



# **Datenschutzordnung**

des SV Eglöfs e.V.

Stand: 09. April 2018

## **A. Ziel der Datenschutzordnung**

Die Datenschutzordnung des SV Eglöfs hat zum Ziel, in einer zusammenfassenden Dokumentation die datenschutzrechtlichen Aspekte darzustellen. Dadurch soll die Einhaltung der europäischen Datenschutz-Grundverordnung (DSGVO) gewährleistet und der Nachweis der Einhaltung erbracht werden. Ziel ist es auch, durch die Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen ein Sicherheitsniveau zu erreichen, das für den normalen Schutzbedarf angemessen und ausreichend ist, um vereinsrelevante, insbesondere personenbezogene Daten bzw. Informationen zu schützen.

## **B. Präambel**

Der SV Eglöfs e.V. ist ein Sportverein bestehend aus mehreren Sparten, wovon einzelne Sparten auch teil-autonom wirtschaften und die dafür erforderlichen Daten verantwortlich pflegen. Die Führung des Vereins obliegt einem Vorstandsgremium aus 7 Vorständen, davon einem Vorstandsvorsitzenden. Der Vorstandsvorsitzende und einer der weiteren Vorstände sind vertretungsberechtigte Vorstände nach § 26 BGB.

Weitere Gremien des Vereins sind die Mitgliederversammlung und der Sportrat. Der Verein ist in Abteilungen und Sportgruppen gegliedert.

Zweck des Vereins ist die Förderung des Sports. Die unmittelbare Erfüllung des Vereinszwecks erfolgt in den Sportgruppen unter der Leitung von Übungsleitern oder Trainern.

Zuständiges Finanzamt ist Wangen i.A. Der Verein erfüllt die satzungsmäßigen Voraussetzungen nach den §§ 51, 59, 60 und 61 AO.

Der Verein ist im Vereinsregister des Amtsgerichts Ulm als gemeinnütziger Verein eingetragen (VR 620026).

Mit ca. 900 Mitgliedern ist der Verein datenschutzrechtlich großen Herausforderungen ausgesetzt, die mittels eines umfassenden Regelwerks zum Datenschutz gemäß DSGVO bzw. BDSG angenommen und bewältigt werden.

## **C. Datenschutzpolitik und Verantwortlichkeiten im Verein**

- 1) Datenschutz im SV Eglöfs soll einerseits die für eine optimale Vereinsführung und insbesondere die für die notwendige Mitgliederverwaltung erforderliche Bearbeitung von personenbezogenen Daten nicht behindern, andererseits den größtmöglichen Schutz dieser Daten sicherstellen. Dies soll erreicht werden durch
  - a) das Erzeugen eines Verantwortungsgefühls für den sorgfältigen Umgang mit personenbezogenen Daten bei allen Betroffenen im Verein;
  - b) klare Regelungen für den Umgang mit personenbezogenen Daten für alle Vereinsmitglieder;
  - c) durch enge Kontrolle der Datenverarbeitungsprozesse im Verein;
  - d) die auf das notwendige Minimum begrenzte Verarbeitung von personenbezogenen Daten.
  - e) den Schutz von Hard- und Software durch technische Maßnahmen.
  
- 2) Der Vorstandsvorsitzende des SV Eglöfs ist der erste Verantwortliche für den Datenschutz im Verein. Er legt in Absprache mit dem Vorstand die Datenschutzrichtlinien des Vereins fest. Der Vorstand erlässt die Datenschutzordnung des Vereins. Die Funktion eines

Datenschutzbeauftragten soll von einer Person außerhalb des Vorstands wahrgenommen werden. Ist dies nicht möglich, nimmt der Vorstandsvorsitzende oder eine von ihm benannte Person im Vorstand diese Funktion wahr.

