Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO

1. Angaben zum Verantwortlichen

1.1 Verantwortliche Stelle (Art. 4 Nr. 7 DSGVO)

Sport- und Spielverein Heidenau e.V.
Am Sportforum 5
01809 Heidenau

1.2 Gesetzlicher Vertreter

1. Vorsitzender: Frank Müller
   Adresse: Werner-Seelenbinder-Str. 5, 01809 Heidenau
   Tel.: 03529-5267286
   Mobil: 0160-5335531
   E-Mail: vorstand[at]ssvheidenau.de
2. Vorsitzender: Bernd Heinze
3. Schatzmeister: Kirsten Müller

1.3 Operativ verantwortlicher Ansprechpartner

Martin Leichsenring
Adresse: Ernst-Schneller-Straße 11, 01809 Heidenau
Tel.: 03529-5741516
E-Mail: martin[at]leichsenring-homepage.de

1.4 Datenschutzbeauftragter

Ein Datenschutzbeauftragter ist nicht bestellt, da die zugehörigen Tatbestände nach Artikel 37 DSGVO nicht vorliegen.

2. Grundsätzliche Angaben zur Verarbeitung

2.1 Bezeichnung der Verarbeitungstätigkeit

a) vereinsinterne Mitgliederverwaltung:
b) Datenerhebung von Besuchern des Internetauftrittes des Vereins:

2.2 Verantwortlicher Ansprechpartner

Martin Leichsenring
Adresse: Ernst-Schneller-Straße 11, 01809 Heidenau
Tel.: 03529-5741516
E-Mail: martin[at]leichsenring-homepage.de

2.3 Art der Verarbeitung / Name der Software

zu 2.1 a) Mitgliederverwaltung: Admidio (Vertrag zur Auftragsdatenverarbeitung mit Hoster)
zu 2.1 b) Google-Analytics (Vertrag zur Auftragsdatenverarbeitung mit Google)
zu 2.1 b) Log-Software des Hosters (Vertrag zur Auftragsdatenverarbeitung mit Hoster)

3. Allgemeine datenschutzrechtliche Anforderungen DSGVO

3.1 Zweckbestimmung

zu 2.1 a) vereinsinterne Mitgliederverwaltung:
- Nachweisführung der Teilnahme am Trainings- und Wettkampfbetrieb,
- Nachweis des Mitgliederbestandes gegenüber übergeordneten Verbänden zur Beantragung öffentlicher Zuschüsse und Förderungen
- Versicherungsnachweis im Rahmen der Sportversicherung des LSB

zu 2.1 b) Datenerhebung von Besuchern des Internetauftrittes des Vereins:
- persönliche Daten über Kontaktformular werden ausschließlich zur Beantwortung gestellter Anfragen verwendet.
- Daten über das Besucherverhalten (Herkunft, Verweildauer, aufgerufene Seiten, Wanderungsverlauf über die Homepage) werden im Rahmen von Google Analytics in anonymisierter Form erhoben und dienen ausschließlich der Optimierung des Internetauftrittes.
- Wir protokollieren sämtliche Zugriffe auf Inhalte unserer Webseite. Hierzu gehören die IP-Adresse, Datum und Uhrzeit des Zugriffes sowie die von unserer Seite abgerufenen Daten. Eine Verarbeitung dieser Daten erfolgt nur dahingehend, dass wir IP-Adressbereiche, von denen unberechtigte Zugriffe (Login-Versuche, Spamming) auf unsere Seite erfolgten, für künftigen Datenverkehr sperren.

3.2 Rechtmäßigkeit der Verarbeitung nach Art. 6 DSGVO
zu 2.1 a) Einwilligung / Einwilligung Sorgeberechtigter / Vertrag
zu 2.1 b) Wahrung berechtigter Interessen des Verantwortlichen

3.3 Datenschutz-Folgeabschätzung nach Art. 35 DSGVO
Es besteht durch die Verarbeitungstätigkeit kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen. Eine Datenschutz-Folgeabschätzung ist daher nicht erforderlich.

