Datenschutzrichtlinie

SSV 1952 Torgau e.V.

Inkraftsetzung durch Vorstandsbeschluss am 25.05.2018 in Torgau.
Zuletzt geändert durch Vorstandsbeschluss am 15.10.2018.
Alle Bezeichnungen betreffen sowohl die weibliche als auch die männliche Form.

Inhalt

Teil 1: Verarbeitung personenbezogener Daten

§ 1 Allgemeines

(1) Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten erfolgt im Verein nach den Richtlinien der EU-Datenschutzgrundverordnung (DSGVO) sowie des Bundesdatenschutzgesetzes (BDSG) in der jeweils gültigen Fassung. Die Konformität zum Datenschutz im Umgang mit personenbezogenen Daten im Verein wird insbesondere durch die Satzung und diese Datenschutzrichtlinie gewährleistet.

(2) „Daten“ im Sinne dieses Teils der Datenschutzrichtlinie sind personenbezogene Daten.

§ 2 Verantwortlichkeit

Verantwortlich für die Verarbeitung von Daten ist der Vorstand:

- Präsident: Bernd Karau
- Vizepräsident: Sven Kaminski
- Vizepräsident: Heiko Trinks
- Organisationsleiter: Mirko Stock

Der Vorstand ist erreichbar:

- postalisch: SSV 1952 Torgau e.V.
  -Vorstand-
  Ziegeleiweg 2c
  04860 Torgau
- per E-Mail: info@ssv1952torgau.de
- per Telefon: 03421-904479

§ 3 Datenschutzbeauftragter

Der Datenschutzbeauftragte des Vereins ist:

- Silvana Ochelka

Der Datenschutzbeauftragte ist erreichbar:

- postalisch: SSV 1952 Torgau e.V.
  -Datenschutzbeauftragter-
  Ziegeleiweg 2c
  04860 Torgau
- per E-Mail: datenschutzbeauftragter@ssv1952torgau.de
- per Telefon: 03421-904479

§ 4 Verpflichtungserklärung

Personen, die im Auftrag des Vereins Daten verarbeiten, sind vorab zu belehren und zur Abgabe einer „Verpflichtungserklärung zur Wahrung des Datengeheimnisses und dem datenschutzrechtlich konformen Umgang mit personenbezogenen Daten“ verpflichtet. Verantwortlich für die Verpflichtung ist der Vorstand.

§ 5 Datenverarbeitung

(1) In dem Mitgliedsantrag erfolgt eine datenschutzrechtliche Unterrichtung des Mitglieds durch Verweis auf diese Datenschutzrichtlinie. Der Verein gewährt dem Antragsteller vor dem Unterzeichnen des Mitgliedsantrages Einsicht in diese Datenschutzrichtlinie. Mit dem Mitgliedsantrag einer Person nimmt der Verein folgende Daten auf und verarbeitet diese:

- Vorname und Name
- Anschrift
- Geburtsdatum
- Geburtsort
- Geschlecht
- Kommunikationsdaten
- Mitgliedschaft anderer Familienmitglieder im Verein
- Firma (sofern zutreffend)
- Bankverbindung

Diese Daten sind für das Bestehen einer Mitgliedschaft zwingend notwendig. Eine Person die einen Mitgliedsantrag stellt, ist zur vollständigen Angabe dieser Daten verpflichtet. Kommt diese Person dem nicht nach, ist eine Mitgliedschaft ausgeschlossen.

(2) Bestimmte Abteilungen des Vereins bedürfen zur Durchführung ihrer Tätigkeiten Gesundheitsdaten der Teilnehmer. Um diese Gesundheitsdaten verarbeiten zu können, bedarf der Verein der gesonderten ausdrücklichen Einwilligung der betroffenen Person.