- 3) Die Datenschutzordnung ist kontinuierlich zu überprüfen und gesetzlichen oder vereinsinternen Veränderungen anzupassen.
- 4) Alle mit der Verarbeitung von personenbezogenen Daten befassten Personen sind mit der Datenschutzordnung vertraut zu machen und zum sorgfältigen Umgang mit solchen Daten zu verpflichten. Wo notwendig sind Schulungen auf Kosten des Vereins durchzuführen.
- 5) Personenbezogenen Daten, die dem Vereinsmanagement anvertraut wurden, sind nicht über soziale Medien zu kommunizieren.

## **D. Rechtliche Rahmenbedingungen im Verein**

- 1) Die datenschutzrechtlichen Grundlagen für den SV Eglöfs e.V. sind die Satzung des Vereins, die Datenschutzgrundverordnung (DSGVO), gültig ab 25.05.2018, das Bundesdatenschutzgesetz (BDSG) in seiner jeweils aktuellen Fassung, sowie der BSI – Standard 100-2.
- 2) Weiterhin sind die Regelungen des Kinder- und Jugendschutzkonzepts des SV Eglöfs zu beachten.
- 3) Personenbezogene Daten dürfen nur zur Erfüllung des Vereinszwecks an eindeutig zweckdienliche Organisationen oder Personen weitergeleitet werden. Die Erfüllung der datenschutzrechtlichen Voraussetzungen beim Empfänger der Informationen ist vorher zu prüfen.

## **E. Dokumentation**

- 1) Der Schutzbedarf für die Datenverarbeitung im SV Eglöfs bezüglich Vertraulichkeit, Integrität und Verfügbarkeit wird gemäß BDI Standard 100-2 als NORMAL bewertet, d.h.:
  - a) Der Schutz von Informationen, die nur für den internen Gebrauch bestimmt sind, muss gewährleistet sein.
  - b) Kleinere Fehler können toleriert werden. Fehler, die die Aufgabenerfüllung erheblich beeinträchtigen, müssen jedoch erkenn- oder vermeidbar sein.
  - c) Längere Ausfallzeiten, die zu Terminüberschreitungen führen, sind nicht zu tolerieren.
  - d) Der Schutz personenbezogener Daten muss gewährleistet sein. Anderenfalls besteht die Gefahr, dass der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt wird.
- 2) Für die Definition von personenbezogenen Daten gilt § 3 Abs. 1 des BDSG<sup>1</sup>.
- 3) Im SV Eglöfs werden personenbezogene Daten für folgende Zwecke genutzt:
  - a) Führen der Mitgliederliste des Vereins zum Zweck
    - i) der Beitragsbemessung (Geburtsdatum, Familienverhältnisse)
    - ii) der Sportgruppenzuteilung (Geschlecht, Alter)
    - iii) des Beitragseinzugs (Kontodaten)
    - iv) von Ehrungen (Eintrittsdatum)

---

<sup>1</sup> Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (Betroffener).

- b) Führen von Abteilungs- und Gruppenlisten und deren periodischer Abgleich mit der Mitgliederliste.
- c) Führen der Übungsleiter- bzw. Trainerlisten
- d) Meldungen an Sportverbände zwecks Mannschaftsaufstellungen
- e) Meldungen an Behörden (z.B. BGB § 26 Vorstände)
- f) Mitteilungen an Banken zwecks Vollmachtserteilung und Online-Banking
- g) Prüfung von geeigneten Bewerbern für die Kinder- und Jugendarbeit (Führungszeugnisse)

