Datenschutzordnung des Sportverein Aschau e. V.

§1 Präambel

Der Sportverein Aschau e. V. („Verein“) verarbeitet personenbezogene Daten seiner Mitglieder, Beschäftigten, Ehrenamtlichen, Übungsleiter, Funktionsträger und weiterer Beteiligter im Rahmen seiner satzungsgemäßen Aufgaben (§ 1 der Satzung, u. a. Förderung des Sports) sowie zur Kommunikation, Öffentlichkeitsarbeit und Verwaltungszwecken. Die Verarbeitung erfolgt im Einklang mit der **DSGVO**, dem **BDSG** und unter Beachtung datenschutzrechtlicher Grundsätze.

§2 Verantwortlicher und Datenschutzkontakt

Verantwortlich für die Datenverarbeitung im Verein:

Sportverein Aschau e. V.
Schulstraße 3, 84544 Aschau am Inn, Bayern

Vertreten durch den Vorstand im Sinne des § 26 BGB (1. Vorsitzender) – dieser ist datenschutzrechtlich verantwortlich.

Datenschutzkontakt:

Ein Datenschutzverantwortlicher / –beauftragter kann auf Vorstandsbeschluss benannt werden (freiwillig, empfohlen, vgl. Hinweise für Vereine). Dessen Kontaktdaten sind auf der Internetseite des Sportvereins www.sv-aschau.de angegeben.

§3 Geltungsbereich

Diese Datenschutzordnung gilt für:

- alle Mitglieder und sonstigen Betroffenen,
- alle Vereinsorgane,
- alle ehrenamtlich Tätigen,
- alle datentechnischen und organisatorischen Ebenen des Vereins inklusive Abteilungen.
- Sie umfasst alle Verfahren der Datenverarbeitung – digital und analog.

§4 Grundsätze

Der Verein verarbeitet personenbezogene Daten nach den Grundsätzen von

- Rechtmäßigkeit,
- Zweckbindung,
- Datenminimierung,

- Transparenz,
- Integrität und Vertraulichkeit,
- Rechenschaftspflicht.

Nur Daten, die zur Erfüllung der satzungsgemäßen Aufgaben und Pflichten erforderlich sind, werden verarbeitet.

§5 Datenverarbeitung und Datennutzung

Daten dürfen ausschließlich verarbeitet und genutzt werden in Übereinstimmung mit den in Anhang 1: Verzeichnis der Verarbeitungstätigkeiten (VVT) genannten Punkten.

§6 Betroffenenrechte

(1) Betroffene Personen haben die Rechte auf:

- Auskunft,
- Berichtigung,
- Löschung,
- Einschränkung der Verarbeitung,
- Datenübertragbarkeit,
- Widerspruch.

(2) Anfragen sind schriftlich an den Vorstand oder den Datenschutzkontakt zu richten.

(3) Die Anfragen sind vom Vorstand unverzüglich zu bearbeiten und zu beantworten.

§7 Vertraulichkeit

(1) Alle Personen, die im Verein mit personenbezogenen Daten umgehen, verpflichten sich zur Vertraulichkeit und werden entsprechend geschult (Ehrenamtsvereinbarung).

§8 Datenschutz-Notfall-Plan (Datenschutzvorfälle)

(1) Ein Datenschutzvorfall liegt vor, wenn personenbezogene Daten verloren gehen, unbefugt offengelegt, verändert oder missbräuchlich verwendet werden.

(2) Datenschutzvorfälle sind unverzüglich dem Vorstand oder der benannten datenschutzverantwortlichen Person zu melden.

(3) Der Vorstand prüft den Vorfall und entscheidet über erforderliche Maßnahmen, insbesondere eine Meldung an die Datenschutzaufsichtsbehörde gemäß Art. 33 DSGVO innerhalb von 72 Stunden, sofern ein Risiko für Betroffene besteht.

(4) Besteht ein hohes Risiko für die Rechte und Freiheiten betroffener Personen, werden diese gemäß Art. 34 DSGVO informiert.

(5) Datenschutzvorfälle sind intern zu dokumentieren, einschließlich Ursache, Auswirkungen und getroffener Maßnahmen.

§9 Passwort-Richtlinie

(1) Zugangsdaten und Passwörter zu vereinsbezogenen Systemen sind vertraulich zu behandeln und dürfen nicht an Dritte weitergegeben werden.

(2) Passwörter sind bei einem Rollen- oder Amtswechsel sowie bei Verdacht auf Missbrauch unverzüglich zu ändern.