(3) Sonstige Informationen und Informationen über Nichtmitglieder werden von dem Verein verarbeitet, wenn sie zur Erfüllung des Vereinszweckes nützlich bzw. zur Erfüllung eines Vertrages notwendig sind und keine Anhaltspunkte bestehen, dass die betroffene Person ein schutzwürdiges Interesse hat, das der Verarbeitung entgegensteht. Des Weiteren kann der Verein Daten verarbeiten, wenn die betroffene Person eingewilligt hat oder der Verein ein berechtigtes Interesse an den Daten hat.

(4) Daten dürfen nur durch die Personen verarbeitet werden, die im Verein nach Satzung, Geschäftsordnung oder Abteilungsordnungen eine Funktion ausüben, nach deren Aufgabenbereich dies gerechtfertigt ist. Hierzu zählen insbesondere die Mitglieder des Präsidiums, die Trainer und die Übungsleiter. Der Vorstand kann weitere Personen bestimmen, die zur Verarbeitung von Daten ermächtigt sind.

(5) Die Daten können in einem EDV-System verarbeitet bzw. in Karteien geführt werden.

(6) Im Rahmen moderner Kommunikation mit den Mitgliedern nutzen insbesondere Vorstand, Abteilungsleiter, Trainer und Übungsleiter E-Mails, Messenger-Dienste (z.B. WhatsApp, Facebook-Messenger) und Telefon. Insbesondere bei kurzfristigen Absprachen (z.B. Trainingsausfall, Krankheit) sind diese Kommunikationswege zielführend. Postalische Zusendungen werden aus Kostengründen nur in Ausnahmefällen vorgenommen.

(7) Die gesetzlichen Vertreter von nicht voll geschäftsfähigen Mitgliedern sind verpflichtet, dem Verein E-Mailadressen und Telefonnummern zu benennen, unter denen sie erreichbar sind. Der Verein nutzt diese, um im Rahmen seiner Aufsichtspflicht die gesetzlichen Vertreter zu kontaktieren, wenn die Situation dies erfordert (z.B. Unfall, Trainingsausfall, Trainingsverlegung, Absprachen über Wettkämpfe). Zu diesem Zweck werden diese Kontaktdaten der gesetzlichen Vertreter als Empfänger in die jeweiligen Verteilerlisten aufgenommen (z.B. E-Mail-Verteiler, WhatsApp-Gruppe).

§ 6 Übermittlung von Daten an Verbände

(1) Als Mitglied von übergeordneten Verbänden (LSB, DOSB, KSB Nordsachsen) und Fachverbänden ist der Verein verpflichtet, seine Mitglieder an diese zu melden. Übermittelt werden dabei Daten nach den Meldestandards des jeweiligen Verbandes.

(2) Bei Mitgliedern mit besonderen Aufgaben bzw. Funktionen laut Vereinssatzung oder Geschäftsordnung (Vorstandsmitglieder, Ausschussmitglieder), werden die vollständige Adresse mit Telefonnummer, E-Mailadresse sowie der Bezeichnung ihrer Funktion im Verein übermittelt.
(3) Der Verein erklärt bei Abgabe einer Mitgliedermeldung an die Verbände, dass die Daten ausschließlich für verbandsinterne Zwecke verwendet werden dürfen.

