DATENSCHUTZKONZEPT

DER PONY EVENTS FEDERATION E.V.

REVISION 1.2
04.12.2019

Versionshistorie

05.05.2018	Angelegt	LS
25.11.2019	Neufassung	LS
04.12.2019	Änderung Benutzerverwaltung, Rollenkonzept, Mitgliederverwaltung	LS

INHALTSVERZEICHNIS

GELTUNGSBEREICH

Diese Richtlinie regelt die datenschutzkonforme Informationsverarbeitung und die entsprechenden Verantwortlichkeiten bei der Pony Events Federation mitsamt aller angehörigen Veranstaltungs- und Querschnittteams. Alle aktiv tätigen Mitglieder und Mitarbeiter sind zur Einhaltung dieser Richtlinie verpflichtet.

Sie richtet sich insbesondere an:

- Vorstandsmitglieder
- Mitarbeiter und Teamleiter der Veranstaltungs- und Querschnittteams
- Veranstaltungshelfer
- PR- und Kommunikationsbeauftragte
- Revisoren und mit übrigen Vereinsämtern bzw. Vereinsaufgaben betraute Mitglieder

Hierbei gelten folgende Grundsätze:

- Die Datensicherheit ist wichtiges Vereinsziel und stets zu berücksichtigen.
- Die Freiwilligkeit der Datenabgabe ist oberstes Datenschutzprinzip. Daten werden in aller Regel nur erhoben, soweit die betroffene Person aktiv einwilligt.
- Es sind so wenige Daten wie möglich zu erheben. Erhobene Daten sind so schnell wie möglich zu löschen.
- Anonymisierung und Pseudonymisierung sind, wenn möglich, zu nutzen.
- Markt- und Meinungsforschung sind nachrangig zu betrachten und dürfen nur unter Verwendung anonymisierter Daten betrieben werden.
- Wir versenden keine personalisierte Werbung und nutzen keine Newsletter. Unaufgeforderte Kundenkontakte finden nicht statt.
- Leitende Mitglieder und Mitarbeiter berücksichtigen stets Datenschutzinteressen und prüfen regelmäßig die Prozesse und Datenbestände in ihrem Aufgabenbereich.
- IT-Fachverfahren u.ä. werden vor der Nutzung bzw. Auswahl nach Datenschutzbelangen geprüft.
- Besonders schützenswerte personenbezogene Daten werden nicht erhoben, soweit es nicht Interesse der betroffenen Person unbedingt erforderlich ist.

Zu beachten ist, dass die Regelungen nicht nur für die Verarbeitung personenbezogener Daten Dritter, sondern auch für die Verarbeitung personenbezogener Daten der Mitglieder und Mitarbeiter gelten.

BEGRIFFSDEFINITIONEN

PERSONENBEZOGENE DATEN

Einzelangaben über persönliche oder sachliche Verhältnisse einer natürlichen Person (Betroffener); alle Daten, die einen Rückschluss auf die betroffene Person zulassen.

Beispiele: Name, Vorname, Geburtstag, Adressdaten, Bestelldaten, E-Mail-Inhalte.

Achtung: Daten sind personenbezogen, wenn sie sich einer Person zuordnen lassen. Dies kann auch der Fall sein, wenn zwar nicht der Name angegeben wird, aber ein bekannter Spitzname oder ein technisches Merkmal wie z.B. eine IP-Adresse.

BESONDERE PERSONENBEZOGENER DATEN

Angaben über rassische, ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

VERANTWORTLICHE STELLE

ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

Zu den Begriffsbestimmungen wird im Übrigen auf die Regelungen der DSGVO sowie des BDSG verwiesen.

DER BETRIEBLICHE DATENSCHUTZBEAUFTRAGTE

Die Pony Events Federation hat nach Maßgabe der §§ 4f und d BDSG einen betrieblichen Datenschutzbeauftragten (DSB) bestellt.

Es handelt sich um den Schatzmeister (Lukas Sanders).

Dieser nimmt die ihm kraft Gesetzes und aus dieser Richtlinie zugewiesenen Aufgaben bei weisungsfreier Anwendung seiner Fachkunde wahr.

Für Meldungen, Auskünfte etc. gegenüber den Datenschutzaufsichtsbehörden ist allein der DSB zuständig. Die Fachabteilungen stellen die hierfür erforderlichen Informationen, Unterlagen etc. zur Verfügung. Gleiches gilt für Anfragen, Beschwerden oder Auskunftsersuchen.

Jeder Mitarbeiter und jedes Mitglied sich unmittelbar mit Hinweisen, Anregungen oder Beschwerden an den DSB wenden, wobei auf Wunsch absolute Vertraulichkeit gewahrt wird.

Der DSB darf aufgrund dieser Richtlinie Anordnungen zur Umsetzung datenschutzrechtlicher Anforderungen, insbesondere zur Beseitigung von Risiken, erlassen.

ERHEBEN, VERARBEITEN UND NUTZEN PERSONENBEZOGENER DATEN

Personenbezogene Daten werden nur erhoben und verarbeitet, soweit dies zur Erfüllung der Vereinsaufgaben erforderlich ist. Hierbei sind als Verarbeitungszwecke insbesondere zu nennen

- Durchführung von Veranstaltungen
    - Verkauf von Eintrittskarten einschließlich Abwicklung des Vertragsverhältnisses
    - Bearbeitung von Besucheranliegen und Anfragen (Support)
    - Abwicklung des Zahlungsverkehrs
    - Betrieb von Web-Präsenzen
    - Durchführung von Zufriedenheitsbefragungen
    - Anwerbung und Anmeldung von Helfern
    - Anwerbung und Anmeldung von Beitragenden, Musikern und sonstigen Partnern
    - Kommunikation über soziale Medien
- Mitgliederverwaltung
    - Beitritte und Austritte
    - Mitgliederkommunikation
    - Durchführung von Mitgliederversammlungen
- Interne Verwaltung
    - Abwicklung der Buchführung und des Controllings
    - Planung, Steuerung und strategische Entscheidungsfindung
    - Erfüllung gesetzlicher Pflichten

VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN

Verarbeitungstätigkeit ist jeder Prozess, gleich ob EDV-gestützt oder nicht, in welchem personenbezogene Daten verarbeitet werden. Hierzu zählen unter anderem auch alle Anmelde- und Registrierungsprozesse, die Annahme von Anfragen über Formulare auf Webseiten oder die Abwicklung von Verträgen.

Der Vorstand führt ein Verzeichnis der Verarbeitungstätigkeiten und Verfahren (siehe Anhänge), in welchen er eine Prozessbeschreibung, die eingesetzten IT- (Fach-) Verfahren, die betroffenen Personen, die erhobenen Daten und den Zweck der Verarbeitung verzeichnet. Ebenfalls soll dort verzeichnet werden, ob und in welcher Form Daten übermittelt werden, wie die Löschungsfrist für die erhobenen Daten ist und welche Sicherheitsmaßnahmen getroffen werden, um das Verfahren abzusichern.

Die Verarbeitung produktiver Daten darf erst begonnen werden, wenn die Aufnahme in das Verzeichnis der Verarbeitungstätigkeiten und Verfahren aufgenommen wurde.

Teamleiter der Veranstaltungs- und Querschnittteams bedürfen vor Einführung der Zustimmung eines Vorstandsmitglieds.

Der Vorstand evaluiert das Verzeichnis regelmäßig, mindestens einmal im Jahr, und bewertet die eingesetzten Verfahren kritisch nach datenschutzrechtlichen Aspekten. Er wirkt darauf hin, dass nicht mehr benötigte Verfahren unverzüglich abgeschaltet und riskante Verfahren unverzüglich ersetzt werden.

ZUGÄNGE ZU PERSONENBEZOGENEN DATEN

Als Zugang zu personenbezogenen Daten zählen alle faktischen Zugangsmöglichkeiten, insbesondere aber auch Benutzerkonten zu Verfahren, Web-Diensten und Software, in welchen personenbezogene Daten verarbeitet werden.

Alle Personen, die einen Zugang zu personenbezogenen Daten erhalten, werden durch den DSB über datenschutzrechtliche Grundsätze belehrt und auf die Einhaltung des Datengeheimnisses verpflichtet. Die Belehrung kann auch über das hierfür bereitgestellte Online-Formular abgegeben werden.

Weiterhin ist der Zugang auf das absolut erforderliche Maß zu beschränken. Benutzerrechte und -Rollen sind so eng wie technisch möglich zu fassen und nach Möglichkeit personenscharf sein.

Der Vorstand erarbeitet hierzu ein Berechtigungskonzept, welches im Anhang abgedruckt ist, und vermerken entsprechende Rollen in der Mitglieder- und Mitarbeiterdatenbank. Administratoren vergeben Berechtigungen individuell gemäß dem festgelegten Rollen und überprüfen den Bestand an Zugängen und Benutzerkonten regelmäßig kritisch. Wird ein Zugang nicht mehr benötigt, ist dieser unverzüglich zu entziehen.

Darüber hinaus prüft der Vorstand, ob durch Pseudonymisierung und Anonymisierung vor der Zugänglichmachung der Daten ein höheres Datenschutzniveau erreicht und dennoch die Tätigkeit ungehindert ausgeübt werden kann. Zugänge sind bei Beendigung einer Tätigkeit unverzüglich zu löschen. Hierunter fällt insbesondere das Anonymisieren von Daten, die lediglich zu statistischen Zwecken weiterverarbeitet werden sollen.

Eine Person, die Zugriff auf personenbezogene Daten erhalten soll, darf ihre Tätigkeit für den Verein nicht aufnehmen, bis dem Vorstand eine abgegebene Belehrung vorliegt und der Eintrag im Benutzerverzeichnis erfolgt ist. Soweit Teamleiter selbst Personen in ihre Teams aufnehmen, haben sie sicherzustellen, dass der Vorstand rechtzeitig benachrichtigt wird.

Dies gilt unabhängig davon, ob es sich um eine dauerhafte oder nur kurzfristige oder probeweise Tätigkeit handelt.