## **F. Bestehende technische und organisatorische Maßnahmen (TOM)**

- 1) Personenbezogene Daten, die ein Vereinsmitglied dem Vorstand oder weiteren autorisierten Personen zur Nutzung für dem Vereinszweck dienlichen Aufgaben überlässt, genießen Vertrauensschutz. Die betroffene Person ist über die vorgesehene Nutzung in Kenntnis zu setzen und muss der Nutzung schriftlich zustimmen.
- 2) Mitgliederdaten werden, wie von den jeweiligen Betroffenen durch die Beitrittserklärung übermittelt, zentral in einer Mitgliederliste unter Nutzung eines Vereinsmanagementprogramms gespeichert. Weitere Daten werden für Übungsleiter(innen) / Trainer(innen) erhoben und ebenfalls im Vereinsmanagementprogramm gespeichert. Diese Daten bilden die Grundlage für das personenbezogene Vereinsmanagement und sind nur für die o.g. Zwecke zu nutzen. Die für die Mitgliederliste verantwortliche Person (Vorstand Logistik und Mitgliederverwaltung) stellt eine regelmäßige Datensicherung sicher.
- 3) Die Speicherung der personenbezogenen Daten erfolgt auf einer Online-Plattform (Pro-Winner) und ist durch die individuelle Zuteilung und Nutzung von Passwörtern geschützt. Kopien dürfen für die o.g. Zwecke (siehe E.3)) erstellt werden und sind nur an autorisierte Vereinsfunktionäre auszuhändigen. Der Inhalt von Kopien von Datensätzen ist auf die absolut notwendigen personenbezogenen Daten zu beschränken.
- 4) Autorisierte Nutzer und deren Datenempfangs- und Datenverarbeitungsprivilegien
 

a) Vorstandsvorsitzender	Alle Daten
b) Vorstand Finanz & Rechnungswesen, zgl. Stv VV	Alle Daten
c) Vorstand Logistik und Mitgliederverwaltung	Alle erforderlichen Mitgliederdaten
d) Weitere Vorstände	Funktionsorientierte Mitgliederdaten
e) Abteilungsleiter und Gruppenleiter	Funktionsorientierte Mitgliederdaten
f) Jugendleiter / Spielleiter	Funktionsorientierte Mitgliederdaten
g) Referent für Öffentlichkeitsarbeit	Zweckorientierte Mitgliederdaten
h) Schriftführer(in)	Zweckorientierte Mitgliederdaten
i) Kassenwarte der selbständigen Abteilungen	Zweckorientierte Mitgliederdaten
- 5) Zugangssteuerung
  - a) Pro-Winner: Zugang zur Pro-Winner Plattform wird autorisierten Nutzern gemäß F.4) auf der Basis „nur bei Bedarf“ gewährt. Der Zugang erfolgt über eine „Remote Desktop“ Applikation und individuellen Zugangsdaten (Benutzerkennwort und Passwort).

- b) Geschäftsstellen-PC: Zugang wird grundsätzlich nur den autorisierten Nutzern gem. F.4) a – d und g-h gewährt. Zugang zur Windows Oberfläche erfolgt über ein einheitliches Passwort. Ordnergruppen sind individuell mit Passwort zu sichern.
- c) Online-Banking: Zugang wird nur den autorisierten Nutzern gem. F. 4) a, b und i gewährt, wobei die Bank-internen Regelungen zu beachten sind (VV ist in der Regel der Kontoinhaber, der seinerseits weitere Bevollmächtigte benennen kann).
- d) Homepage des SV Eglöfs: Zugang zwecks Datenpflege wird nur dem Webmaster (F.4 g) und dem Vorstandsvorsitzenden gewährt.
- e) Email: Vereinsfunktionäre nutzen für elektronische Kommunikation die für diesen Zweck durch den Verein betriebene Plattform des Betreibers STRATO. Das Nutzungsverfahren ist in der Geschäftsordnung des SV Eglöfs festgelegt und gilt in dieser Form auch für die Datenschutzordnung des Vereins.
- f) Weitere externe Plattformen: Nutzung nur bei ausreichender Gewährleistung des Datenschutzes. Es gelten die Zugangssteuerungsregeln der Plattformbetreiber. Soziale Medien stellen derzeit für den SV Eglöfs keinen ausreichenden Schutz personenbezogener Daten sicher und sind deshalb nicht als Kommunikationsmittel für die Übertragung von personenbezogenen Daten zu nutzen.
- g) Personenbezogene Daten, die im Rahmen der Tätigkeit der/des Beauftragten für den Kinder- und Jugendschutz gesammelt werden, genießen besonderen Vertrauensschutz und sind nur dem unmittelbaren gemäß Kinder- und Jugendschutzordnung des SVE festgelegten Personenkreis zur Einsicht zugänglich zu machen.