§ 7 Presse- und Öffentlichkeitsarbeit, Vereinschronik

(1) Der Vorstand macht Ereignisse des Vereinslebens, insbesondere die Durchführung von Wettkämpfen, Veranstaltungen und Vereinsfesten, die Ergebnisse von Prüfungen, Ehrungen und Feierlichkeiten sowie Mannschaftsaufstellungen auf der Homepage und den Social Media Profilen des Vereins, in den Verbandszeitschriften der übergeordneten Verbände und Fachverbände sowie in verschiedenen Medien bekannt bzw. übernimmt diese in seine Vereinschronik.
(2) Berichterstattungen über Vereinstätigkeiten in Sinne des Absatzes 1, in denen auch Daten und Fotos enthalten sein können, dienen der öffentlichkeitswirksamen Repräsentation des Vereins sowie dessen geschichtlicher Dokumentation und begründen ein berechtigtes Interesse des Vereins an der diesbezüglichen Verarbeitung und Weitergabe von Daten, da es sich dabei um zeitgeschichtliche Vorgänge handelt. Nach ständiger Rechtsprechung des Bundesgerichthofes[1] haben die geschützten Interessen des Vereins dabei Vorrang vor den persönlichen Interessen der betroffenen Personen. Der Verein darf auf dieser Grundlage Daten und Fotos ohne die gesonderte Zustimmung der betroffenen Personen verarbeiten, weitergeben und veröffentlichen.
(3) Das Veröffentlichungsrecht des Vereins nach Absatz 2 besteht nicht, wenn die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz der Daten erfordern, überwiegen. Die betroffene Person hat dem Vorstand das Überwiegen seiner Interessen oder Grundrechte und Grundfreiheiten nachzuweisen.
(4) Der Verein trifft auf Grundlage dieser Datenschutzrichtlinie ausreichende technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes. Dennoch kann bei einer Veröffentlichung von Daten ein umfassender Datenschutz nicht garantiert werden. Insbesondere können Daten auch in Staaten abrufbar sein, die keine der Bundesrepublik Deutschland vergleichbaren Datenschutzbestimmungen kennen. Der Verein kann die Vertraulichkeit, Integrität (Unverletzlichkeit), Authentizität (Echtheit) und Verfügbarkeit der personenbezogenen Daten daher nicht garantieren. Die Teilnehmer der Vereinsveranstaltungen sind sich der Risiken für eine eventuell daraus resultierenden Persönlichkeitsrechtsverletzung bewusst.

§ 8 Weitergabe von Daten an Mitglieder

(1) Daten werden nur an Vorstandsmitglieder und sonstige Mitglieder ausgehändigt, die im Verein nach Satzung, Geschäftsordnung oder Abteilungsordnungen eine besondere Funktion ausüben, welche die Kenntnis der Daten erfordert.
(2) Macht eine Person, die nicht zur Personengruppe des Absatzes 1 gehört, geltend, dass sie Daten zur Wahrnehmung ihrer satzungsmäßigen Rechte bzw. Pflichten benötigt, kann der Vorstand dieser Person die Verarbeitung der Daten gestatten.

§ 9 Verletzung des Schutzes von Daten

(1) Im Falle einer Verletzung des Schutzes von Daten informiert der Vorstand unverzüglich den Datenschutzbeauftragten und ergreift in Absprache mit diesem angemessene Sofortmaßnahmen.

[1] BGH, Urteil v. 28.5.2013 – Az. VI ZR 125/12; BGH, Urteil v. 8.4.2014 – Az. VI ZR 197/13.

(2) Der Vorstand meldet unverzüglich und binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde diese der zuständigen Aufsichtsbehörde nach den gesetzlichen Vorschriften.
(3) Stellt eine Person, die nicht Vorstandsmitglied ist, eine Verletzung des Schutzes von Daten fest, ist diese verpflichtet, diese Verletzung unverzüglich dem Vorstand zu melden.

§ 10 Löschung von Daten

(1) Der Verein löscht Daten, sobald diese für die Erfüllung der Aufgaben des Vereins nicht mehr benötigt werden.
(2) Von der unmittelbaren Löschung nach Absatz 1 sind Daten ausgenommen, für die besondere gesetzliche, satzungsgemäße oder vertragliche Aufbewahrungsfristen gelten. Dies sind insbesondere:

- steuerrechtliche Aufbewahrungsfristen
- handelsrechtliche Aufbewahrungsfristen
- gesetzliche bzw. vertragliche Verjährungsfristen

In diesen Fällen erfolgt die Löschung der Daten zum Ablauf der jeweiligen Frist.