IT-FACHVERFAHREN, HARD- UND SOFTWARE

Diese Regelungen finden Anwendung für IT-Fachverfahren, Cloud-Dienste, Hosting-Dienste, Webseiten, Add-Ins und Plug-Ins zu bestehenden Lösungen, übrige Online-Dienste sowie Soft- und Hardware sowie Social-Media- und Nachrichtendienste.

Diese Lösungen werden vor der Nutzung bzw. Auswahl nach Datenschutzbelangen geprüft. Eingesetzte Lösungen müssen mit den geltenden Datenschutzvorschriften vereinbar sein und, soweit sie nicht auf einem entsprechend abgesicherten System isoliert betrieben werden, über eine Zugriffskontrolle durch Benutzerkonten verfügen. Falls eine Datenverarbeitung im Auftrag erfolgt, ist vorab ein Vertrag über die Auftragsdatenverarbeitung (ADV) abzuschließen.

Es ist zu prüfen, ob vorrangig zu automatisierten Verfahren, Drittanbieter-, Cloud- oder Online-Diensten

- eine On-Premise-Lösung auf eigener Hardware,
- ein Online-Dienst auf einem selbstverwalteten Server oder Webspace oder
- ein weniger automatisiertes bzw. analoges Verfahren oder
- ein Verfahren mit geringerer Datenerhebung

zur Verfügung stehen und wirtschaftlich genutzt werden können.

Über eingesetzte IT-Fachverfahren und Software führt der Vorstand ein Verzeichnis, in welchem folgende Angaben enthalten sind:

- Hersteller der Lösung
- ggf. Hoster oder Anbieter
- Webseite(n) der Lösung
- Link zur (technischen) Dokumentation der Lösung
- Zweck des Einsatzes, Kurzbeschreibung der Funktion
- Art der gespeicherten oder verarbeiteten Daten
- Stattfinden einer automatisierten Datenverarbeitung
- ggf. Vorliegen eines ADV
- Art und Umfang einer Zugriffsbeschränkung
- Verwaltung (Administration) oder Zugriffe durch Dritte
- Maßnahmen zur Sicherstellung der Datensicherheit und -Integrität
- ggf. Angaben des Herstellers zur DSGVO-konformität oder entsprechende Zertifikate
- ggf. bekannte Risiken oder Sicherheitslücken sowie getroffene Gegenmaßnahmen

Eine Lösung darf produktiv nur genutzt werden, wenn diese vom Vorstand freigegeben und in das Verfahrensverzeichnis aufgenommen wurde.

Der Einsatz eigener Lösungen, etwa die Nutzung von Online-Diensten über private Benutzerkonten oder eigener Software für Vereinszwecke, neben den offiziell freigegebenen Lösungen ist zwingend zu unterlassen. Keinesfalls dürfen über solche Lösungen personenbezogene Daten erhoben, gespeichert oder verarbeitet werden. Eine Zuwiderhandlung stellt eine Pflichtverletzung dar und begründet schlimmstenfalls Schadenersatzansprüche, falls dem Verein etwa durch Bußgelder oder Regressansprüche betroffener Personen ein Schaden entsteht.

Eingesetzte Hardware ist nach dem aktuellen Stand der Technik abzusichern und gegen unbefugte Zugriffe zu schützen. Falls nicht erforderlich, soll auf einen Internetzugang verzichtet werden.

Vereinstätigkeiten dürfen nicht auf privater Hardware bzw. nur innerhalb eines geschützten Bereichs (Virtuelle Maschine, Sandbox) oder Benutzerkontos ausgeführt werden. Die Hardware ist in jedem Fall durch ein sicheres Passwort zu schützen und durch eine aktuelle Antivirensoftware gegen Zugriffe Unbefugter abzusichern.

Veraltete Hardware oder nicht mehr benötigte Hardware soll ersetzt werden. Bei Verkauf, sonstiger Abgabe oder Entsorgung sind alle Datenträger der Vernichtung durch einen zertifizierten Anbieter zuzuführen.

Daten werden, soweit der ständige Zugriff nicht mehr erforderlich ist, aus Online- und Cloud-Speichern sowie von internen Festplatten gelöscht und auf externen Speichermedien archiviert. Diese Speichermedien sind in geschlossenen Räumen aufzubewahren und, wenn möglich, zu verschlüsseln.

Alle Mitglieder und Mitarbeiter müssen Passwort- und Datenverluste oder einen Verdacht auf unbefugte Zugriffe unverzüglich melden.

MELDEKETTE BEI DATENSCHUTZVORFÄLLEN

Wird ein Datenschutzvorfall bekannt, sind unverzüglich alle Vorstandsmitglieder und der Datenschutzbeauftragte zu unterrichten.

Diese treffen die erforderlichen Maßnahmen zur Eliminierung des Risikos und Verhinderung weiterer Schäden.

Datenschutzvorfälle sind insbesondere

- das Bekanntwerden unbefugter Zugriffe,
- das Bekanntwerden verfahrensimmanenter Risiken,
- der Verlust von Passwörtern, Zugangsdaten oder Speichermedien sowie
- Veränderungen in Verfahren oder Prozessen, die ein zusätzliches Risiko bewirken können.

Datenschutzvorfälle werden in einem Verzeichnis festgehalten. Der Vorstand evaluiert zeitnah die Vorfälle, entwickelt geeignete Maßnahmen zur Beseitigung des Risikos und optimiert ggf. Verfahren und Prozesse.

Im Verzeichnis der Datenschutzrelevanten Risiken werden auch die gefundenen Ursachen sowie die getroffenen Maßnahmen dokumentiert.

DATENHALTUNG UND AUFBEWAHRUNG

Daten sollen nicht doppelt gespeichert werden. Eine redundante Speicherung ist nur dann zulässig, soweit es technisch oder aus sonstigen wichtigen Gründen erforderlich ist.

Alle Datenträger sollen an einer Stelle aufzubewahren. Dies ist das Vorstandsbüro laut Satzung. Alle Datenträger sind unverzüglich dorthin weiterzuleiten. Das Vorstandsbüro ist durch Zugangskontrollen und technische Maßnahmen gegen jeden Zugriff durch Unbefugte zu sichern (siehe Anhang TOM).

DATENWEITERGABE

Daten dürfen nur im Rahmen eines Vertragsverhältnisses über die Auftragsdatenverarbeitung oder bei gesetzlicher Verpflichtung weitergegeben werden.

Soweit eine Behörde oder Stelle eine gesetzliche Verpflichtung geltend macht, prüft der Datenschutzbeauftragte ggf. unter Hinzunahme eines Rechtsanwalts, ob eine solche Verpflichtung tatsächlich besteht. Betroffene sind über die Weitergabe zu unterrichten, soweit keine rechtlichen Bedenken bestehen.

DATENSCHUTZERKLÄRUNG

Der Datenschutzbeauftragte fertigt gemeinsam mit dem Vorstand eine Datenschutzerklärung, welche die Betroffenen über ihre Rechte aufklärt sowie mögliche Formen der Datenerhebung aufführt.

Die Datenschutzerklärung ist auf allen Online-Präsenzen aufzuführen sowie auf Veranstaltungen auszuhängen.

VERPFLICHTUNG AUF DAS DATENGEHEIMNIS

Alle Mitarbeiter und Mitglieder sind bei der Aufnahme einer Tätigkeit schriftlich auf das Datengeheimnis (gem. § 5 BDSG), die Einhaltung der Regelungen der DSGVO sowie und die Einhaltung dieser Richtlinie zu verpflichten.

Liegt eine schriftliche Verpflichtung nicht vor, darf die Tätigkeit nicht begonnen werden.

Die Verpflichtung muss gesondert von einem sonstigen Vertrag erfolgen und darf nicht nur Teil einer allgemeinen Vereinbarung sein. Sie ist in einer solchen Form auszugestalten und auszuhändigen, als dass diese die Wichtigkeit der Verpflichtung verdeutlicht.

BELEHRUNG, UNTERWEISUNG UND SCHULUNG

Alle Mitarbeiter und Mitglieder werden regelmäßig über ihre Verpflichtungen nach der DSGVO und die geltenden Datenschutzregeln unterrichtet. Bei Veranstaltungen mit zahlreichen Helfern und Mitarbeitern findet diese Unterweisung vor Veranstaltungsbeginn gesammelt statt.

Der Datenschutzbeauftragte stellt Selbstlernangebote und Materialien zur Verfügung, damit Mitglieder und Mitarbeiter möglichst einfach Zugang zu den benötigten Informationen erhalten können.

Der Vorstand und die Teamleiter stellen sicher, dass Mitarbeiter und Mitglieder sich regelmäßig informieren und unterwiesen werden. Sie sind selbst weiterhin verpflichtet, regelmäßig relevante Rundschreiben, Richtlinien und Regelungen in Sachen Datenschutz zur Kenntnis zu nehmen.

BEREITSTELLUNG INTERNER UND EXTERNER INFORMATIONEN

Sämtliche in diesem Datenschutzkonzept genannten Verzeichnisse und Listen werden in einem für alle beteiligten Personen zugänglichen, internen Wissensmanagement-System (derzeit Vereins-Wiki) zentral geführt.

Externe Informationen, etwa das Datenschutzkonzept oder die Datenschutzerklärung, werden zentral auf dem Webspace des Vereins unter einem statischen Pfad abgelegt. Alle Seiten des Vereins, auch die der einzelnen Veranstaltungen und Teams, sollen ausschließlich auf diese statischen Quellen verweisen, um die Aktualität und Einheitlichkeit der Informationen zu gewährleisten.

LÖSCHUNG PERSONENBEZOGENER DATEN (LÖSCHKONZEPT)

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie sie für den jeweils definierten Zweck benötigt werden oder so lange ihre Aufbewahrung aufgrund rechtlicher Bestimmungen oder zur Erfüllung einer gesetzlichen Pflicht unerlässlich ist.

Für jede Verarbeitungstätigkeit ist im Vorfeld zu definieren,

- wann die Daten unter Berücksichtigung von Aufbewahrungsfristen gelöscht werden können und
- ggf. wann eine Pseudonymisierung oder Anonymisierung trotz bestehender Aufbewahrungspflichten möglich ist.

Liegen Daten mehrfach vor (bspw. aus einem Vorverfahren sowie in der Hauptbuchhaltung) und werden diese nicht zwingend zur rechtlich einwandfreien Dokumentation, sind die Duplikate schnellstmöglich zu löschen.