## 6) Informationsklassifizierung (und deren Handhabung)

- a) **Alle personenbezogenen Daten bzw. Informationen sind grundsätzlich als vertrauliche Daten zu behandeln.** Die Veröffentlichung von solchen Daten / Informationen bedarf zwingend der Zustimmung der betroffenen Person oder des/der gesetzlichen Vertreter(s).
- b) Nicht-personenbezogene Daten bzw. Informationen sind so zu behandeln, dass durch ihre Veröffentlichung keine Rufschädigung des Vereins entstehen kann. Öffentlichkeitsarbeit erfolgt grundsätzlich nur über den Referent für Öffentlichkeitsarbeit, der sich mit dem Vorstandsvorsitzenden über veröffentlichungsfähige Informationen verständigt.
- c) Informationen, die im Rahmen des Internetauftritts des Vereins publiziert werden, können entweder als Informationen für die Mitglieder oder Informationen für die Allgemeinheit klassifiziert werden. Die Zuteilung nimmt der Referent für Öffentlichkeitsarbeit in Absprache mit dem Vorstand vor. Informationen, die nur für die Mitglieder bestimmt sind, sind in einem dafür reservierten Bereich abzulegen und durch Passwort zu schützen.
- d) Protokolle und andere schriftliche Dokumente sind grundsätzlich nicht für die Veröffentlichung vorgesehen und unterliegen dem vertraulichen Umgang innerhalb der jeweiligen Gremien des Vereins. Über die auszugswise Veröffentlichung von Protokolldaten oder Inhalten anderer interner Dokumente entscheidet der Vorstandsvorsitzende, ggf in Abstimmung mit dem Vorstand und den beteiligten Personen.

## 7) Physische und umgebungsbezogene Sicherheit

- a) Der PC der Geschäftsstelle ist gegen Diebstahl zu sichern. Dazu zählt in erster Linie das Absperrern des Vereinsraumes durch alle Personen, die Schlüssel für den Raum erhalten haben.

- b) Alle autorisierten Nutzer können Online-Anwendungen für das Vereinsmanagement auch über private Computer nutzen (Home-Office). Dabei verpflichten sich diese Anwender darauf zu achten, dass nicht-autorisierte Personen keinen Zugang zu den verarbeiteten Daten erhalten. Kopien der Online-Daten des Vereins auf privaten Computern (einschl. Smartphones) für private Zwecke sind strikt untersagt.
- c) Für die Weitergabe von Vereinsinformationen, insbesondere von vertraulichen Informationen und Daten, ist die Vereins-Email-Plattform STRATO zu nutzen. Der Empfängerkreis von Informationen ist immer auf das notwendige Minimum zu begrenzen.
- d) Werden Personallisten in Papierform weitergereicht, sind diese an einem sicheren, nicht für Unbefugte zugänglichen Ort aufzubewahren und nach Abschluss der Nutzung zu vernichten (Schreddern oder verbrennen).

#### 8) Anweisung für Endanwender

Endanwender sind die unmittelbaren Nutzer von Informationen. Sie verarbeiten die Daten strikt nur für den Zweck, für den ihnen die Daten überlassen wurden. Dazu zählen:

- a) der Datenabgleich zwischen Mitgliederverwaltung und den einzelnen Sportgruppen,
- b) die erforderliche Datenübertragung für die Anmeldung zu Wettkämpfen und anderen sportlichen Ereignissen, die im Vereinsinteresse stehen,
- c) die Erhebung der Mitgliederbeiträge und anderer autorisierter Finanztransaktionen,
- d) die Meldung von Sportunfällen an die Sportversicherung des Vereins,
- e) die Meldung weiterer Versicherungsfälle im Verein,
- f) der Austausch von Finanzdaten mit dem Steuerberater und dem Finanzamt,
- g) die Übertragung von Mitgliederdaten an den WLSB zum Nachweis der Förderungswürdigkeit von Kooperationen und Lizenzen,
- h) die Herausgabe von Mitgliederdaten auf Verlangen des jeweiligen Mitglieds. Dies beinhaltet auch Informationen über alle im Familienbeitrag dieses Mitglieds gelisteten Mitglieder,

