

VfL Herrenberg
Schießmauer 6
71083 Herrenberg



Datenschutzrichtlinie des VfL Herrenberg e.V.

Zweck

Dieses Dokument soll haupt- und ehrenamtlichen Mitarbeiter des Vereins mit den wesentlichen Bestimmungen des Datenschutzes vertraut machen. Darüber hinaus werden einige Empfehlungen gegeben, wie Sie im Umgang mit personenbezogenen Daten Verstöße gegen Datenschutzgesetze und interne Regelungen vermeiden können.

Zielgruppe

Alle Mitarbeiter im VfL Center, (Geschäftsstelle und Fitness- und Gesundheitsstudio) und sämtliche ehrenamtliche Mitarbeiter in den Abteilungen, insbesondere Abteilungsleiter, Kassier, Jugendleiter und Schriftführer, sofern sie im Rahmen ihrer Tätigkeit personenbezogene Daten verarbeiten.

1 Datenschutz

Personenbezogene Daten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person, z.B. Name, Vorname, Geburtsdatum und Ort, Wohnanschrift, Rufnummer, Mailadressen, Bankverbindung oder Vereinstätigkeiten. Das Datenschutzrecht kennt keine frei verwendbaren, personenbezogenen Daten.

Personenbezogene Daten unterliegen hohen Sicherheitsanforderungen. Der VfL Herrenberg e.V. verfolgt einen einheitlich hohen Datenschutz durch den Abschluss und die Umsetzung dieser Datenschutzrichtlinie. Diese bietet die Grundlage hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten von Personen.

1.1 Grundsätze des Datenschutzes

Personenbezogene Daten müssen

- nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden;
- für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und dürfen nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden;
- den Zwecken entsprechen, für die sie erhoben und / oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen;
- sachlich richtig und aktuell sein;
- nach Realisierung der Zwecke, für die sie erhoben oder weiter verarbeitet wurden, gelöscht oder anonymisiert werden.

1.2 Zulässigkeit der Verarbeitung und Nutzung personenbezogener Daten

Das Erheben und Verarbeiten von personenbezogenen Daten bedarf entweder einer Rechtsvorschrift, einem Vertragsverhältnis oder der eindeutigen Einwilligung der Betroffenen. Eine Übermittlung an Dritte ist ohne diese Erlaubnistatbestände nicht zulässig.

Beim VfL Herrenberg ergibt sich die Zulässigkeit entweder aus der Vereinsmitgliedschaft oder dem Vertragsverhältnis im Sportbetrieb.

Die Empfänger von personenbezogenen Daten dürfen Sie nur für den Zweck verarbeiten oder nutzen, für den Sie ihnen von der verantwortlichen Stelle zur Verfügung gestellt wurden.

Die Daten dürfen nur zweckgebunden verwendet werden und sind nach Zweckerfüllung oder nach Ablauf der Aufbewahrungsfrist zu löschen.

1.3 Maßnahmen zur Gewährleistung des Datenschutzes

Der VfL Herrenberg e.V. ist verpflichtet, angemessene technische und organisatorische Maßnahmen zu treffen, um den Schutz der Daten zu gewährleisten. Grundsätzlich sind alle personenbezogenen Daten vor Verlust, Manipulation, aber auch vor unbefugter Einsichtnahme zu schützen. Speziell für die automatisierte Datenverarbeitung gibt es gesetzliche Anforderungen, die der Datensicherheit dienen (z. B. Zugangskontrolle, Zugriffskontrolle, Eingabekontrolle, Weitergabekontrolle). Im Bereich der Zentralen Datenverarbeitung beim VfL Herrenberg wurden umfangreiche Maßnahmen ergriffen, die den Anforderungen des Gesetzes Genüge tun.

Besondere Aufmerksamkeit erfordert der Einsatz von Personal-Computern bei der Verarbeitung personenbezogener Daten, da die Schutzmöglichkeiten für Daten hier im Allgemeinen geringer sind als bei zentralen EDV-Anlagen. Die Verantwortung dafür tragen die jeweiligen Benutzer.

Eine wesentliche Datenschutzmaßnahme liegt in der Datenvermeidung und Datensparsamkeit:

Erheben, verarbeiten und nutzen Sie so wenig personenbezogene Daten wie möglich. Belassen Sie die Daten in den Netzwerksystemen des VfL Herrenberg. Alle unter Zielgruppe genannten Mitarbeiter sind vom Verein auf das Datengeheimnis hin informiert und hierzu verpflichtet. Sie haben auf die Einhaltung der nationalen Vorschriften und Gesetze und der vereinsintern getroffenen Datenschutzregelungen zu achten. Die Mitarbeiter sind persönlich für die Einhaltung der Gesetze verantwortlich.

In Deutschland ist die Berufung eines Datenschutzbeauftragten gesetzlich vorgeschrieben. Ihm obliegt es, auf die Einhaltung aller Bestimmungen der Gesetze hinzuwirken. Hier sind lokal die entsprechenden Vorschriften zu beachten.

2 Empfehlungen

Mitarbeiterinnen und Mitarbeiter, die mit personenbezogenen Daten zu tun haben, sollten folgende Richtlinien beachten:

2.1 Zweckbindung

Erfassen und verarbeiten Sie nur personenbezogene Daten, die Sie zur Erfüllung der Ihnen übertragenen Aufgabe benötigen. Handeln Sie nach dem Prinzip der Datenvermeidung und Datensparsamkeit:

Vermeiden Sie die Erzeugung von Kopien in andere Systeme oder auf andere Datenträger, da für diese Kopien nicht mehr der umfassende Schutz des Originalsystems gewährleistet werden kann, insbesondere ist das Einhalten von Löschrufen nicht mehr kontrolliert möglich.

