Datenschutzrichtlinie

Turnverein TV 1864 Bernsbach e.V.

1. Grundsätze

Der Schutz personenbezogener Daten ist uns ein wichtiges Anliegen. Deshalb verarbeiten wir die personenbezogenen Daten unserer Mitglieder in Übereinstimmung mit den anwendbaren Rechtsvorschriften zum Schutz personenbezogener Daten und zur Datensicherheit. In dieser Datenschutzrichtlinie wird beschrieben, welche Arten von personenbezogenen Daten wir erheben, wie diese Daten genutzt werden, an wen sie übermittelt werden und welche Wahlmöglichkeiten und Rechte betroffene Personen im Zusammenhang mit unserer Verarbeitung der Daten haben. Außerdem beschreiben wir, mit welchen Maßnahmen wir die Sicherheit der Daten gewährleisten und wie betroffene Personen Kontakt mit uns aufnehmen können, wenn Sie Fragen zu unserer Datenschutzpraxis haben. Diese Richtlinie regelt die datenschutzkonforme Informationsverarbeitung und die insoweit bei Turnverein TV 1864 Bernsbach e.V. bestehenden Verantwortlichkeiten. Alle Mitglieder sind zur Einhaltung der Richtlinie verpflichtet.
Sie richtet sich:

An den Vorstand sowie Mitglieder der Vereinsorganisation und alle anderen Mitglieder des Vereins, soweit diese mit personenbezogenen Daten anderer in Beziehung kommen.

Dabei gelten folgende Grundsätze:

Die Hard- und Software sind für Vereinsaufgaben, und zwar für die jeweils vorgesehenen Zwecke, zu verwenden und gegen Verlust und Manipulation zu sichern.
Eine Nutzung für private Zwecke bedarf der ausdrücklichen Genehmigung.
Jedes Mitglied ist in seinem Verantwortungsbereich für die Umsetzung der Richtlinie verantwortlich. Die Einhaltung muss von ihm regelmäßig kontrolliert werden.
Der Vorstand stellt sicher, dass seine Mitglieder (Benutzer) über diese Richtlinie informiert werden; das gilt auch für temporär Beschäftigte.

2. Der Datenschutzkoordinator

Der Verein ist von der Bestellung eines Datenschutzbeauftragten befreit, da die Bedingungen §38 Abs. 1 BDSG n.F. nicht erfüllt werden.
Davon unbeschadet kann der Verein jederzeit einen Datenschutzbeauftragten bestellen, sofern sich die Notwendigkeit hierfür ergibt.
Verantwortlicher i.S.d. Datenschutzes ist der Vorstand.

3. Beschaffung/Hard- und Software

3.1 Die Beschaffung von Hard- und Software erfolgt grundsätzlich auf Anforderung des Vereinsvorstandes.
3.2. Bereits bei der Auswahl von Hard- und Software wird das Prinzip der Gewährleistung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen als ein tragendes Kriterium beachtet.
3.3 Private Hard- und Software dürfen nicht zur Verarbeitung personenbezogener Daten Verwendung finden.
3.4 Bei Verdacht des Diebstahls von Hard- und Software, des unbefugten Zugriffs auf personenbezogene Daten, von Sabotage etc. ist der Vorstand unverzüglich zu informieren. Näheres regelt die Verfahrensanweisung „Verhaltensmaßnahmen bei einer Datenpanne“.

4. Verpflichtung/Schulung der Mitarbeiter

Jedes Mitglied, welches Umgang mit personenbezogenen Daten hat, ist auf einen vertraulichen Umgang mit personenbezogenen Daten und die Einhaltung dieser Richtlinie zu verpflichten.

5. Transparenz der Datenverarbeitung

5.1 Über Verfahren, die den Umgang mit personenbezogenen Daten betreffen, wird ein Verzeichnis von Verarbeitungen gem. Art. 30 DS-GVO geführt.
5.2 Der Vorstand erstellt eine Datenschutzrichtlinie zur Aufklärung Betroffener über Art und Umfang der Verarbeitung personenbezogener Daten. Die Datenschutzrichtlinie ist öffentlich und für jeden einsehbar. Für ergänzende Fragen steht der Vorstand zur Verfügung.
5.3 Macht ein Betroffener von seinem Auskunftsrecht nach Art. 15 DS-GVO oder seinem Korrektur- oder Widerspruchsrecht nach Art. 16 und Art. 21 DSGVO Gebrauch, so erfolgt die zentrale Bearbeitung durch den Verantwortlichen.
Auskunfts- und Einsichtsrechte von Mitgliedern werden durch die Vereinsleitung erfüllt.
Es ist sicherzustellen,dass dem Betroffenen seine Daten auf Wunsch in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden können.