#### 9) Einschränkung von Software Installation und -verwendung

Auf Vereinscomputern ist Soft- und Hardware nur durch den IT-Administrator zu installieren. Dies betrifft nicht die Installation von Updates von bereits installierter Software, die auch von jedem autorisierten Nutzer vorgenommen werden kann, sofern sie/er die nötigen Kenntnisse für eine derartige Maßnahme besitzt.

#### 10) Datensicherung

- a) Nach jeder Session zur Aktualisierung der ML ist eine Datensicherung durch die für die ML zuständige Person vorzunehmen,
- b) IT-Admin stellt sicher, dass mindestens 14-tägig für alle auf dem Vereins-PC genutzten datenverarbeitenden Programmen eine Datensicherung durchgeführt wird.

#### 11) Informationsübertragung

Für vertrauliche Informationen hat die Informationsübertragung möglichst verschlüsselt zu erfolgen.

#### 12) Schutz vor Schadsoftware

- a) Zum Schutz vor Schadsoftware ist auf allen Geräten, auf denen Vereinsinformationen verarbeitet werden, ein aktuelles Schadsoftware-Abwehrprogramm zu betreiben. Jede Information, die von einem privaten Computer auf den Vereins-PC übertragen werden soll, ist vor dem Speichern auf Schadsoftware zu überprüfen.
- b) Zur Verhinderung der versehentlichen Speicherung von Schadsoftware ist auf dem Vereins-PC eine „Firewall“ zu installieren.
- c) Verdächtige Emails sind sofort zu löschen bzw. in den SPAM-Ordner zu verschieben.

### 13) Handhabung technischer Schwachstellen

Wird nachgereicht.

### 14) Kommunikationssicherheit

Zusätzlich zu den bereits beschriebenen Schutzmaßnahmen zur Vermeidung von Datenlecks ist bei der Kommunikation mittels Telefon darauf zu achten, dass personenbezogene Daten nicht beiläufig von beistehenden Personen aufgefasst werden können.

### 15) Privatsphäre und Schutz von personenbezogenen Informationen

Der Schutz der Privatsphäre eines jeden Mitglieds hat oberste Priorität bei der Verarbeitung von Informationen für Vereinszwecke, insbesondere bei der Verarbeitung von personenbezogenen Informationen. Jedes Vereinsmitglied, das aufgrund seiner Funktion im Verein mit der personenbezogenen Informationsverarbeitung beauftragt ist, muss sich stets bewusst sein, welchen Schaden sie oder er anrichten kann, wenn durch Sorglosigkeit vertrauliche Informationen an die Öffentlichkeit geraten. Insbesondere bei grob fahrlässiger oder gar vorsätzlicher Verletzung der Sorgfaltspflicht im Umgang mit personenbezogenen Daten muss jeder Einzelne mit empfindlichen Strafen rechnen. Die Reputation des Vereins kann durch mangelnde Seriosität empfindlich verletzt werden.

### 16) Regelmäßige Überprüfung und Bewertung der Informationssicherheit

- a) Datenverarbeitungsvorgänge und Maßnahmen zum Datenschutz sind laufend zu überprüfen und, wo nötig, zu aktualisieren.
- b) Technische Mittel sind im Rahmen des finanziell Möglichen und unter Berücksichtigung des Verhältnismäßigkeitsprinzips zu nutzen.
- c) Organisatorische und strukturelle Maßnahmen sind stets auch unter dem Gesichtspunkt des Informations- bzw. Datenschutzes und der Informations- bzw. Datensicherheit zu betrachten.

### 17) Diese Datenschutzerklärung wurde am 09.04.2018 vom Vorstand gebilligt und tritt mit sofortiger Wirkung in Kraft.

Offinger  
Vorstandsvorsitzender