§ 11 Persönliche Rechte

(1) Personen, von denen der Verein Daten verarbeitet, haben gegenüber dem Vorstand das Recht auf

- Auskunft
- Berichtigung
- Löschung
- Einschränkung der Verarbeitung
- Widerspruch gegen die Verarbeitung
- Datenübertragbarkeit

bezüglich der betroffenen Daten nach den dafür jeweils geltenden gesetzlichen Verfahren.
(2) Erfolgt eine Verarbeitung von Daten aufgrund einer gesonderten Einwilligung, kann die Person die Einwilligung jederzeit gegenüber dem Vorstand widerrufen. Der Widerruf berührt nicht die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung.

§ 12 Beschwerderecht bei einer Aufsichtsbehörde

Als Aufsichtsbehörde für die Einreichung von Beschwerden der Betroffenen zum Datenschutz steht der Sächsische Datenschutzbeauftragte zur Verfügung. Kontaktmöglichkeiten zur Einreichung von Anfragen und Beschwerden sind Online einsehbar unter:
https://www.saechsdsb.de/anfragen-und-beschwerden

Teil 2: Daten- und IT-Sicherheit

§ 13 Allgemeines

(1) Informationsverarbeitung spielt eine Schlüsselrolle für unsere Vereinstätigkeit. Alle wesentlichen Funktionen und Aufgaben werden durch Informationstechnik (IT) maßgeblich unterstützt. Ein Ausfall von IT-Systemen muss insgesamt kurzfristig kompensiert werden können. Auch in Teilbereichen darf unser Vereinsleben nicht zusammenbrechen. Der Schutz von Informationen und Daten vor unberechtigtem Zugriff und vor unerlaubter Änderung ist von existenzieller Bedeutung.
(2) „Daten“ im Sinne dieses Teils der Datenschutzrichtlinie sind jede Art von Daten und Informationen, die vom Verein genutzt werden.

§ 14 Übergreifende Ziele

(1) Unsere Daten und unsere IT-Systeme werden in ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Stillstandszeiten toleriert werden können. Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel (Integrität). Die Anforderungen an Vertraulichkeit haben ein normales, an Gesetzeskonformität orientiertes Niveau.
(2) Die Standard-Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen. Schadensfälle mit hohen finanziellen Auswirkungen müssen verhindert werden.
(3) Alle Mitglieder des Vereins halten die einschlägigen Gesetze (z.B. Strafgesetzbuch, Bundesdatenschutzgesetz, Datenschutzgrundverordnung) und vertraglichen Regelungen ein. Negative finanzielle und immaterielle Folgen für den Verein sowie für die Mitglieder durch Gesetzesverstöße sind zu vermeiden.
(4) Alle Mitglieder sind sich ihrer Verantwortung beim Umgang mit IT bewusst und unterstützen die Sicherheitsstrategie nach besten Kräften.

§ 15 Detailziele

(1) Verspätete oder fehlerhafte Vorstandsentscheidungen können weitreichende Folgen nach sich ziehen. Daher ist für den Vorstand bei wichtigen Entscheidungen der Zugriff auf aktuelle Steuerungsdaten wichtig. Für diese Informationen ist ein hohes Sicherheitsniveau in Bezug auf Verfügbarkeit und Integrität sicher zu stellen.
(2) Die Datenschutzgesetze und die Interessen unserer Mitglieder verlangen eine Sicherstellung der Vertraulichkeit der Daten. Die Daten und die IT-Anwendungen der Mitgliederverwaltung werden daher einem hohen Vertraulichkeitsschutz unterzogen. Gleiches gilt für die Daten unserer Kunden und Geschäftspartner.
(3) Für den Vorstand ist die Aufrechterhaltung der Kommunikation nach außen zu den Mitgliedern und Partnern und der Zugriff auf die Kundendatenbank elementar. Die Geschäftsabwicklung darf nicht verzögert oder gar gefährdet werden. Wenn vertraglich festgelegte Leistungsfristen nicht eingehalten werden können, kann dies weitreichende negative Folgen haben. Insbesondere eine mangelhafte Verfügbarkeit der IT-Systeme und der Daten, aber auch Fehlfunktionen können zu Verlusten führen. Die Aufrechterhaltung der Kommunikation und der ständige Zugriff auf korrekte Daten für den Vorstand hat einen hohen Schutzbedarf.