LÖSCHVORGANG

Die Datenlöschung nach Ablauf der Aufbewahrungsfrist muss innerhalb von 3 Monaten erfolgen.

Die Löschung ist je nach Datenträger durchzuführen:

- Digitale Daten auf wiederverwendbaren Massenspeichern (CD-RW, USB-Speicher, Festplatten, SSD) werden logisch gelöscht und überschrieben, sodass eine Wiederherstellung nicht möglich ist. Wird der Datenträger selbst nicht mehr weiter genutzt, ist er zu vernichten (siehe unten)
- Digitale Daten in Online- und Cloud-Speichern werden logisch gelöscht.
- Digitale Datenträger, welche nicht wiederverwendbar sind (CD-ROM, CD-R), oder nicht wiederverwendet werden sollen werden so zerstört, dass sie mit üblichen Mitteln nicht mehr ausgelesen werden können (Zerkleinern, Verkratzen, Verbrennen, Herbeiführen eines Festplattenschadens durch Magnete). Datenträger mit sensiblen Daten sollen einer nach DIN 66399 zertifizierten Stelle zur Vernichtung übergeben werden.
- Papierdatenträger werden mittels DSGVO-konformen Aktenvernichtern zerkleinert und dem örtlichen Abfallentsorger übergeben. Papierdatenträger mit sensiblen Daten sollen einer nach DIN 66399 zertifizierten Stelle zur Vernichtung übergeben werden. Papierdatenträger können in Ausnahmefällen auch verbrannt werden.

Die Löschung wird unter Angabe, welche Daten an welchem Datum wie vernichtet wurden, protokolliert.

LÖSCHUNG AUF ANFORDERUNG

Machen Betroffene von Ihrem Recht auf Löschung gebrauch, muss die Löschung bzw. begründete Information über die Nichtlöschung innerhalb von 14 Tagen ab Zugang der Anforderung erfolgen.

Der Vorstand prüft, ob die Daten unter Beachtung gesetzlicher Bestimmungen gelöscht werden können und kommt der Bitte unverzüglich nach, soweit keine Bedenken entgegenstehen, oder legt die Gründe für eine weitere Aufbewahrung dar.

Können Daten nicht gelöscht werden, ist vor der Auskunft zusätzlich zu prüfen, ob diese gesperrt oder pseudonymisiert bzw. anonymisiert werden können.

ÜBERTRAGUNG AUF SICHERE SPEICHERMEDIEN UND ARCHIVIERUNG

Stellt der Vorstand bei einer Prüfung fest, dass Daten zwar noch aufbewahrt werden müssen, allerdings nicht mehr in der derzeitigen Form (elektronisch bzw. online) ständig im Zugriff sein müssen, überträgt er die Daten auf ein sichereres Medium (Offline-Speicher wie CDs, Offline-Festplatten oder Papierdatenträger) und löscht sie im Originalsystem (Archivierung).

Entsprechende Situationen können etwa sein:

- Das Exportieren und Ausdrucken von Listen aus Buchungs- oder Reservierungssystemen nach Abrechnung einer Veranstaltung
- Das Ausdrucken von Support- oder Stornovorgängen
- Das Ausdrucken von PDF-Dateien
- Das Übertragen von elektronischen Dokumenten und Dateien auf Offline-Speicher
- Die Nutzung von Archivierungsfunktionen einer Datenbank und Übertragung der Archivdateien auf Offline-Speicher

Diese Überprüfung führt der Schatzmeister hinsichtlich Buchhaltungsdaten spätestens nach Rechtskraft der Steuerbescheide (endgültiger Abschluss der Buchhaltung für das Vorjahr) durch.

Hierdurch wird sichergestellt, dass die Daten zusätzlich vor unbefugten Zugriffen geschützt und nicht mehr automatisiert ausgewertet werden können.

AUSKÜNFTE

Stellen Betroffene Auskünfte über die gespeicherten Daten oder weitergehende Auskünfte, so werden diese durch den Vorstand innerhalb von 14 Tagen beantwortet.

Die einzelnen Organisationseinheiten werden hierzu befragt, ob über die dem Vorstand unmittelbar vorliegenden Datenbestände noch weitere Daten verfügbar sind.

Der Datenschutzbeauftragte legt gemeinsam mit dem Vorstand und den einzelnen Teamleiter ein Verzeichnis von Speicherorten an, an welchen – je nach Art der Geschäftsbeziehung – Daten gespeichert sein könnten.

Wird die Auskunft elektronisch mit einfacher E-Mail angefragt, erfolgt die Auskunft sicherheitshalber an die letzte bekannte Anschrift per Post oder über ein vergleichbar sicheres Medium (Telefax, E-Postbrief, De-Mail, eIDAS-Brief etc.). Der Empfänger ist per E-Mail hierüber zu benachrichtigen.

Die Übermittlung von Daten per E-Mail ist nicht zulässig, da weder die sichere Übertragung noch die Identität des Empfängers mit hinreichender Sicherheit bestimmt werden können.

Verlangt der Empfänger ausdrücklich die Übermittlung per E-Mail bzw. in elektronischer Form, ist die Auskunft entweder auf einem Datenträger per Post zu versenden oder in einem verschlüsselten Archiv. Das Passwort des verschlüsselten Archivs ist per Post oder über ein gleichwertig sicheres Übertragungsmedium zu transportieren (Telefax, E-Postbrief, De-Mail, eIDAS-Brief etc.).

Behördenauskünfte werden durch den Datenschutzbeauftragten unverzüglich beantwortet.

ANHANG - ROLLEN- UND BERECHTIGUNGSKONZEPT

Zur Vereinfachung der Administration erfolgt die Festlegung von Berechtigungen gemäß eines festen Rollenkonzeptes, welches Benutzerrollen in zwei Stufen gliedert.

Gruppen bündeln sachliche Arbeitsbereiche oder in sich geschlossene Organisationseinheiten wie etwa ein Veranstaltungsteam, ein Projektteam oder den Vorstand. Daten sind stets einer Gruppe **sachlich** zugeordnet. Ein Gruppenmitglied hat stets nur auf die Daten seiner Gruppe sowie untergeordneter Gruppen Zugriff.

Funktionen stellen den Status einer einzelnen Person innerhalb der Gruppe dar. Sie entscheiden, welche Befugnisse eine Person innerhalb der Gruppe hat und somit auch, zu Daten welcher Geheimhaltungsstufe bzw. Relevanz die Person Zugang hat.

Bei Zuweisung von Daten zu Rollen gilt: BERECHTIGUNGEN SIND SO ZU VERGEBEN, DASS DER INHABER EINER ROLLE NUR ZUGRIFF AUF DATEN ERHÄLT, OHNE WELCHE DIE TATSÄCHLICHE FUNKTION - GEMESSEN AN SACHLICHER ZUSTÄNDIGKEIT UND ENTSCHEIDUNGSBEFUGNIS - NICHT AUSZUÜBEN WÄRE.

Die Administratoren entscheiden, welche Einzelberechtigungen in welchen Rollen zusammengefasst werden.

VERZEICHNIS DER BENUTZERZUGRIFFE

Die Zuweisung von Rollen durch Gruppen und Funktionen erfolgt innerhalb der Mitglieder- und Mitarbeiterdatenbank ClubDesk.

BESCHREIBUNG DER FUNKTIONEN

VORSITZENDER, ZWEITER VORSITZENDER, SCHATZMEISTER UND PRÄSIDENT (VORSTANDSMITGLIEDER)

Vorstandsmitglieder haben als allein vertretungsberechtigte, geschäftsführende Mitglieder naturgemäß vollen Zugriff auf jedweden Datenbestand des Vereins im operativen Geschäft. Der Zugriff ist zur Erfüllung ihrer Leitungsfunktion zwingend erforderlich.

REVISOR

Revisoren überwachen die Buchhaltung und die finanziellen Geschäfte des Vereins. Sie haben Zugriff auf sämtliche Daten, die gemäß den Vorschriften der GoBD, der AO oder des HGB als steuerlich bzw. buchhalterisch relevant gelten und für die eine gesetzliche Aufzeichnungs- und Aufbewahrungspflicht gilt.

BEISITZER

Beisitzer werden durch den Vorstand oder die Mitgliederversammlung für besondere Geschäfte, die in den Zuständigkeitsbereich des Vorstands fallen, bevollmächtigt. Hierbei kann es sich um

zentrale Funktionen wie die Künstlerische Leitung oder einen Kommunikationsbeauftragten handeln, ebenso aber um Regionalvertreter.

Da Beisitzer eine sachlich eingegrenzte Zuständigkeit haben, legt der Vorstand in der Vollmacht fest, auf welche Daten der Beisitzer Zugriff erhalten soll. Die Administratoren setzen die Vorgaben der Vollmacht individuell um.

TEAMLEITER

Teamleiter haben Zugriff auf alle Daten, die für das operative Geschäft ihres Teams (z.B. Veranstaltungsteam oder PR-Team) relevant sind. Sie haben eine übergreifende Leitungsfunktion inne und müssen somit alle Angelegenheiten, die das Team unmittelbar betreffen, überblicken.

MITARBEITER, TEAMMITGLIEDER (PERSONEN OHNE BESONDERE FUNKTION)

Mitarbeiter und Teammitglieder haben lediglich Zugriff auf die Daten, die für die Erfüllung der ihnen zugewiesenen Funktion zwingend erforderlich sind (z.B. Gästemanager im Veranstaltungsteam nur Zugriff auf Personalien, Flugdaten und Buchungsdaten der Gäste).

ÜBRIGE PERSONEN (OHNE FUNKTIONS- ODER GRUPPENZUORDNUNG)

Übrige Personen haben keinen Zugriff auf personenbezogene Daten, außer diese werden im Rahmen einer Mitgliederversammlung öffentlich erörtert oder sind sonst wie mitzuteilen.

BESCHREIBUNG DER GRUPPEN

VORSTAND

Der Vorstand leitet das operative Geschäft und hat somit Zugriff auf alle Daten, die im Besitz des Vereins sind, ohne Rücksicht auf die sachliche Zuständigkeit.