Löschen Sie personenbezogene Daten, sobald ihre Kenntnis für die Zweckerfüllung der Speicherung nicht mehr erforderlich ist. Löschen Sie insbesondere nach Ende der Aufbewahrungsfrist.

2.2 Datenqualität und Verhältnismäßigkeit

Halten Sie die Daten sachlich richtig und aktuell. Sie dürfen im Hinblick auf die Zweckbestimmung nicht exzessiv sein.

2.3 Transparenz

Erheben Sie nur Daten mit Kenntnis der Betroffenen oder wenn die Speicherung durch Gesetz oder Vertrag vorgesehen ist. Andernfalls sind die Betroffenen bei der erstmaligen Speicherung über die Art der Daten, den Zweck der Erhebung und die Identität der verantwortlichen Stelle zu benachrichtigen.

2.4 Sicherheit und Vertraulichkeit

- Ergreifen Sie Schutzvorkehrungen gegen die Risiken der Verarbeitung: Verhindern Sie jeglichen Missbrauch Ihres Benutzernamens. Verwenden Sie sichere Passwörter und geben Sie diese auf keinen Fall weiter.
- Verlassen Sie Ihre Arbeitsgeräte nicht ohne ordnungsgemäße Beendigung oder Sperrung der Sitzung (Ctrl – Alt – Del -> Lock). Verwenden Sie Bildschirmschoner mit automatischem Passwort-Schutz nach kurzer Zeit.
- Wenn Ihr PC auch anderen zugänglich ist: Stellen Sie sicher, dass auf der lokalen Festplatte keine personenbezogenen Daten gespeichert sind, z.B. durch Verwendung eines Ordners auf dem zentralen Dateiserver (Homedrive) oder eines besonders geschützten Abteilungs-Servers. Prinzipiell müssen auch in solchen Fällen - soweit der Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht - die Forderungen des Gesetzes erfüllt werden.
- Sorgen Sie dafür, dass nur Berechtigte Einblick in Ihre Unterlagen nehmen können. Halten Sie auch Datenträger mit personenbezogenen Daten wie vertrauliche Unterlagen unter Verschluss.
- Stellen Sie sicher, dass nicht mehr benötigte Unterlagen, soweit Sie sie nicht selbst vernichten können, kontrolliert entsorgt werden (Shredder, verschlossene Abfall-Container).
- Kopieren Sie keine personenbezogenen Daten aus dem Netzwerksystem auf eigene Datenträger über Download, Cut & Paste, Screenshots usw., wenn es nicht ausdrücklich im Verarbeitungsprozess vorgesehen ist.
- Nutzen Sie bei der internen und externen Kommunikation von Daten mit hohem Vertraulichkeitsgrad (Geschäftsgeheimnisse oder sensible personenbezogenen Daten) sichere Medien. Unverschlüsselte E-Mails, offene Hauspost oder Faxverkehr sind nicht dafür geeignet.

2.5 Recht auf Auskunft, Berichtigung, Löschung und Widerspruch

Betroffene Personen haben das Recht, Auskunft über ihre Daten zu verlangen und sachlich unrichtige Daten berichtigen, sperren oder löschen zu lassen.

Wenden Sie sich bei allen Auskunftersuchen von Betroffenen, die über die an Ihrem Arbeitsplatz üblichen Routineanfragen hinausgehen an die Geschäftsführung oder den Beauftragten für den Datenschutz. Dieser wird veranlassen, dass die Auskunft dem Gesetz entsprechend gegeben wird.

2.6 Beschränkung der mündlichen Weiterübermittlung

Geben Sie an Stellen außerhalb des Unternehmens auch keine mündlichen Auskünfte über Daten einzelner Personen, es sei denn, es bestehen besondere Anweisungen hierzu.

Geben Sie aus Ihren Unterlagen nur eindeutig Berechtigten innerhalb des Vereins, des Verbandes oder einer berechtigten Behörde Auskünfte.

2.7 Besondere Datenkategorien

Besonders sensitive wie zum Beispiel rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, etc. werden beim VfL Herrenberg nicht erfasst oder verarbeitet.

Im Zusammenhang mit der Gesundheitsversorgung im Fitness- und Gesundheitsstudio werden medizinische Daten nur nach Zustimmung durch die betroffene Person erhoben und verwaltet.

2.8 Direktmarketing

Die Betroffenen müssen jederzeit die Möglichkeit zum „opt-out“ haben, um sich gegen die Verwendung ihrer Daten für diese Zwecke zu entscheiden.

2.9 Bußgeldvorschriften

Bitte beachten Sie, dass Verletzungen des Datenschutzes abhängig von nationalen Gesetzen zu Ordnungswidrigkeiten oder gar Straftatbeständen führen können.

In Deutschland liegt z.B. eine Ordnungswidrigkeit vor, wenn unbefugt personenbezogene Daten gespeichert werden oder wenn Daten für andere Zwecke genutzt werden. Ordnungswidrigkeiten können hier mit einem Bußgeld bis zu € 250.000 geahndet werden. Werden diese Handlungen gegen Entgelt begangen oder in der Absicht, sich zu bereichern oder andere zu schädigen, liegt eine Straftat vor, die mit Freiheitsstrafe bis zu zwei Jahren bestraft werden kann.