4. Erhebung der Daten

4.1 Kreis der betroffenen Personengruppen
Es werden zu folgenden Gruppen zur Erfüllung der Zweckbestimmung aufgeführten personenbezogene Daten bzw. Datenkategorien erhoben, verarbeitet und genutzt:
- Mitglieder des Vereins
- Interessenten an einer Mitgliedschaft
- Beschäftigte des Vereins
- Lieferanten des Vereins
- Mitarbeiter übergeordneter Verbände sowie öffentlicher Einrichtungen
- Besucher des Internetauftrittes

4.2 Art der gespeicherten Daten
- Abrechnungsdaten/Adressdaten
- Bankverbindungsdaten/Kreditkartendaten
- Geburtsdatum
- IT-Nutzungsdaten/Log Daten/Protokolldateien
- IP-Adresse
- Interessen/Präferenzen
- Kontaktdaten
- Lebenslauf
- Name/Vorname/Anrede/Titel
- Qualifikationsdaten
- sportartrelevante körperliche Beeinträchtigungen
- Standortdaten
- Vertragsdaten
- Vertragsstammdaten
- Zahlungsdaten
- Zeiterfassungsdaten

4.3 Herkunft der Daten
IP-Nutzungsdaten, IP-Adressen und damit verbundene Standortdaten werden vom Hoster erhoben, alle anderen Daten werden vom Betroffenen erhoben.

5. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können

5.1 Interne Empfänger
- Mitgliederverwaltung
- Buchhaltung
- IT-Sicherheit
- Übungsleiter

5.2 Externe Empfänger und Dritte
- **Öffentliche Stellen**, die Daten aufgrund gesetzlicher Vorschriften erhalten dürfen oder anfordern (z.B. Finanzbehörden, Stadt- und Kreisverwaltungen im Rahmen der Sportförderung, Sozialversicherungsträger, Aufsichtsbehörden).
- **Öffentliche Stellen der Strafverfolgung**, zur Wahrung eigener Interessen im Falle von Angriffen auf unser Internetangebot oder unsere IT.
- **Externe Stellen** (Auftraggeber und Auftragnehmer) im Rahmen der Auftragsdatenverarbeitung.
- **Weitere externe Stellen** wie z.B. Banken / Steuerberater / Rechtsanwälte (Soweit dies zur Erfüllung des Vertragsverhältnisses notwendig ist.)

6. Zugriffsberechtigte Personen

6.1 zugriffsberechtigte Personen
- Vorstandsmitglieder
- Verantwortlicher für Mitgliederverwaltung
- Verantwortlicher für Buchhaltung
- Verantwortlicher für IT-Sicherheit
- Übungsleiter

6.2 Berechtigungskonzept
- Vorstandsmitglieder sowie der/die Verantwortliche für die Mitgliederverwaltung erhalten Vollzugriff auf die von Mitgliedern erhobenen Daten.
- Der/die Verantwortliche für Buchhaltung erhält Zugriff auf die für die Beitragsberechnung und Verbuchung gezahlter Beiträge notwendigen Daten (Anschrift, Zugehörigkeit zu Beitragsgruppen und Abteilungen sowie Bank- und Zahlungsverkehrsdaten).
- Der/die Verantwortliche für IT-Sicherheit erhält Vollzugriff auf die von Mitgliedern erhobenen Daten (nur in Zusammenhang mit Gewährleistung der IT-Sicherheit der Mitgliederverwaltung).
- Übungsleiter erhalten eingeschränkten Zugriff auf Mitgliederdaten wie folgt: Notrufnummer der Eltern bei Minderjährigen, sportartrelevante körperliche Beeinträchtigungen.
- Der/die Verantwortliche für IT-Sicherheit erhält Vollzugriff auf die im Rahmen der Gewährleistung der IT-Sicherheit sowie der Reichweitenermittlung der Homepage erhobenen Daten von Besuchern.