ALLGEMEINE VERWALTUNG

Die Allgemeine Verwaltung unterstützt den Vorstand beim operativen Geschäft und übernimmt Assistenztätigkeiten (z.B. Botengänge, Abfassung von Schriftstücken, Besorgungen im Auftrag etc.). Grundsätzlich besteht daher auch die Möglichkeit, mit Daten aller Art unabhängig von der sachlichen Zuständigkeit in Kontakt zu kommen.

Bei Mitarbeitern der Allgemeinen Verwaltung sind grundsätzlich keine selbstständigen Zugänge zu eröffnen. Datensätze werden über den Vorstand zur Erledigung einzelner Aufgaben weitergeleitet.

Der Vorstand weist die Administratoren in Einzelfällen an, falls erforderlich einen Zugang zu einem Datenbestand technisch zu eröffnen, wenn dies zur Erfüllung einer längerfristig oder vorübergehend ausgeübten Aufgabe erforderlich ist.

DATENZENTRALE

Mitarbeiter der Datenzentrale haben als technische Administratoren, Entwickler und Programmierer Zugriff zu allen Daten ohne Rücksicht auf die sachliche Zuständigkeit.

KÜNSTLERISCHER BETRIEB

Es besteht kein Zugang zu personenbezogenen Daten außer den Kontaktdaten der Künstlerinnen und Künstler, mit denen eine Zusammenarbeit besteht.

NETZWERKARBEIT

Es besteht kein Zugang zu personenbezogenen Daten außer den Kontaktdaten der Personen und Institutionen, mit denen eine Zusammenarbeit besteht. Die Abrechnung erfolgt über die Rechnungsstelle.

PUBLIC RELATIONS

Es besteht ausschließlich Zugriff auf Social-Media-Konten und Webseiten einschließlich der dort (zwischen-) gespeicherten Daten.

RECHNUNGSSTELLE

Es besteht Zugriff auf alle Daten, die gemäß den Vorschriften der GoBD, der AO oder des HGB als steuerlich bzw. buchhalterisch relevant gelten und für die eine gesetzliche Aufzeichnungs- und Aufbewahrungspflicht gilt. Hierzu zählen ggf. auch begründende Unterlagen, welche Daten aus anderen Zuständigkeitsbereichen enthalten können.

EINKAUF

Es besteht Zugriff ausschließlich auf Kontaktdaten der Geschäftspartner.

VERTRIEB

Es besteht Zugriff ausschließlich auf personenbezogene Kontakt-, Adress-, Namens- und Abrechnungsdaten von Kunden, die Eintrittskarten oder sonstige Waren bzw. Dienstleistungen einkaufen oder eingekauft haben bzw. bezüglich Support-Anliegen an den Verein herantreten.

KASSENVERWALTUNG

Es besteht Zugriff ausschließlich auf personenbezogene Daten der Kunden, die an Kassen bar oder unbar einkaufen. Hierzu zählen ggf. auch Abrechnungsdaten oder bei begründeter Ablehnung von Kartenzahlungen der vom Kreditinstitut übermittelte Grund.

Die sachliche Zuständigkeit beschränkt sich auf das operative Geschäft der jeweiligen Veranstaltungen. Zugriff auf Daten, die der Selbstverwaltung oder einer anderen Veranstaltung zugewiesen sind, ist nicht zu gewähren.

Veranstaltungsteams sind derzeit:

- GalaCon
- Everfree Encore
- Serienfinale 2019
- Serienjubiläum 2020

ANHANG – TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

Folgende technische und organisatorische Maßnahmen werden – neben den im Datenschutzkonzept beschriebenen Maßnahmen – im Einzelnen getroffen, um die Einhaltung datenschutzrechtlicher Vorschriften zu gewährleisten:

1. Gewährleistung der Vertraulichkeit

Zutrittskontrolle *(Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.)*	- mechanische Türen- und Fenstersicherungen - manuelles Schließsystem im Inneren - Schließsystem mit Sicherheitsschlössern - Schlüsselregelung für Beschäftigte - Verschließen der Türen bei Abwesenheit
Zugangskontrolle *(Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.)*	- Erstellen von Benutzerprofilen mit unterschiedlichen Berechtigungen - Pflicht zur Nutzung sicherer Passwörter - Authentifikation durch Benutzername und Passwort - Einsatz von VPN-Technologie bei Zugriff von außen auf die internen Systeme - Sperren von externen Schnittstellen - Einsatz von Intrusion-Detection-Systemen und professioneller Antivirensoftware - ADV-Verträge mit Hostern und Software-Anbietern
Zugriffskontrolle *(Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.)*	- Nutzer-Berechtigungskonzept - Verwaltung der Nutzerrechte durch Systemadministrator - Anzahl der Administratoren auf das Notwendigste reduziert - Verwenden einer Passwortrichtlinie - Protokollierung von Zugriffen auf kritische Anwendungen - physische Löschung von Datenträgern vor Wiederverwendung - ordnungsgemäße Vernichtung von Datenträgern - Einsatz von Aktenvernichtern - Inanspruchnahme von Dienstleistern zur Aktenvernichtung (inkl. Protokollierung der Vernichtung) - Aufbewahrung von Datenträgern in abschließbaren Schränken - Aufbewahrung von Aktenordnern in abschließbaren Schränken

Trennungsgebot *(Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.)*	- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern - Trennung der Zuordnungsdaten und der eigentlichen Daten auf einem getrennten System bei Pseudonymisierung - Festlegung von Datenbankrechten durch Vorgaben im Berechtigungskonzept - Trennung von Produktiv- und Testsystemen
Auftragskontrolle *(Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.)*	- sorgfältige Auswahl des Auftragnehmers (Überprüfung des Dienstleisters) - vorherige Prüfung und Dokumentation der beim Auftragnehmer existierenden TOM - schriftliche Vereinbarung mit dem Auftragnehmer (ADV-Vertrag) - Verpflichtung der Mitarbeiter des Auftragnehmers auf Vertraulichkeit - Datenschutzbeauftragter beim Auftragnehmer - Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags - vertraglich festgelegte Kontrollrechte gegenüber dem Auftragnehmer - regelmäßige Überprüfung des Auftragnehmers und seiner Tätigkeiten - vertraglich festgelegte Vertragsstrafen bei Verstößen
Pseudonymisierung und Anonymisierung	- Nutzung von pseudonymisierten Daten bei Datenübermittlung an externe Dienstleister - Pseudonymisierung oder Anonymisierung bei interner Datenweitergabe, falls möglich - Nutzung statistischer Daten nur
Verschlüsselung	- Datenträgerverschlüsselung unter Windows mittels Bitlocker - Nutzung von hardwareseitig verschlüsselten USB-Festplatten - Datenbankverschlüsselung
Zertifizierung (z.B. ISO)	- Bevorzugung zertifizierter Anbieter und Lösungen - Eine Zertifizierung des Vereins ist finanziell und organisatorisch nicht umsetzbar

2. Gewährleistung der Integrität

Eingabekontrolle *(Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.)*	- Protokollierung der Eingabe, Änderung und Löschung von Daten in kritischen Systemen - individuelle Benutzernamen für Nutzer - sichere Aufbewahrung von Papierunterlagen, von denen Daten ins EDV-System übernommen wurden - Nachvollziehbarkeit durch Berechtigungskonzept
Weitergabekontrolle *(Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.)*	- Nutzung von Standleitungen bzw. VPN-Tunneln - Weitergabe von Daten in anonymisierter oder pseudonymisierter Form (wenn möglich) - verschlüsselte E-Mail-Übertragung (SSL/TLS) - Verschlüsselung E-Mail-Inhalte (Software-Zertifikat) - vertraglich vereinbarte Rechte und Pflichten in Bezug auf die Datenweitergabe - festgelegte Löschfristen - sichere Transportverpackungen - sorgfältige Auswahl von Transportpersonal bzw. -dienstleistern - Nutzung von mobilen Datenträgern mit Verschlüsselungsfunktion - Regelungen zum sicheren Transport von Datenträgern

3. Gewährleistung der Verfügbarkeit

Verfügbarkeitskontrolle *(Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.)*	- unterbrechungsfreie Stromversorgung (USV), zumindest für Server - Alarmanlage im Serverraum - Klimaanlage in Serverräumen - Überwachung von Temperatur und Feuchtigkeit in Serverräumen - Schutzsteckdosenleisten für EDV-Geräte - Feuer- bzw. Rauchmeldeanlagen - Feuerlöschgeräte an mehreren, entsprechend gekennzeichneten Stellen im Gebäude - Datensicherungs-Konzept - regelmäßiges Testen der Funktionsweise der Datensicherung - Notfallkonzept - Aufbewahrung von Datensicherung an sicherem, ausgelagertem Ort - Serverräume nicht unterhalb von sanitären Anlagen gelegen - keine Wasserleitungen in Serverräumen bzw. über den Server-Rechnern - Serverräume nicht in Hochwasser gefährdeten Kellerräumen

4. Gewährleistung der Belastbarkeit der Systeme

Belastbarkeit der IT-Systeme	- Antiviren-Software - Hardware-Firewall - Software-Firewall - Intrusion-Detection-System - sorgfältige Auswahl des externen IT-Dienstleisters

5. Wiederherstellung der Verfügbarkeit

Wiederherstellbarkeit von IT-Systemen	- sorgfältig ausgewählter interner System-Administrator - Vorhaltung von Ersatz-Hardware / Server - Vorhaltung von Ersatz-Hardware / Arbeitsplätze - sorgfältig ausgewählter IT-Dienstleister

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM

Informations-Sicherheits-Management-System (ISMS)	- regelmäßige Prüfung der TOM (mind. 1 x jährlich) durch Vorstand und System-Administrator zusammen mit dem Datenschutzbeauftragten - Einsatz einer ISMS-Software - elektronisches Datenschutz-Handbuch mit Vorgaben zu regelmäßigen Prüfintervallen (eingebunden im Vereins-Wiki)

Die benannten TOM gelten für die im Folgenden beschriebenen EDV-Verfahren und Verarbeitungstätigkeiten.

Soweit Daten durch Dritte im Auftrag verarbeitet werden, wurden die im ADV-Vertrag benannten TOM hier teilweise wiedergegeben, soweit sie unmittelbare Relevanz haben.

