbezogener Daten in Berührung kommen, bekannt zu geben und ist eine Grundlage für deren Arbeit. Die Verantwortung für die operative Umsetzung liegt demnach bei diesem Personenkreis und ist ebenso für evtl. Dritte, die im Auftrag des Vereins tätig sind oder handeln, anzuwenden.

Zweiter Teil: Technische und organisatorische Maßnahmen

3 Zutrittskotrollen

Räume, in denen personenbezogene Daten verarbeitet oder gelagert werden gelten als sensible Bereiche.
Technische Maßnahmen: Bereiche in denen personenbezogene Daten verarbeitet oder gelagert werden sind zu verschließen, wenn sich kein Berechtigter im Raum befindet. Im Einzelfall ist für den Zugriffsschutz auf Unterlagen auch ein verschlossener Schrank/ eine Schublade ausreichend. Besondere Anforderungen an Sicherheitsschlösser oder Schutzklassenschränke werden hierbei nicht gestellt.
Organisatorische Maßnahme: Personen die über einen Schlüssel verfügen der den Zugang zu den Daten ermöglicht sind zu dokumentieren (Schlüsselausgabeliste).

4 Zugangskontrollen

Technische Maßnahmen: EDV-Geräte auf denen personenbezogene Daten verarbeitet oder gespeichert werden sind mindestens mit einem Zugang aus Benutzername und Passwort abzusichern. Greifen mehrere Personen auf diese Geräte zu, ist eine Liste der Berechtigten zu führen. Bei Veränderung des Benutzerkreises ist das Passwort zu ändern. Auf solchen Geräten ist eine aktuelle Anti-Viren-Software zu betreiben. Externe

Datenträger auf denen personenbezogene Daten gespeichert werden sind zu verschlüsseln.

Organisatorische Maßnahmen: Die Berechtigungsvergabe des Zugangs zu bestimmten personenbezogenen Daten liegt beim 1. Vorstand (wer darf was). Beim Einsatz von Software zur Mitgliederverwaltung können dazu bei Bedarf Benutzerprofile angelegt werden. Bei der Passwortnutzung sind die Empfehlungen „Sicheres Passwort“ des BSI (https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html)

anzuwenden. Nach der Arbeit sind in nicht verschlossenen Räumen Unterlagen mit personenbezogenen Daten einzusperren (Clean Desk). EDV-Geräte sollen nach einer Untätigkeit von 15 Minuten automatisch eine Desktopsperre aktivieren.

5 Zugriffskontrolle

Technische Maßnahmen: Akten mit personenbezogenen Daten die nicht mehr benötigt werden sind zu vernichten (Schredder). Bei Datenträgern ist auf eine physische Löschung zu achten. Bei Zugriffen auf die Verwaltungssoftware (Eingabe, Änderung, Löschung von Daten) hat eine Zugriffsprotokollierung zu erfolgen.

Organisatorische Maßnahmen: Die Anzahl an Personen mit Administratorrechten ist so gering wie möglich zu halten. Der Administrator verwaltet Benutzerrechte und Berechtigungskonzepte (falls vorhanden).

6 Trennungskontrolle

Technische Maßnahmen: Eine physikalische Trennung (Systeme/Datenbanken/Datenträger) ist wünschenswert, aber nicht zwingend.

Organisatorische Maßnahmen: Es gilt das Minimalprinzip. Jeder hat nur auf die Daten Zugriff, die er für seine Arbeit benötigt. Dies wird über Berechtigungen gesteuert.

7 Weitergabekontrolle

Technische Maßnahmen: Personenbezogene Daten die per Mail übertragen werden sind nach Möglichkeit zu verschlüsseln, signaturverfahren zu nutzen oder über eine sichere Verbindung (z.B. VPN) zu übertragen. Bei der Bereitstellung von Daten zum Abruf ist auf eine verschlüsselte Verbindung (sftp, https) zu achten.

Organisatorische Maßnahmen: Der Datenempfänger ist festzuhalten. Wo möglich und keine persönlichen Daten erforderlich haben Angaben anonymisiert oder pseudonymisiert zu erfolgen.

8 Eingangskontrolle

Technische Maßnahmen: In der Verwaltungssoftware sind Eingaben, Änderungen und Löschungen von Daten zu protokollieren. Der 1. Vorstand prüft unregelmäßig die Protokolle.

Organisatorische Maßnahmen: Die eingesetzte Software ist zu definieren. Eingaben, Änderungen und Löschungen von Daten sind nachvollziehbar zu gestalten, in dem jeder berechtigte einen eigenen Zugang (Nutzer) erhält (keine Benutzergruppen). Die Berechtigung des Zugangs entspricht den notwendigen Arbeiten. Formulare, von denen Daten in automatisierte Verfahren übernommen werden sind aufzubewahren, solange ihre Daten notwendig sind. Löschungen/Vernichtungen von Daten erfolgen nur von den dafür Zuständigen.

9 Verfügbarkeitskontrolle

Technische Maßnahmen: Orte, an denen Daten zentral gelagert werden sollen über eine Feuer-/Rauchmeldeanlage verfügen. Falls Server eingesetzt werden sind Serverräume zu überwachen. Eine regelmäßige Sicherung der Daten (z.B. RAID-System, Festplattenspiegelung) hat zu erfolgen. Ein Datenschutztresor (S60DIS o.ä.) wird nicht gefordert.

Organisatorische Maßnahmen: Falls eigene Datensicherung erfolgt ist der Verantwortliche dafür zu benennen. Ein Test zur Datenwiederherstellung und eine Protokollierung des Ergebnisses sollen jährlich erfolgen. Das Sicherungsmedium ist verschlossen und räumlich getrennt vom ursprünglichen Datenträger aufzubewahren (anderer Brandabschnitt/anderes Gebäude). In Serverräumen dürfen keine Sanitären Anschlüsse verlaufen. Für Betriebssystem und Daten sind auf EDV-Geräten getrennte Partitionen zu nutzen.

10 Datenschutz-Maßnahmen

Technische Maßnahmen: Eine zentrale Dokumentation aller Verfahren zur Verarbeitung personenbezogener Daten wird geführt.

Organisatorische Maßnahmen: Ein Datenschutzbeauftragter wird bestellt. Die umgehenden Personen werden auf Vertraulichkeit/ das Datengeheimnis verpflichtet und regelmäßig sensibilisiert. Eine Datenschutzfolgeabschätzung erfolgt nur bei Bedarf. Der FC Stöckach kommt seinen Informationspflichten nach Art. 13 und 14 DSGVO nach. Vor Erteilung von Auskünften an Betroffene ist deren Identität festzustellen und der Datenschutzbeauftragte bei Bedarf zu konsultieren.

11 Incident-Response-Management

Technische Maßnahmen: Eine Firewall wird eingesetzt und regelmäßig aktualisiert, ebenso Spamfilter und Virenscanner.

Organisatorische Maßnahmen: Bei Sicherheitsvorfällen und Datenpannen ist der DSB einzubinden. Vorfälle sind zu Dokumentieren und ggf. an den Landesdatenschutzbeauftragten zu melden.

12 Outsourcing an Dritte

Organisatorische Maßnahmen: Auftragsnehmer und deren Sicherheitsmaßnahmen sind zu prüfen. Vereinbarungen zur Auftragsdatenverarbeitung werden geschlossen. Sein einhalten der Mindeststandards ist zu gewährleisten.

Igensdorf, den 27.09.2018

Uwe Zollikofer, 1. Vorsitzender