6. Erhebung/Verarbeitung von personenbezogenen Daten

6.1 Die Erhebung und Verarbeitung personenbezogener Daten darf nur im Rahmen des rechtlich Zulässigen erfolgen (siehe Punkt 11). Hierbei sind auch die besonderen Voraussetzungen für die Erhebung und Verarbeitung sensibler Daten gemäß Art.9 Abs. 1 DSGVO zu beachten. Grundsätzlich dürfen nur solche Informationen verarbeitet und genutzt werden, die zur Aufgabenerfüllung des Vereins erforderlich sind und in unmittelbarem Zusammenhang mit dem Verarbeitungszweck stehen.
6.2 Es wird sichergestellt, dass Betroffene keiner Entscheidung unterworfen werden, die ausschließlich auf einer automatisierten Verarbeitung beruhen und zugleich den Betroffenen gegenüber eine rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen (bspw. Profiling).
6.3 Vor Einführung neuer Arten von Erhebungen ist die die Zulässigkeit bestimmende Zweckbestimmung der Daten durch den für die Anwendung Verantwortlichen schriftlich zu dokumentieren. Grundsätzlich ist eine Zweckänderung nur dann zulässig, wenn die Verarbeitung mit denjenigen Zwecken vereinbar ist, für die die Daten ursprünglich erhoben worden sind. Die im Rahmen der Zweckänderung genutzten Abwägungskriterien sind einzeln zu prüfen.
Die Prüfung ist darüber hinaus auch zu einem ordnungsgemäßen Nachweis zu dokumentieren.
Eine Zweckänderung ist auch zulässig, wenn eine Einwilligung der betroffenen Person durch den Verantwortlichen eingeholt wird. Gleichzeitig hat der für die Verarbeitung Verantwortliche vor der Erhebung bzw. der Speicherung von Daten schriftlich festzulegen, ob und in welcher Art und Weise der gesetzlichen Benachrichtigungspflicht des Betroffenen zu genügen ist.
6.4 Falls andere Stellen Informationen über Betroffene anfordern, dürfen diese ohne Einwilligung des Betroffenen nur gegeben werden, wenn hierfür eine gesetzliche Verpflichtung oder ein die Weitergabe rechtfertigendes legitimes Interesse des Vereins oder des Betroffenen besteht und die Identität des Anfragenden zweifelsfrei feststeht.

7. Datenhaltung/Versand/Löschung

7.1 Die Speicherung von Daten erfolgt grundsätzlich auf den hierzu zur Verfügung gestellten Speichermedien. Eine Speicherung auf mobilen Datenträgern oder Cloudspeicher bedarf der Genehmigung durch den Vorstand.

7.2 Gesetzliche Aufbewahrungsfristen und Löschungstermine sind von dem über die Verarbeitung der Daten Entscheidenden in seiner Verantwortung zu beachten. Der Vorstand ist über die Einhaltung der Termine insbesondere im Hinblick auf die Löschung personenbezogener Daten in Sicherungskopien zu informieren.
7.3 Bei der Weiter- oder Rückgabe nicht mehr benötigter IT-Komponenten ist der Benutzer verpflichtet, dafür zu sorgen, dass zuvor sämtliche Daten wirksam gelöscht wurden.
7.4 Jede Form der Speicherung oder Weitergabe ist mit geeigneten Schutzmechanismen zu versehen (z.B. Zugriffsschutz durch Passwort, Verschlüsselung).

8. Externe Dienstleister/Auftragsverarbeitung/Wartung

8.1 Sollen externe Dienstleister erstmals mit der Verarbeitung personenbezogener Daten bzw. einzelnen Verarbeitungsschritten (z.B. Erhebung, Löschung = Entsorgung) bzw. mit Tätigkeiten (z.B. Wartung, Reparatur) beauftragt werden, bei denen sie die Möglichkeit der Kenntnis personenbezogener Daten bekommen, so ist der Vorstand vor der Beauftragung unter Vorlage des den Anforderungen des Art. 28 DS-GVO genügenden Vertragsentwurfs (ADV-Vertrag) und der Kriterien der erfolgten bzw. nachfolgend vorgesehenen Auftragskontrolle zu informieren.

9. Sicherheit der Verarbeitung

9.1 Für jedes Verfahren ist eine dokumentierte Schutzbedarfsfeststellung sowie eine Analyse bzgl. der für den Betroffenen möglichen Risiken zu erstellen. Diese richten sich an der Art, dem Umfang, der Umstände und Zwecke der Verarbeitung sowie der Wahrscheinlichkeit des Eintritts einer solchen Gefahr.
9.2 Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität der Daten sowie der Belastbarkeit der Daten verarbeitenden Systeme ist ein allgemeines Sicherheitskonzept zu erstellen. Das Konzept orientiert sich an der zuvor erstellten Schutzbedarfsfeststellung und der Risikoanalyse. Dieses Konzept ist maßgeblich für alle weiteren Verfahren.

10. Rechenschafts- und Dokumentationspflicht

Die Einhaltung der Vorgaben, die sich aus dieser Richtlinie ergeben, muss jederzeit nachweisbar sein. Eine Nachweisbarkeit hat insbesondere durch eine schlüssige und nachvollziehbare schriftliche Dokumentation hinsichtlich getroffener Maßnahmen und dazugehöriger Abwägungen zu erfolgen.

11. Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten

Artikel 6 Abs. 1 DSGVO regelt die Rechtmäßigkeit.

12: Vorgehensweise bei Auskunftsersuchen

- Im Falle eines Auskunftsersuchens ist die Anfrage durch den Betroffenen schriftlich zu stellen (Nachweispflicht).
- Auskünfte werden grundsätzlich nur nach bestätigter Identität und schriftlich erteilt
- Auskünfte sind unverzüglich, jedoch binnen eines Monats zu beantworten

13. Verhaltensmaßnahmen bei einer Datenpanne

- Datenschutzvorfälle sind unverzüglich dem Verantwortlichen zu melden
- Der Verantwortliche entscheidet über die weitere Vorgehensweise
- Besteht ein Risiko für den Betroffenen, so ist der Vorfall der Datenschutzbehörde anzuzeigen (binnen 72 Stunden nach Bekanntwerden)
- Besteht ein hohes Risiko, ist zusätzlich der Betroffene zu benachrichtigen