ANHANG – VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN

Im Folgenden sind die Verarbeitungstätigkeiten der PEF verzeichnet.

BESCHREIBUNG DER VERARBEITUNGSTÄTIGKEIT "MITGLIEDERVERWALTUNG"

Die Mitgliederverwaltung umfasst die Mitgliedsbetreuung vom Eingang des Mitgliedsantrags über die Prüfung des Antrags, dessen Annahme oder Ablehnung, die laufende Zustellung von Informationen gemäß Satzung und zugehörige Nebenleistungen bis hin zur Entgegennahme des Austrittsersuchens und der Bestätigung des Austritts.

Welchen Zweck hat die Verarbeitung von Daten?

Erfüllung der Aufgaben und Verpflichtungen im Rahmen des Mitgliedsverhältnisses.

Wie werden Daten erhoben?

Anträge gehen elektronisch (Web-Formular, E-Mail), postalisch oder persönlich ein.

Auf welcher Grundlage werden die Daten verarbeitet?

- Erfüllung gesetzlicher Verpflichtungen (Vereinsrecht)
- Explizite Einwilligung (mit Mitgliedsantrag erteilt)

Welche Personen sind betroffen?

- Mitglieder
- Mitgliedsanwärter

Welche Daten werden gespeichert und verarbeitet?

- Name, Vorname
- ggf. Geburtsdatum
- Anschrift
- E-Mailadresse
- Mitgliedsstatus
- Mitgliedsbeitrag
- Ein- und Austrittsdatum

Werden besonders schützenswerte Daten erhoben?

Im Regelfall nicht. Ein Mitglied kann jedoch aufgrund persönlicher Umstände eine Befreiung von der Beitragspflicht beantragen und im Rahmen dieses Antrages etwa Gesundheits- oder Sozialdaten übermitteln.

Wie wird die Rechtmäßigkeit der Verarbeitung sichergestellt?

Die erhobenen Daten werden auf das Mindestmaß beschränkt. Falls Daten freiwillig angegeben werden können, wird dies besonders gekennzeichnet. Bei Anträgen wird auf die Datenschutzbestimmungen hingewiesen, bei elektronischen Anträgen erfolgt ein manuelles Opt-In-Verfahren.

Die Mitglieder und Anwärter werden umfassend durch Hinweistexte und Verweise auf Formularen und Webseiten über die Datenschutzbestimmungen belehrt und müssen diesen explizit zustimmen.

Welche Sicherheitsmaßnahmen werden ergriffen?

Auf die verfahrensimmanenten TOM wird verwiesen. Nur Vorstandsmitglieder erhalten Zugriff auf Mitgliedsdaten (Benutzerverwaltung ownCloud). Nicht erforderliche Daten oder Aufzeichnungen werden unverzüglich gelöscht oder vernichtet.

Welche Verfahren sind beteiligt?

Vorrangig ClubDesk, ownCloud und WordPress.

Wann werden die Daten gelöscht (Rechtsgrundlage/Erfordernis)?

Da die Daten steuerlich relevant sind, erfolgt die Löschung 10 Jahre nach Austritt (Abgabenordnung/Handelsgesetzbuch).

Werden Daten an Dritte übermittelt?

Es werden folgende Daten übermittelt:

- Protokolle von und Einladungen zu Mitgliederversammlungen mitsamt Anlagen, sofern über eine Satzungsänderung oder die Vereinsauflösung entschieden oder der Vorstand neu gewählt wurde, an ein Notariat und das zuständige Registergericht (Amtsgericht Hamm) zur Veröffentlichung im Vereinsregister
- Die Namen der Vorstandsmitglieder an Banken, Auskunfteien und Firmen zur Identifikation

BESCHREIBUNG DER VERARBEITUNGSTÄTIGKEIT "BEARBEITUNG VON FÖRDERANTRÄGEN"

Die Verarbeitung umfasst die Bearbeitung von Förderanträgen vom Eingang des Antrags über dessen Prüfung, dessen Annahme oder Ablehnung, die Abwicklung des Fördervertragsverhältnisses und zugehörige Nebenleistungen bis hin zur Beendigung der Förderung.

Welchen Zweck hat die Verarbeitung von Daten?

Förderung von Vereinen und Privatpersonen gemäß Satzung.

Wie werden Daten erhoben?

Anträge gehen elektronisch (Web-Formular, E-Mail), postalisch oder persönlich ein.

Auf welcher Grundlage werden die Daten verarbeitet?

- Erfüllung gesetzlicher Verpflichtungen (AO/HGB)
- Explizite Einwilligung (mit Förderantrag erteilt)

Welche Personen sind betroffen?

- Geschäftspartner
- Interessenten

Welche Daten werden gespeichert und verarbeitet?

- Name, Vorname
- ggf. Geburtsdatum
- Anschrift
- E-Mailadresse
- Vereinszugehörigkeit
- ggf. wirtschaftliche Verhältnisse
- ggf. die in § 4 der Förderrichtlinie genannten Angaben

Werden besonders schützenswerte Daten erhoben?

Im Regelfall nicht. Unter Umständen können jedoch Angaben, welche nach § 4 der Förderrichtlinie zur Beurteilung der Zuverlässigkeit genutzt werden, hierunter fallen.

In diesem Falle erfolgt eine Speicherung nur zur vorübergehenden Prüfung in Papierform, wobei der Vorstand bei positivem Entscheid lediglich einen Vermerk über das Ergebnis der Prüfung (ohne Begründung oder Entscheidungsgrundlagen) zu den laufenden Akten nimmt und im Ablehnungsfalle die Daten lediglich zur Begründung der Ablehnung nutzt und hiernach unverzüglich vernichtet.

Wie wird die Rechtmäßigkeit der Verarbeitung sichergestellt?

Die erhobenen Daten werden auf das Mindestmaß beschränkt. Falls Daten freiwillig angegeben werden können, wird dies besonders gekennzeichnet. Bei Anträgen wird auf die Datenschutzbestimmungen hingewiesen.

Die Antragsteller werden umfassend durch Hinweistexte und Verweise auf Formularen und Webseiten über die Datenschutzbestimmungen belehrt und müssen diesen explizit zustimmen.

Welche Sicherheitsmaßnahmen werden ergriffen?

Auf die verfahrensimmanenten TOM wird verwiesen. Nur Vorstandsmitglieder erhalten Zugriff auf Antragsdtaen (Benutzerverwaltung ownCloud). Nicht erforderliche Daten oder Aufzeichnungen werden unverzüglich gelöscht oder vernichtet.

Welche Verfahren sind beteiligt?

Vorrangig ownCloud und WordPress.

Wann werden die Daten gelöscht (Rechtsgrundlage/Erfordernis)?

Da die Daten steuerlich relevant sind, erfolgt die Löschung 10 Jahre nach Beendigung der Förderung (Abgabenordnung/Handelsgesetzbuch).

Werden Daten an Dritte übermittelt?

Es werden folgende Daten übermittelt:

- Im Rahmen einer Überprüfung sämtliche Daten zu erfolgten Förderungen an das Finanzamt Hamm

BESCHREIBUNG DER VERARBEITUNGSTÄTIGKEIT "KUNDENSUPPORT"

Die Tätigkeit umfasst die gesamte Abwicklung von Kundenanfragen, Beschwerden und sonstigen Anliegen.

Welchen Zweck hat die Verarbeitung von Daten?

- Abwicklung von Anfragen
- Durchführung (vor-) vertraglicher Maßnahmen

Wie werden Daten erhoben?

Die Daten gehen per E-Mail oder elektronisch über WordPress-Formulare ein. Formulare können nur abgesendet werden, wenn die explizite Einwilligung zur Datenverarbeitung erteilt wird.

Auf welcher Grundlage werden die Daten verarbeitet?

- Erfüllung gesetzlicher Verpflichtungen (AO/HGB/GoBD)
- Erfüllung von Verträgen
- Explizite Einwilligung der betroffenen Personen

Welche Personen sind betroffen?

- Mitglieder
- Kunden
- Geschäftspartner
- Interessenten

Welche Daten werden gespeichert und verarbeitet?

- Name, Vorname
- Anschrift
- E-Mailadresse
- Nationalität
- ggf. Mitgliedsstatus
- weitere mitgeteilte Daten

Werden besonders schützenswerte Daten erhoben?

Im Regelfall nicht. Ein Kunde kann jedoch freiwillig solche Daten übermitteln; in einem solchen Falle sind alle Mitarbeiter angewiesen, diese zu sperren und die ausdrückliche Einwilligung zu erfragen, falls die Daten relevant sind, oder die Daten sofort zu löschen, falls dem Anliegen auch anders abgeholfen werden kann.

Wie wird die Rechtmäßigkeit der Verarbeitung sichergestellt?

Die erhobenen Daten werden auf das Mindestmaß beschränkt. Gesetzlich nicht erforderliche Daten werden nach Erfüllung des Kundenanliegens gelöscht.

Welche Sicherheitsmaßnahmen werden ergriffen?

Auf die verfahrensimmanenten TOM wird verwiesen. Nur Vorstandsmitglieder erhalten Zugriff auf den Ticketshop und die Buchhaltungsdaten (Benutzerverwaltung). Nicht erforderliche Daten oder Aufzeichnungen werden unverzüglich gelöscht oder vernichtet.

Daten werden nur anonymisiert und/oder kumuliert für statistische Zwecke genutzt.

Welche Verfahren sind beteiligt?

Vorrangig TicketToaster und E-Mail-Postfächer. Unterlagen werden auch in Papierform oder digital in ownCloud abgelegt, wenn sie für die Buchhaltung relevant sind.

Wann werden die Daten gelöscht (Rechtsgrundlage/Erfordernis)?

Da die Daten steuerlich relevant sind, erfolgt die Löschung nach 10 Jahren (Abgabenordnung/Handelsgesetzbuch). Andere Vorgänge werden schnellstmöglich nach Erledigung gelöscht.

Werden Daten an Dritte übermittelt?

Es werden keine Daten an Dritte übermittelt.