(3) Passwörter sind sicher aufzubewahren und dürfen nicht ungeschützt gespeichert oder offen notiert werden.

(4) Der Verein kann Mindestanforderungen an die Passwortsicherheit (z. B. Länge, Komplexität, Zwei-Faktor-Authentifizierung) festlegen.

§10 Datenhaltung auf privaten Geräten

(1) Personenbezogene Vereinsdaten dürfen nur auf privaten Geräten gespeichert oder verarbeitet werden, wenn diese angemessen gegen unbefugten Zugriff gesichert sind (z. B. Gerätesperre, Passwortschutz).

(2) Sensible personenbezogene Daten (z. B. Bankdaten, Ausweiskopien, Gesundheitsdaten) dürfen nicht auf ungesicherten Privatgeräten gespeichert werden.

(3) Soweit möglich, sind zentrale Vereinslösungen (z. B. Vereinssoftware, Cloud-Dienste des Vereins) gegenüber privaten Speichern zu bevorzugen.

(4) Beim Verlust oder Diebstahl eines privaten Geräts mit Vereinsdaten ist unverzüglich der Vorstand zu informieren.

§11 Auftragsverarbeitung und Dienstleister (AV-Verträge)

(1) Beauftragt der Verein externe Dienstleister mit der Verarbeitung personenbezogener Daten (z. B. Hosting, Vereinssoftware, Zahlungsdienstleister), stellt der Vorstand sicher, dass ein Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO abgeschlossen wird.

(2) Der Vorstand prüft und dokumentiert, dass Dienstleister angemessene Datenschutz- und Sicherheitsstandards einhalten.

(3) Die Nutzung von Dienstleistern ohne entsprechende datenschutzrechtliche Vereinbarung ist unzulässig.

(4) Eine Übersicht der eingesetzten Dienstleister ist vom Vorstand aktuell zu halten.

§12 Amtsübergabe und Datenrückgabe

(1) Beim Ausscheiden von Funktionsträgern oder Ehrenamtlichen sind alle vereinsbezogenen Daten, Unterlagen und Zugangsdaten unverzüglich zurückzugeben oder zu löschen.

(2) Der Vorstand stellt sicher, dass Zugriffsrechte entzogen, Passwörter geändert und Benutzerkonten gesperrt werden.

(3) Vereinsdaten dürfen nach dem Ausscheiden nicht weiter gespeichert oder verwendet werden.

(4) Amtsübergaben sind geordnet zu dokumentieren, um Datenverlust oder unbefugte Nutzung zu vermeiden.

§13 Inkrafttreten

(1) Diese Datenschutzordnung tritt mit ihrer Verabschiedung durch Beschluss des Vereinsausschusses am 02.02.2026 in Kraft.

(2) Sofern die Datenschutzordnung keine Regelungen enthält, gilt die Vereinssatzung.

(3) Bei Verstößen gegen die Datenschutzordnung können diesbezüglich Handelnde haftungsrechtlich in Anspruch genommen werden.

Das Original dieser Datenschutzordnung ist von folgenden Mitgliedern unterzeichnet:

Volk Johannes	1. Vorsitzender	.....
Höpfinger, Andreas	2. Vorsitzender (Geschäftsführer)	.....
Knoll, Irina	Schatzmeisterin	.....
Rappensperger, Karola	Schriftführerin	.....
Erber, Sebastian	Abteilungsleiter Badminton	.....
Wehrle, Christian	Abteilungsleiter Fußball	.....
Schebesta, Michael	Abteilungsleiter Kegeln	.....
Hiebel, Helmut	Abteilungsleiter Tae Kwon Do	.....
Salzeder, Georg	Abteilungsleiter Tennis	.....
Sättler, Claudia	Abteilungsleiterin Turnen	.....
John, Armin	Abteilungsleiter Volleyball	.....
Harwalik, Alfred	Abteilungsleiter Wintersport	.....
Höpfinger, Gerhard	Beisitzer	.....
Weyrich, Christian	Beisitzer	.....
Wimmer, Andreas	Beisitzer	.....