(4) Die Nutzung des Internets zur Informationsbeschaffung und zur Kommunikation via E-Mail, WhatsApp usw. ist für uns selbstverständlich. Durch entsprechende Maßnahmen wird sichergestellt, dass die Risiken der Internet-nutzung möglichst gering bleiben.

§ 16 Sicherheitsmanagement

(1) Zur Erreichung der Sicherheitsziele kann der Vorstand einen Datenschutzbeauftragten bestellen.
(2) Der Datenschutzbeauftragte ist durch die IT-Benutzer ausreichend in seiner Arbeit zu unterstützen. Der Datenschutzbeauftragte ist frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen.
(3) Die IT-Benutzer haben sich in sicherheitsrelevanten Fragestellungen an die Anweisungen des Datenschutzbeauftragten zu halten.

§ 17 Sicherheitsmaßnahmen

Zur Erreichung der Sicherheitsziele sind folgende Sicherheitsmaßnahmen anzuwenden:

1. Für alle Verfahren, Daten, IT-Anwendungen und IT-Systeme bestimmt der Vorstand den jeweiligen Schutzbedarf und legt den zugriffsberechtigten Personenkreis fest.
2. Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertreter ihre Aufgaben erfüllen können.
3. Gebäude, Räumlichkeiten und Anlagen werden ausreichend gegen unbefugten Zutritt gesichert.
4. Der Zugang zu IT-Systemen wird durch angemessene Zugangskontrollen (Konten und Passwörter) und der Zugriff auf die Daten durch ein restriktives Berechtigungskonzept geschützt.
5. Benutzernamen und Passwörter sind geheim zu halten.
6. Auf allen IT-Systemen werden automatische Updates des Betriebssystems aktiviert.
7. Auf allen IT-Systemen werden automatische Updates des Internetbrowsers aktiviert.
8. Computer-Viren-Schutzprogramme mit automatischen Updates werden auf allen IT-Systemen eingesetzt.
9. Alle Internetzugänge werden durch eine geeignete Firewall gesichert.
10. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden.
11. Die IT-Benutzer unterstützen durch eine sicherheitsbewusste Arbeitsweise alle Sicherheitsmaßnahmen und informieren bei Auffälligkeiten den Vorstand.
12. E-Mails mit verdächtigen oder unbekannten Dateianhängen dürfen nicht geöffnet werden.
13. Mobile Datenträger sind vor dem Öffnen der darauf befindlichen Dateien durch ein Virenschutzprogramm zu untersuchen.
14. Datenverluste können nie vollkommen ausgeschlossen werden. Durch eine umfassende und kontinuierliche Datensicherung wird daher gewährleistet, dass der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des Datenbestandes verloren gehen oder offensichtlich fehlerhaft sind.
15. Informationen werden einheitlich gekennzeichnet und so aufbewahrt, dass sie schnell auffindbar sind.
16. Um größere Schäden in Folge von Notfällen zu begrenzen bzw. diesen vorzubeugen, muss auf Sicherheitsvorfälle zügig und konsequent reagiert werden. Unser Ziel ist, auch bei einem

Systemausfall kritische Vereinsprozesse aufrecht zu erhalten und die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen.