BESCHREIBUNG DER VERARBEITUNGSTÄTIGKEIT "BESTELLUNG, EINKAUF UND ÄNDERUNG VON EINTRITTSKARTEN"

Die Tätigkeit umfasst die gesamte Abwicklung einer Bestellung von deren Eingang über deren Bezahlung bis hin zur Zustellung der Eintrittskarte und ggf. geleistetem Support.

Daten aus dem Ticket-Shop werden später in die Buchhaltung (Lexware) importiert.

Welchen Zweck hat die Verarbeitung von Daten?

- Vertrieb von Eintrittskarten
- Erfüllung der gesetzlichen Buchführungs- und Meldepflichten nach AO, HGB und GoBD

Wie werden Daten erhoben?

Die Daten gehen elektronisch über den Ticket-Shop ein.

Auf welcher Grundlage werden die Daten verarbeitet?

- Erfüllung gesetzlicher Verpflichtungen (AO/HGB/GoBD)
- Erfüllung von Verträgen
- Explizite Einwilligung der betroffenen Personen

Welche Personen sind betroffen?

- Mitglieder
- Kunden
- Geschäftspartner
- Mitarbeiter/Honorarkräfte

Welche Daten werden gespeichert und verarbeitet?

- Name, Vorname
- Anschrift
- E-Mailadresse
- Nationalität
- ggf. Mitgliedsstatus
- Zahlungsdaten

Werden besonders schützenswerte Daten erhoben?

Im Regelfall nicht. Ein Kunde kann jedoch aufgrund persönlicher Umstände eine Ermäßigung oder eine kostenfreie Stornierung beantragen und im Rahmen dieses Antrages etwa Gesundheits- oder Sozialdaten übermitteln.

Wie wird die Rechtmäßigkeit der Verarbeitung sichergestellt?

Die erhobenen Daten werden auf das Mindestmaß beschränkt. Gesetzlich nicht erforderliche Daten werden entfernt oder gar nicht erst importiert.

Welche Sicherheitsmaßnahmen werden ergriffen?

Auf die verfahrensimmanenten TOM wird verwiesen. Nur Vorstandsmitglieder erhalten Zugriff auf den Ticketshop und die Buchhaltungsdaten (Benutzerverwaltung). Nicht erforderliche Daten oder Aufzeichnungen werden unverzüglich gelöscht oder vernichtet.

Daten werden nur anonymisiert und/oder kumuliert für statistische Zwecke genutzt.

Welche Verfahren sind beteiligt?

Vorrangig TicketToaster und Lexware. Unterlagen werden auch in Papierform abgelegt. Kundenanfragen und Kundenanliegen werden über Zammad abgewickelt, ansonsten sind die Zahlungsdienstleister PayPal und stripe sowie die Sparkasse HRV beteiligt.

Wann werden die Daten gelöscht (Rechtsgrundlage/Erfordernis)?

Da die Daten steuerlich relevant sind, erfolgt die Löschung nach 10 Jahren (Abgabenordnung/Handelsgesetzbuch). Daten werden jedoch regelmäßig archiviert und der Zugriff somit weiter eingeschränkt.

Werden Daten an Dritte übermittelt?

Es werden folgende Daten übermittelt:

- Kumulierte Daten (Steueranmeldungen, betriebswirtschaftliche Auswertungen) an das Finanzamt Hamm
- Auf Anforderung sämtliche Daten an das Finanzamt Hamm (Überprüfung)
- Name, Anschrift und Vergütung von Mitarbeitern und Honorarkräften an das Finanzamt Hamm bzw. das Bundeszentralamt für Steuern
- ggf. sämtliche Daten an Steuerkanzleien

BESCHREIBUNG DER VERARBEITUNGSTÄTIGKEIT "HELFERBEWERBUNGEN UND -BETREUUNG"

Die Verarbeitungstätigkeit umfasst die Bearbeitung von Helferbewerbungen von deren Eingang über die Prüfung der Bewerbung, deren Annahme oder Ablehnung, die Durchführung (vor-) vertraglicher Maßnahmen bis hin zur Beendigung des Vertragsverhältnisses.

Welchen Zweck hat die Verarbeitung von Daten?

Erfüllung gesetzlicher Verpflichtungen im Rahmen des Auftragsverhältnisses; Akquise von Helfern für Veranstaltungen und deren Betreuung.

Wie werden Daten erhoben?

Anträge gehen elektronisch (Web-Formular, E-Mail), postalisch oder persönlich ein.

Auf welcher Grundlage werden die Daten verarbeitet?

- Erfüllung gesetzlicher Verpflichtungen (Aufzeichnungspflichten nach AO/HGB, Nachweispflichten Datenschutz/Arbeitsschutz/Ausländerbeschäftigung)
- Explizite Einwilligung (mit Bewerbung erteilt)

Welche Personen sind betroffen?

- Helfer
- Bewerber

Welche Daten werden gespeichert und verarbeitet?

- Name, Vorname
- ggf. Geburtsdatum
- Anschrift
- E-Mailadresse
- Mitgliedsstatus
- Daten zu vorherigen Tätigkeiten
- Daten zu Ausbildung und beruflichem Werdegang

Werden besonders schützenswerte Daten erhoben?

Im Regelfall nicht. Ein Bewerber kann jedoch im Rahmen der Bewerbung etwa Gesundheitsdaten übermitteln, um auf besondere Umstände oder Ansprüche hinzuweisen. Solche Daten werden besonders geschützt und verschlüsselt.

Wie wird die Rechtmäßigkeit der Verarbeitung sichergestellt?

Die erhobenen Daten werden auf das Mindestmaß beschränkt. Falls Daten freiwillig angegeben werden können, wird dies besonders gekennzeichnet. Bei Anträgen wird auf die Datenschutzbestimmungen hingewiesen, bei elektronischen Anträgen erfolgt ein manuelles Opt-In-Verfahren.

Die Helfer und Bewerber werden umfassend durch Hinweistexte und Verweise auf Formularen und Webseiten über die Datenschutzbestimmungen belehrt und müssen diesen explizit zustimmen.

Welche Sicherheitsmaßnahmen werden ergriffen?

Auf die verfahrensimmanenten TOM wird verwiesen. Nur zuständige Mitarbeiter und Mitglieder erhalten Zugriff auf die gespeicherten Daten (Benutzerverwaltung). Nicht erforderliche Daten oder Aufzeichnungen werden unverzüglich gelöscht oder vernichtet.

Welche Verfahren sind beteiligt?

Vorrangig Helferverwaltung, ownCloud und WordPress.

Wann werden die Daten gelöscht (Rechtsgrundlage/Erfordernis)?

Da die Daten teilweise steuerlich relevant sind oder zur Erfüllung von Nachweispflichten benötigt werden, erfolgt die Löschung nach 10 Jahren (Abgabenordnung/Handelsgesetzbuch).

Werden Daten an Dritte übermittelt?

Es werden folgende Daten übermittelt:

- Im Rahmen von Überprüfungen sämtliche Daten an Aufsichtsbehörden

BESCHREIBUNG DER VERARBEITUNGSTÄTIGKEIT "BEWERBUNG UND REGISTRIERUNG FÜR VERANSTALTUNGEN, ALS REFERENT ODER ALS KÜNSTLER"

Die Verarbeitungstätigkeit umfasst die Bearbeitung von Bewerbungen und Registrierungen von deren Eingang über die Prüfung der Bewerbung, deren Annahme oder Ablehnung, die Durchführung (vor-) vertraglicher Maßnahmen bis hin zur Beendigung des Vertragsverhältnisses.

Welchen Zweck hat die Verarbeitung von Daten?

Erfüllung gesetzlicher Verpflichtungen im Rahmen des Auftragsverhältnisses; Akquise von Referenten und Künstlern für Veranstaltungen und deren Betreuung.

Wie werden Daten erhoben?

Anträge gehen elektronisch (Web-Formular, E-Mail), postalisch oder persönlich ein.

Auf welcher Grundlage werden die Daten verarbeitet?

- Erfüllung gesetzlicher Verpflichtungen (Aufzeichnungspflichten nach AO/HGB, Nachweispflichten Datenschutz/Arbeitsschutz/Ausländerbeschäftigung)
- Explizite Einwilligung (mit Bewerbung erteilt)

Welche Personen sind betroffen?

- Künstler
- Bewerber
- Personen, die sich zu anmeldepflichtigen Veranstaltungen anmelden

Welche Daten werden gespeichert und verarbeitet?

- Name, Vorname
- ggf. Geburtsdatum
- Anschrift
- E-Mailadresse
- Mitgliedsstatus
- Daten zu vorherigen Tätigkeiten
- Daten zu Ausbildung und beruflichem Werdegang

Werden besonders schützenswerte Daten erhoben?

Im Regelfall nicht. Ein Bewerber kann jedoch im Rahmen der Bewerbung etwa Gesundheitsdaten übermitteln, um auf besondere Umstände oder Ansprüche hinzuweisen. Solche Daten werden besonders geschützt und verschlüsselt.

Wie wird die Rechtmäßigkeit der Verarbeitung sichergestellt?

Die erhobenen Daten werden auf das Mindestmaß beschränkt. Falls Daten freiwillig angegeben werden können, wird dies besonders gekennzeichnet. Bei Anträgen wird auf die

Datenschutzbestimmungen hingewiesen, bei elektronischen Anträgen erfolgt ein manuelles Opt-In-Verfahren.

Die Helfer und Bewerber werden umfassend durch Hinweistexte und Verweise auf Formularen und Webseiten über die Datenschutzbestimmungen belehrt und müssen diesen explizit zustimmen.

Welche Sicherheitsmaßnahmen werden ergriffen?

Auf die verfahrensimmanenten TOM wird verwiesen. Nur zuständige Mitarbeiter und Mitglieder erhalten Zugriff auf die gespeicherten Daten (Benutzerverwaltung). Nicht erforderliche Daten oder Aufzeichnungen werden unverzüglich gelöscht oder vernichtet.

Welche Verfahren sind beteiligt?

Vorrangig ownCloud und WordPress.

Wann werden die Daten gelöscht (Rechtsgrundlage/Erfordernis)?

Da die Daten teilweise steuerlich relevant sind oder zur Erfüllung von Nachweispflichten benötigt werden, erfolgt die Löschung nach 10 Jahren (Abgabenordnung/Handelsgesetzbuch).