7. Auftragsverarbeitung als Auftraggeber
Auftragsverarbeiter:
- 1&1 Internet SE

Auftragsbereich:
- Datenbank zur Mitgliederverwaltung
- Protokoll der Internetzugriffe (IT-Sicherheit)
- Vereinsinterner E-Mail-Verkehr
- Hoster für geschlossenen Benutzerbereich der Homepage

- Online-Datenspeicher

Verarbeitungsvertrag:
- AV-Vertrag nach BDSG

Eignung:
- zertifiziert nach ISO 27001

Standort:
- Deutschland

8. Datenübermittlung in Drittstaaten / internationale Organisationen

8.1 Übermittlung personenbezogener Daten
Die Übermittlung personenbezogener Daten in Drittstaaten findet ausschließlich nach schriftlicher Einwilligung des Betroffenen statt.

8.2 Drittstaaten / internationale Organisationen
Drittstaaten sind Länder außerhalb der EU / des EWR. Hierzu zählt unter anderem Japan (Sitz der Shotokan Karate-Do International Federation, Beantragungsstelle für DAN-Prüfungen, Organisation von Lehrgängen und Wettkämpfen). Zu weiteren Drittstaaten bestehen gegenwärtig keine Verbindungen des Vereins, die eine weitergehende Prüfung erforderlich machen. Sollten aufgrund sportlicher Verbindungen neue Drittstaaten hinzukommen, ist dieser Verfahrenspunkt entsprechend zu ergänzen.

8.3 angemessenes Datenschutzniveau
Die unter 8.2 namentlich aufgeführten Länder und Organisationen gewährleisten kein angemessenes Datenschutzniveau gemäß Angemessenheitsbeschluss der EU-Kommission (Art. 45 Abs. 3 DS-GVO). Eine Übermittlung personenbezogener Daten ist daher nur nach besonderer Prüfung vorzunehmen.

9. Regelfristen für die Löschung von Daten

9.1 Speicherdauer
Es bestehen vielfältige Aufbewahrungspflichten und -fristen. Nach Ablauf dieser Fristen werden die entsprechenden Daten routinemäßig gelöscht, wenn sie nicht mehr zur Vertragserfüllung erforderlich sind. Da persönliche Daten auch in der Buchhaltung und Veranstaltungsmanagement verwendet werden, hierzu nachfolgend weitere Erläuterungen:

Löschung nach 10 Jahren:
- Buchhaltungsdaten, also beispielsweise über die Zahlung von Mitgliedsbeiträgen oder die Erstattung von Auslagen.
- Teilnahmelisten an Veranstaltungen, welche über öffentliche Zuwendungen kofinanziert werden

Löschung nach 6 Jahren:
- Daten über Lohnabrechnungen und vergleichbare Vergütungen
- Geschäftsbriefe und E-Mails

Löschung nach 3 Jahren:
- Beitritts- und Kündigungserklärungen (Löschung erfolgt 3 Jahre nach Kündigung des Vereinsmitglieds)

Löschung nach 14 Monaten:
- anonymisierte Daten in Google Analytics

Daten, die nicht unter die vorstehenden Aufbewahrungsfristen fallen, werden gelöscht, sobald diese nicht mehr für den Zweck der ursprünglichen Speicherung benötigt werden. Dies betrifft beispielsweise unmittelbar nach Wirksamwerden der Kündigung Angaben zu Allergien oder körperlichen Beeinträchtigungen, Größenangaben für Teambekleidung, E-Mail-Adresse und Telefonnummer sowie die eventuelle Erfassung in internen Ergebnislisten.