Anhang 1: Verzeichnis der Verarbeitungstätigkeiten (VVT)

Kategorien personenbezogener Daten

Es werden insbesondere verarbeitet:

1. Mitgliederdaten
1.1 Name, Anschrift, Geburtsdatum, Geschlecht,
1.2 Kontaktdaten (Telefon, E-Mail), Status (aktiv/passiv),
1.3 Abteilungszugehörigkeit, Funktion/Ämter.
2. Vertragsdaten
2.1 Bankverbindung für Beitragseinzug,
2.2 Eintrittsdatum, Kündigungs-/Austrittsdatum.
3. Organisationsdaten
3.1 Anwesenheitslisten, Einsatz- und Veranstaltungsdaten,
3.2 Qualifikationen, Befähigungsnachweise.
3.3 Eintragungen im Führungszeugnis oder Unbedenklichkeitsbescheinigung
4. Kommunikations- und Mediendaten
4.1 Beiträge für Web, soziale Medien,
4.2 Foto-/Video-Material von Vereinsaktivitäten.
5. Sonstige Daten
5.1 nur im Rahmen gesetzlicher Vorgaben oder mit Einwilligung.

Zwecke der Verarbeitung

Daten werden verarbeitet zur:

- Mitgliederverwaltung und Beitragseinzug,
- Organisation des Sportbetriebs,
- Kommunikation intern (E-Mail/ Messenger) und extern,
- Öffentlichkeitsarbeit (Website, Social Media, Presse),
- Erfüllung gesetzlicher Pflichten (Steuerrecht, Verbandspflichten),
- Sicherstellung der Vereinsarbeit.

Rechtsgrundlagen

Rechtsgrundlagen sind u. a.:

- **Art. 6 Abs. 1 lit. b DSGVO:** Erfüllung des Mitgliedschaftsverhältnisses,
- **Art. 6 Abs. 1 lit. c DSGVO:** gesetzliche Verpflichtungen,
- **Art. 6 Abs. 1 lit. f DSGVO:** berechtigtes Vereinsinteresse,
- **Art. 6 Abs. 1 lit. a DSGVO:** Einwilligung (z. B. Fotos).

Interne Nutzung der Daten

(1) Empfänger von Daten können sein:

- Vorstand
- Vereinsorgane
- Abteilungsleiter

- Trainer, Übungsleiter und ehrenamtlich tätige Personen
- Nutzung in E-Mails nur mittels klar definiertem Verteiler sowie vertrauliche Inhalte nur an berechtigte Personen.

(2) Messenger-Gruppen von Drittanbietern dürfen unter folgenden Maßgaben genutzt werden:

- Nutzung für interne Organisation zulässig
- Gruppen nur geschlossen und kontrolliert mit Berechtigten
- keine Verbreitung sensibler Daten in Messenger-Chats
- Teilnahme für Mitglieder ist freiwillig

Weitergabe von Daten an Dritte

(1) Daten werden nur weitergegeben an:

- Verbände (z. B. Bayerischer Landes-Sportverband) im Rahmen bestehender Pflichten,
- Behörden bei gesetzlicher Verpflichtung,
- Dienstleister (z. B. Banken, Versicherungen, Website-Hoster, Druckereien, Fotografen) zur Leistungserfüllung.

(2) Es dürfen nur die zur Leistungserfüllung notwendigen Daten weitergegeben werden.

(3) Eine sonstige Weitergabe findet nicht statt.

Internetseite und Social Media

(1) Offizielle Auftritte (Homepage/ soziale Netzwerke) werden vom Verein verantwortet.

(2) Zuständigkeiten und Zugriffsrechte werden durch den Vorstand geregelt.

(3) Veröffentlicht werden Berichte, Ergebnisse, Mannschaftsbilder etc. unter Beachtung der Datenschutzregeln.

(4) Einzelporträts/ Namensnennungen nur bei rechtlicher Grundlage oder Einwilligung.

Foto- und Videoaufnahmen

(1) Bei Veranstaltungen können Fotos und Videos erstellt werden.

(2) Veröffentlichung erfolgt regelmäßig auf Basis eines berechtigten Interesses; bei Minderjährigen oder Einzelaufnahmen ist eine **schriftliche Einwilligung** einzuholen.

(3) Betroffene können der Veröffentlichung widersprechen.

Speicherdauer, Aufbewahrung und Löschung

(1) Daten werden gelöscht, sobald sie für den Zweck nicht mehr erforderlich sind und keine gesetzlichen Aufbewahrungsfristen (z. B. steuerliche, handelsrechtliche) bestehen. Für Beiträge/ Buchhaltungsunterlagen gelten längere Fristen.

Datensicherheit mittels technischer und organisatorischer Maßnahmen (TOM)

(1) Technische und organisatorische Maßnahmen werden getroffen, um Daten vor unbefugtem Zugriff, Verlust oder Missbrauch zu schützen. Insbesondere sind dies:

- Zugriffsbeschränkungen und Zugriffskontrollen
- Passwortschutz mittels sicherer Passwörter
- Datensicherung
- Vertraulichkeitsverpflichtung