Werden Daten an Dritte übermittelt?

Es werden folgende Daten übermittelt:

- Im Rahmen von Überprüfungen sämtliche Daten an Aufsichtsbehörden

BESCHREIBUNG DER VERARBEITUNGSTÄTIGKEIT "FINANZBUCHHALTUNG"

Die Finanzbuchhaltung umfasst die gesamte Abwicklung finanzieller Angelegenheiten vom Belegeingang über die Zahlbarmachung bis hin zur Erstellung von Auswertungen und Steueranmeldungen.

Daten aus dem Ticket-Shop oder Kassenverfahren werden hierzu importiert.

Welchen Zweck hat die Verarbeitung von Daten?

Erfüllung der gesetzlichen Buchführungs- und Meldepflichten nach AO, HGB und GoBD.

Wie werden Daten erhoben?

Die Daten gehen elektronisch (Web-Formular, E-Mail), postalisch oder persönlich ein.

Auf welcher Grundlage werden die Daten verarbeitet?

- Erfüllung gesetzlicher Verpflichtungen (Vereinsrecht)
- Erfüllung von Verträgen

Welche Personen sind betroffen?

- Mitglieder
- Kunden
- Geschäftspartner
- Mitarbeiter/Honorarkräfte

Welche Daten werden gespeichert und verarbeitet?

- Name, Vorname
- Anschrift
- E-Mailadresse
- Nationalität
- ggf. Mitgliedsstatus
- ggf. Kontokorrent
- ggf. gezahlte Vergütungen

Werden besonders schützenswerte Daten erhoben?

Nein.

Wie wird die Rechtmäßigkeit der Verarbeitung sichergestellt?

Die erhobenen Daten werden auf das Mindestmaß beschränkt. Gesetzlich nicht erforderliche Daten werden entfernt oder gar nicht erst importiert.

Welche Sicherheitsmaßnahmen werden ergriffen?

Auf die verfahrensimmanenten TOM wird verwiesen. Nur Vorstandsmitglieder erhalten Zugriff auf die Buchhaltungsdaten (Benutzerverwaltung Lexware). Nicht erforderliche Daten oder Aufzeichnungen werden unverzüglich gelöscht oder vernichtet.

Welche Verfahren sind beteiligt?

Vorrangig ownCloud, helloCash und Lexware. Unterlagen werden auch in Papierform abgelegt.

Wann werden die Daten gelöscht (Rechtsgrundlage/Erfordernis)?

Da die Daten steuerlich relevant sind, erfolgt die Löschung nach 10 Jahren (Abgabenordnung/Handelsgesetzbuch). Daten werden jedoch regelmäßig archiviert und der Zugriff somit weiter eingeschränkt.

Werden Daten an Dritte übermittelt?

Es werden folgende Daten übermittelt:

- Kumulierte Daten (Steueranmeldungen, betriebswirtschaftliche Auswertungen) an das Finanzamt Hamm
- Auf Anforderung sämtliche Daten an das Finanzamt Hamm (Überprüfung)
- Name, Anschrift und Vergütung von Mitarbeitern und Honorarkräften an das Finanzamt Hamm bzw. das Bundeszentralamt für Steuern
- ggf. sämtliche Daten an Steuerkanzleien

BESCHREIBUNG DER VERARBEITUNGSTÄTIGKEIT "AKTEN- UND DATENTRÄGERVERNICHTUNG"

Die Tätigkeit umfasst die Vernichtung von Akten, Dokumenten und Datenträgern. Die Vernichtung erfolgt gemäß Löschkonzept und ISO 66399.

Welchen Zweck hat die Verarbeitung von Daten?

- Erfüllung von Löschpflichten nach der DSGVO
- Entsorgung nicht mehr benötigter Datenträger, Dokumente und Akten

Auf welcher Grundlage werden die Daten verarbeitet?

- Erfüllung gesetzlicher Verpflichtungen (DSGVO)
- Bei Erhebung der Daten angewandte Rechtsgrundlagen

Welche Personen sind betroffen?

- Mitglieder
- Mitgliedsanwärter
- Kunden und Geschäftspartner
- Mitarbeiter und Helfer

Welche Daten werden gespeichert und verarbeitet?

- Alle Arten personenbezogener Daten

Wie wird die Rechtmäßigkeit der Verarbeitung sichergestellt?

Die Vernichtung erfolgt in der Regel durch zertifizierte Dienstleister oder mittels zertifizierter Einrichtungen. Sollte dies nicht der Fall sein, erfolgt die Vernichtung gemäß DIN-Norm 66399.

Welche Sicherheitsmaßnahmen werden ergriffen?

Die im Datenschutzkonzept angegebenen TOM finden Anwendung. Insbesondere werden verschließbare Behältnisse zur Aufbewahrung und zum Transport verwendet. Bei der Auswahl von Dienstleistern werden die TOM überprüft.

Werden Daten an Dritte übermittelt?

Soweit die Vernichtung durch Dienstleister erfolgt, werden die Datenträger dort in einen verschlossenen Behälter eingeworfen. Zugriff auf die Daten wird in diesem Falle durch vertragliche Verpflichtungen ausgeschlossen.

Folgende Verfahren setzt die PEF für ihre Verarbeitungstätigkeiten ein.

VERFAHRENSBESCHREIBUNG – OWNCLOUD

Anbieter	Hoster	Webseite	Dokumentation
ownCloud GmbH	Hetzner Online GmbH	https://owncloud.org/	https://owncloud.com/whitepapers/

Was ist Zweck des Einsatzes?

Cloud-Speicher als zentraler Datenspeicher sowie Filesharing-Lösung.

Welche Arten von Daten werden gespeichert oder verarbeitet?

- Geschäftliche Daten jeder Art
- auch personenbezogene Daten
- unter Umständen auch besonders geschützte Daten
- auch Personaldaten

Findet eine automatisierte Datenverarbeitung statt?

Nein, die Anwendung ist manuell zu bedienen.

Werden Zugriffe beschränkt?

Ja, es existiert eine Benutzerverwaltung, welche die Festlegung von Gruppen und Berechtigungen für einzelne Verzeichnisse und Dateioperationen zulässt. Dateien können einzeln freigegeben werden. Die Administration stellt eine weitestgehende Beschränkung des Zugangs sicher.

Wird das Verfahren selbst oder durch Dritte verwaltet?

Das Verfahren wird selbst auf einem eigenen Webspace bzw. vServer verwaltet.

Liegt ein Vertrag über die Auftragsverarbeitung mit dem Anbieter vor?

Es besteht ein Vertrag mit dem Hosting-Anbieter.

Wie ist das Verfahren gegen unbefugte Zugriffe und Datenverlust geschützt?

Die im ADV-Vertrag festgelegten TOM stellen Zugriffsschutz und Integrität sicher. Durch eine strenge Benutzerverwaltung und häufige Sicherheitsupdates wird der Zugriffsschutz zusätzlich verstärkt.

Gibt der Hersteller Hinweise zur Konformität mit den Vorschriften der DSGVO?

Die hierzu unter https://owncloud.com/gdpr/ bereitgestellten Maßnahmen werden umgesetzt.

Sind kritische Funktionen (Statistik, Tracking, Drittanbieter-Plugins etc.) bekannt?

Nein.

Sind Sicherheitslücken, Risiken oder sonstige Probleme bekannt?

Nein.

Anbieter	Hoster	Webseite	Dokumentation
DokuWiki	Hetzner Online GmbH	https://www.dokuwiki.org/dokuwiki	https://www.dokuwiki.org/manual

Was ist Zweck des Einsatzes?

1. Bereitstellen interner statischer und dynamischer Informationen
2. Aufbau eines internen Wissensmanagements
3. Protokollierung und Dokumentation

Welche Arten von Daten werden gespeichert oder verarbeitet?

- E-Mailadresse und Namen von Benutzern
- Namen, E-Mailadresse und Anschrift sowie weitere dort benannte Daten aus Formularen für Verzeichnisse (Bewerbungen, Panels, Musiker, Künstler, Gäste etc.)

Es werden für die Auswahl und Verwaltung von Bewerbungen und Belegungsplänen Listen erstellt, die Daten zu Musikern, Künstlern, Gästen, Mitarbeitern oder sonstigen Akteuren enthalten. Soweit solche personenbezogenen Daten gespeichert werden, erfolgt eine entsprechende Zugriffsbeschränkung durch Benutzerrollen.

Findet eine automatisierte Datenverarbeitung statt?

Ja, Daten werden mittels elektronischer Einrichtungen editiert und gespeichert.

Werden Zugriffe beschränkt?

Ja, es existiert eine Benutzerverwaltung, welche die Festlegung von Gruppen und Berechtigungen für einzelne Bereiche zulässt. Die Administration stellt eine weitestgehende Beschränkung des Zugangs sicher.

Wird das Verfahren selbst oder durch Dritte verwaltet?

Das Verfahren wird selbst auf einem eigenen Webspace bzw. vServer verwaltet.

Liegt ein Vertrag über die Auftragsverarbeitung mit dem Anbieter vor?

Es besteht ein Vertrag mit dem Hosting-Anbieter.

Wie ist das Verfahren gegen unbefugte Zugriffe und Datenverlust geschützt?

Die im ADV-Vertrag festgelegten TOM stellen Zugriffsschutz und Integrität sicher. Durch eine strenge Benutzerverwaltung und häufige Sicherheitsupdates wird der Zugriffsschutz zusätzlich verstärkt.

Gibt der Hersteller Hinweise zur Konformität mit den Vorschriften der DSGVO?

Es sind keine Hinweise vorhanden. Die allgemeinen Empfehlungen zur IT-Sicherheit werden berücksichtigt.

Sind kritische Funktionen (Statistik, Tracking, Drittanbieter-Plugins etc.) bekannt?

Nein.

Sind Sicherheitslücken, Risiken oder sonstige Probleme bekannt?

Nein.

Anbieter	Webseite	Dokumentation
PayPal S.a.r.l. & Cie.	https://www.paypal.com/de/webapps/mpp/merchant	https://developer.paypal.com/docs/

Was ist Zweck des Einsatzes?

Abwicklung von Zahlungen für Nutzer des Zahlungsdienstes.