9.2 technische Beschreibung der Datenlöschung
Personenbezogene Daten in automatisierten Datenverarbeitungssystemen werden durch Entfernen des entsprechenden Datensatzes gelöscht. Da zur Aufrechterhaltung der Datenintegrität und Datensicherheit jedoch von der Datenbank Sicherheitskopien gefertigt werden, setzt der Verein die sichere Löschung von personenbezogenen Daten wie folgt um:

- Sicherungskopien der Datenbank werden spätestens 3 Jahre nach Erstellung der Sicherung durch mehrfaches Überschreiben sicher gelöscht.
- einzelne personenbezogene Daten, die nicht in einem Datenverarbeitungssystem, sondern manuell erfasst wurden, wie eingescannte Dokumente, werden, sobald die Notwendigkeit für deren Speicherung entfällt, durch mehrfaches Überschreiben der einzelnen Datei sicher gelöscht.
- E-Mails, die personenbezogene Daten enthalten, werden durch Löschen und anschließendes Leeren des Ordners mit gelöschten Elementen gelöscht.
- Datenträger des Vereins, auf denen personenbezogene Daten gespeichert wurden, werden durch mehrfaches Überschreiben des gesamten Datenträgers sicher gelöscht, bevor eine Weitergabe an Dritte oder Entsorgung erfolgt.
- manuell erfasste oder dokumentierte personenbezogene Daten in Papierform werden zur Vernichtung gesammelt (hierbei weiterhin als zu schützende Daten behandelt) und vom Verein an ein zertifiziertes Unternehmen zur Aktenvernichtung überstellt. Soweit Funktionsträger des Vereins beruflich Zugriff auf entsprechend zertifizierte Unternehmen haben und auch im Rahmen ihrer Tätigkeit als Angestellter oder Selbständiger den Datenschutzbestimmungen unterliegen, darf sich der Verein der Dienste dieser Funktionsträger bedienen, um in Papierform vorhandene personenbezogene Daten einer gesicherten Vernichtung zuzuführen. Der entsprechende Nachweis der Vernichtung durch das zertifizierte Unternehmen ist dem Verein als Kopie zu überlassen.

10. Beurteilung der Angemessenheit technischer und organisatorischer Maßnahmen (TOM)

10.1 Allgemeine Beschreibung
Die Erfassung von Daten über die Homepage des Vereins, die Speicherung in der Vereinsverwaltung, die Verarbeitung im Zahlungsverkehr sowie die Übermittlung von Daten innerhalb des Vereins sowie an berechtigte Dritte erfolgt ausschließlich über gesicherte Verbindungen (SSL/TLS).
Der Zugriffsschutz für die Datenbank zur Mitgliederverwaltung wird durch ein System der Zugangsbeschränkung gewährleistet. Dies beinhaltet neben einer Sicherung über Benutzername und Passwort zusätzlich eine Beschränkung auf explizit zugelassene IP-Adressbereiche. Hierzu müssen Computer der Zugangsberechtigten für jeden einzelnen Zugangspunkt zum Internet (Provider) beim Verantwortlichen für IT-Sicherheit angemeldet werden. (deny from all, allow for separate). Für die gesicherte Übertragung zwischen Client und Server ist die Webadresse mit einem SSL-Zertifikat versehen. Im Rahmen der Auftragsverarbeitung erfolgt regelmäßig eine Kontrolle auf Schadcode.
Die Sicherheit der Verbindung zur öffentlichen Homepage wird durch ein SSL-Zertifikat hergestellt. Vereinsinterne Berichte und Fotosammlungen werden zusätzlich durch ein Passwort geschützt. Sämtliche Zugriffe auf die Homepage werden im Rahmen der