17. Sollen Daten beabsichtigt gelöscht werden ist sicherzustellen, dass die Löschung endgültig durchgeführt wird. Insbesondere dürfen hierbei keine Kopien der Daten in Betriebssystem-Papierkörben oder Datensicherungen verbleiben.
18. Sofern IT-Dienstleistungen an externe Stellen ausgelagert werden, werden von uns konkrete Sicherheitsanforderungen in den Service Level Agreements vorgegeben. Das Recht auf Kontrolle wird festgelegt.
19. Die Datenverarbeitung in einem vereinsfremden Cloud-Speicher ist nur zulässig, wenn deren Betreiber zertifizierter Auftragsverarbeiter im Sinne der DSGVO ist und der Verein mit dem Betreiber einen Vertrag zur Auftragsdatenverarbeitung geschlossen hat.
20. Für umfangreiche oder komplexe Outsourcing-Vorhaben erstellen wir ein detailliertes Sicherheitskonzept mit konkreten Maßnahmenvorgaben.
21. Papierakten sind verschlossen zu lagern und während der Benutzung gegen unbefugte Einsicht zu schützen.
22. Papierakten sind durch einen Standard-Shredder oder durch Verbrennung zu vernichten.

§ 18 Vereinseigene Systeme

(1) Für die Umsetzung der Sicherheitsmaßnahmen nach § 17 ist für vereinseigene Systeme der Vorstand verantwortlich.

(2) Der Vorstand kann einen Administrator oder die Benutzer der Systeme mit der Umsetzung der Sicherheitsmaßnahmen beauftragen. In diesem Fall hat der Vorstand die Ergebnisse der Umsetzung zu kontrollieren und die Einhaltung der Sicherheitsmaßnahmen kontinuierlich zu überwachen.

§ 19 Vereinsfremde Systeme

(1) Der Vorstand kann es insbesondere Abteilungsleitern, Trainern und Übungsleitern gestatten, Daten auf vereinsfremden Systemen zu verarbeiten. Solche Systeme umfassen unter anderem auch private PCs, Laptops, Tablets und Telefone der unter Satz 1 genannten Personen sowie Akten und Ablagesysteme in deren privaten Räumlichkeiten und Anlagen.

(2) Werden Daten auf einem vereinsfremden System verarbeitet, ist dessen Benutzer für die Umsetzung und Einhaltung der Sicherheitsmaßnahmen nach § 17 verantwortlich.

(3) Der Benutzer stellt sicher, dass die Daten auf einem separaten Konto verwaltet werden, wann immer dies möglich ist.

(4) Der Vorstand hat den Benutzer vereinsfremder Systeme über die Sicherheitsmaßnahmen zu belehren. Der Benutzer hat nach erfolgter Einrichtung des vereinsfremden Systems dem Vorstand die Umsetzung der Sicherheitsmaßnahmen unverzüglich zu bestätigen.

§ 20 Verbesserung der Sicherheit

(1) Das Managementsystem der Datensicherheit wird durch den Vorstand und den Datenschutzbeauftragten regelmäßig auf seine Aktualität und Wirksamkeit geprüft. Daneben werden auch die Sicherheitsmaßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Mitgliedern bekannt sind, ob sie umsetzbar und in den Betriebsablauf integrierbar sind.

(2) Der Vorstand unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mitglieder sind angehalten, mögliche Verbesserungen oder Schwachstellen an den Vorstand weiterzugeben.

(3) Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel

analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der IT-Sicherheitstechnik zu halten.

§ 21 Änderungen

(1) Der Vorstand kann diese Datenschutzrichtlinie jederzeit ändern, wenn gesetzliche Vorgaben dies erfordern oder die Änderung den Datenschutz im Verein verbessern.
(2) Bevor der Vorstand Änderungen vornimmt, konsultiert er den Datenschutzbeauftragten.
(3) Der Vorstand gibt die geänderte Datenschutzrichtlinie unverzüglich mit geeigneten Mitteln den Mitgliedern und Vertragspartnern bekannt.
(4) Die geänderte Datenschutzrichtlinie gilt in der dann neuen Fassung ab dem Tag der Bekanntgabe gemäß Absatz 3.