Auftragsverarbeitung (siehe Ziffer 7) protokolliert. Diese Protokolle werden regelmäßig auf Auffälligkeiten überprüft. Sofern bei den Überprüfungen festgestellt wird, dass Zugriffsversuche auf geschützte Bereiche oder Systemroutinen von Seiten nicht dazu Berechtigter erfolgt sind, erfolgt für Adressbereiche außerhalb der Europäischen Union die Sperrung des gesamten Adressbereiches (allow from all, deny from separates). Bei Zugriffsversuchen aus Adressbereichen der Europäischen Union erfolgt neben der Sperrung des Adressbereiches auch eine Sicherheitsmeldung an den jeweiligen Provider des Adressbereiches. Bei unerlaubten Zugriffsversuchen innerhalb Deutschlands erfolgt eine Sicherheitsmeldung an den Provider des Adressbereiches sowie in Kopie an das BSI. Der Adressbereich wird in diesem Fall nicht gesperrt.
Die Mitgliederdatenbank wird im Rahmen der Auftragsverarbeitung (siehe Ziffer 7) kontinuierlich gesichert. Zusätzlich werden vor jeder Veränderung der Programmversionen Komplettsicherungen des Gesamtprogramms sowie der Datenbank vorgenommen. Der Onlinespeicher wird regelmäßig auf Offline-Speichermedien gesichert.
Die Aufbewahrung von Daten in anderer als digitaler Form erfolgt in Räumlichkeiten mit Zugangsbeschränkung.
Alle Zugangsberechtigten des Vereins werden zur Einhaltung der Datenschutzbestimmungen verpflichtet.

10.2 verbleibendes Risiko
Trotz der unter 10.1 beschriebenen Maßnahmen besteht ein Restrisiko auf Verletzung des Schutzes personenbezogener Daten. Hierzu zählen neben menschlichen Fehlern auch das technische Versagen einzelner oder mehrerer Sicherungssysteme (Stichwort Symantec SSL-Gate).
Eine Erhöhung des Sicherheitsniveaus kann in erster Linie durch Verzicht auf die Erhebung sensibler Daten sowie den Verzicht auf Nutzung elektronischer Datenverarbeitungssysteme erreicht werden. Hierzu zählen:
- Anwesenheitspflicht für Erziehungsberechtigte an allen Trainingsstunden und (auch mehrtägigen) Lehrgängen mit minderjährigen Vereinsmitgliedern. Damit kann auf die Erfassung einer Notfall-Telefonnummer sowie von Angaben zu sportartrelevanten körperlichen Beeinträchtigungen verzichtet werden.
- Barzahlung aller Mitgliedsbeiträge und Startgelder.
- Erfassung von Teilnehmern an Trainingszeiten ausschließlich in Papierform.
- Mitgliederverwaltung durch ein System von Karteikarten
- Anschaffung eines Tresors entsprechender Sicherheitsstufe oder Anmietung eines Schließfaches für die karteikartengeführte Mitgliederverwaltung.
- Übermittlung von Mitgliederdaten an den Landessportbund ausschließlich in Papierform (beim LSB Sachsen nicht möglich).
- Anschaffung eines Aktenvernichters auf Vereinskosten.

Die vorstehend beschriebenen Maßnahmen zur Erhöhung der Datensicherheit sind in der Praxis nicht realisierbar. Eine Umsetzung dieser Maßnahmen würde letztlich dazu führen, dass der Verein sich nur noch mit dem Schutz personenbezogener Daten beschäftigt und keine Zeit mehr zur Verwirklichung der satzungsgemäßen Zwecke hätte. In der Folge wäre als sicherste Maßnahme zum Schutz personenbezogener Daten die Auflösung des Vereins zu empfehlen.

11. Stellungnahme durch den Datenschutzbeauftragten
Da der Verein nicht der Verpflichtung zur Bestellung eines Datenschutzbeauftragten unterliegt, entfällt eine entsprechende Stellungnahme.

12. Prüfung durch den Vereinsvorstand
Dieses Verzeichnis ist am 10.05.2018 durch den Vorstand geprüft und bestätigt worden.

© Quellenangabe und Weiterverwendung
Dieses Verzeichnis von Verarbeitungstätigkeiten wurde vom SFV Feuerblume e. V. übernommen und individuell angepasst (abgerufen am 25.05.2018).

Muster: "Dieses Verzeichnis von Verarbeitungstätigkeiten wurde erstellt unter Verwendung des Verzeichnisses von Verarbeitungstätigkeiten des Sport- und Spielvereins Heidenau e. V. und individuell angepasst."