Welche Arten von Daten werden gespeichert oder verarbeitet?

- Name, E-Mailadresse und Anschrift
- Zahlungsdaten

Findet eine automatisierte Datenverarbeitung statt?

Ja, die Zahlungen werden vollständig automatisiert abgewickelt.

Werden Zugriffe beschränkt?

Ja, nur der Vorstand hat Zugriff.

Wird das Verfahren selbst oder durch Dritte verwaltet?

Es handelt sich um ein Zahlverfahren des Anbieters PayPal, welches von diesem verwaltet wird. Die PEF ist selbst lediglich Nutzer des Verfahrens.

Liegt ein Vertrag über die Auftragsverarbeitung mit dem Anbieter vor?

Nein, es handelt sich um einen Zahlungsdienstleister.

Wie ist das Verfahren gegen unbefugte Zugriffe und Datenverlust geschützt?

Auf die auf der Anbieterseite beschriebenen TOM wird verwiesen.

Gibt der Hersteller Hinweise zur Konformität mit den Vorschriften der DSGVO?

Es sind keine unmittelbaren Hinweise vorhanden.

Sind kritische Funktionen (Statistik, Tracking, Drittanbieter-Plugins etc.) bekannt?

Nein.

Sind Sicherheitslücken, Risiken oder sonstige Probleme bekannt?

Nein. Die Nutzer des Zahlverfahrens unterwerfen sich den AGB und Datenschutzbestimmungen des Anbieters.

Anbieter	Webseite	Dokumentation
Sparkasse Hilden-Ratingen-Velbert	https://www.sparkasse-hrv.de/de/home.html	nicht verfügbar

Was ist Zweck des Einsatzes?

Verwaltung von Bankkonten des Vereins.

Welche Arten von Daten werden gespeichert oder verarbeitet?

- Name und ggf. Anschrift von Zahlern und Zahlungsempfängern
- Zahlungsdaten (Kontonummer, Bankleitzahl, Kreditinstitut)

Findet eine automatisierte Datenverarbeitung statt?

Ja, die Zahlungsabwicklung erfolgt automatisiert.

Werden Zugriffe beschränkt?

Ja, nur der Vorstand hat Zugriff.

Wird das Verfahren selbst oder durch Dritte verwaltet?

Es handelt sich um ein Zahlverfahren, welches vom Anbieter selbst verwaltet wird. Die PEF ist selbst lediglich Nutzer des Verfahrens.

Liegt ein Vertrag über die Auftragsverarbeitung mit dem Anbieter vor?

Nein, es handelt sich um einen Zahlungsdienstleister.

Wie ist das Verfahren gegen unbefugte Zugriffe und Datenverlust geschützt?

Auf die auf der Anbieterseite beschriebenen TOM wird verwiesen.

Gibt der Hersteller Hinweise zur Konformität mit den Vorschriften der DSGVO?

Es sind keine unmittelbaren Hinweise vorhanden.

Sind kritische Funktionen (Statistik, Tracking, Drittanbieter-Plugins etc.) bekannt?

Nein.

Sind Sicherheitslücken, Risiken oder sonstige Probleme bekannt?

Nein.

Anbieter	Hoster	Webseite	Dokumentation
stripe, Inc.	–	https://stripe.com/de	https://stripe.com/docs

Was ist Zweck des Einsatzes?

Abwicklung von Zahlungen für Nutzer des Zahlungsdienstes.

Welche Arten von Daten werden gespeichert oder verarbeitet?

- Name, E-Mailadresse und Anschrift
- Zahlungsdaten

Findet eine automatisierte Datenverarbeitung statt?

Ja, die Zahlungen werden vollständig automatisiert abgewickelt.

Werden Zugriffe beschränkt?

Ja, nur der Vorstand hat Zugriff.

Wird das Verfahren selbst oder durch Dritte verwaltet?

Es handelt sich um ein Zahlverfahren des Anbieters stripe, welches von diesem verwaltet wird. Die PEF ist selbst lediglich Nutzer des Verfahrens.

Liegt ein Vertrag über die Auftragsverarbeitung mit dem Anbieter vor?

Nein, es handelt sich um einen Zahlungsdienstleister.

Wie ist das Verfahren gegen unbefugte Zugriffe und Datenverlust geschützt?

Auf die auf der Anbieterseite beschriebenen TOM wird verwiesen.

Gibt der Hersteller Hinweise zur Konformität mit den Vorschriften der DSGVO?

Es sind keine unmittelbaren Hinweise vorhanden.

Sind kritische Funktionen (Statistik, Tracking, Drittanbieter-Plugins etc.) bekannt?

Nein.

Sind Sicherheitslücken, Risiken oder sonstige Probleme bekannt?

Nein. Die Nutzer des Zahlverfahrens unterwerfen sich den AGB und Datenschutzbestimmungen des Anbieters.

Anbieter	Hoster	Webseite	Dokumentation
Bayerisches Landesamt für Steuern - Dienststelle München		https://www.elster.de/	https://www.elster.de/eportal/infoseite/kontakt

Was ist Zweck des Einsatzes?

Erfüllung von Verpflichtungen nach steuerrechtlichen Vorschriften.

Welche Arten von Daten werden gespeichert oder verarbeitet?

- Name, Anschrift sowie Vertrags- und Vergütungsdaten von Personen, an die eine Vergütung geleistet wird, für welche eine Meldung an die Finanzbehörden erfolgen muss

Findet eine automatisierte Datenverarbeitung statt?

Ja, Daten werden mittels elektronischer Einrichtungen editiert und gespeichert.

Werden Zugriffe beschränkt?

Ja, es existiert eine Benutzerverwaltung, welche die granulare Festlegung von Berechtigungen für einzelne Daten und Operationen zulässt. Die Administration stellt eine weitestgehende Beschränkung des Zugangs sicher.

Wird das Verfahren selbst oder durch Dritte verwaltet?

Vollständig durch die Finanzbehörden.

Liegt ein Vertrag über die Auftragsverarbeitung mit dem Anbieter vor?

Nein, es handelt sich nicht um eine Auftragsdatenverarbeitung im Sinne der DSGVO.

Wie ist das Verfahren gegen unbefugte Zugriffe und Datenverlust geschützt?

Da das Verfahren vollständig durch die Finanzbehörden betrieben wird, liegt dort die Verantwortung für adäquate TOM. Intern kann nur sichergestellt werden, dass durch eine

Zugriffsbeschränkung nur der Vorstand bzw. für steuerliche Aufgaben besonders bevollmächtigte Personen Zugriff erhalten.

Gibt der Hersteller Hinweise zur Konformität mit den Vorschriften der DSGVO?

Die allgemeinen Empfehlungen zur IT-Sicherheit werden berücksichtigt. Der Hersteller bietet keine weiteren Hinweise an.

Sind kritische Funktionen (Statistik, Tracking, Drittanbieter-Plugins etc.) bekannt?

Nein.

Sind Sicherheitslücken, Risiken oder sonstige Probleme bekannt?

Nein.

Anbieter	Hoster	Webseite	Dokumentation
Haufe-Lexware GmbH & Co. KG	Hetzner Online GmbH	https://www.lexware.de/	https://www.lexware.de/handbuecher-kostenlos-herunterladen/

Was ist Zweck des Einsatzes?

Abwicklung der (Anlagen-) Buchhaltung.

Welche Arten von Daten werden gespeichert oder verarbeitet?

- Namen und Anschriften von Kunden und Geschäftspartnern
- Allgemeine Buchhaltungsdaten
- Elektronische buchhaltungsrelevante Dokumente
- Kontenstände (Debitoren- und Kreditoren-Kontokorrent)

Findet eine automatisierte Datenverarbeitung statt?

Ja, Daten werden mittels elektronischer Einrichtungen editiert und gespeichert.

Werden Zugriffe beschränkt?

Ja, es existiert sowohl für die virtuelle Maschine als auch für das Verfahren selbst eine Benutzerverwaltung, welche die Festlegung von Gruppen und Berechtigungen für einzelne Operationen zulässt. Die Administration stellt eine weitestgehende Beschränkung des Zugangs sicher.

Wird das Verfahren selbst oder durch Dritte verwaltet?

Das Verfahren wird selbst auf einem eigenen vServer verwaltet.

Liegt ein Vertrag über die Auftragsverarbeitung mit dem Anbieter vor?

Es besteht ein Vertrag mit dem Hosting-Anbieter.

Wie ist das Verfahren gegen unbefugte Zugriffe und Datenverlust geschützt?

Die im ADV-Vertrag festgelegten TOM stellen Zugriffsschutz und Integrität sicher. Durch eine strenge Benutzerverwaltung und häufige Sicherheitsupdates wird der Zugriffsschutz zusätzlich

verstärkt. Die virtuelle Maschine selbst und die Anwendung sind einzeln durch eine eigene Benutzerverwaltung geschützt; die Datenbank ist verschlüsselt.

Gibt der Hersteller Hinweise zur Konformität mit den Vorschriften der DSGVO?

Die allgemeinen Empfehlungen zur IT-Sicherheit werden berücksichtigt. Weiterhin werden die Empfehlungen des Herstellers berücksichtigt und umgesetzt.

Sind kritische Funktionen (Statistik, Tracking, Drittanbieter-Plugins etc.) bekannt?

Nein.

Sind Sicherheitslücken, Risiken oder sonstige Probleme bekannt?

Nein.

Anbieter	Hoster	Webseite	Dokumentation
mRaP GmbH		https://hellocash.de/	https://intercom.help/hellocash-faq/en/collections/130919-faq-deutsch

Was ist Zweck des Einsatzes?

Abwicklung der Kassen-Buchhaltung, Kassierung von Geschäftsvorfällen.

Welche Arten von Daten werden gespeichert oder verarbeitet?

- Namen und Anschriften von Kunden und Geschäftspartnern
- Allgemeine Buchhaltungsdaten
- Elektronische buchhaltungsrelevante Dokumente
- Kontenstände (Debitoren- und Kreditoren-Kontokorrent)

Findet eine automatisierte Datenverarbeitung statt?

Ja, Daten werden mittels elektronischer Einrichtungen editiert und gespeichert.

Werden Zugriffe beschränkt?

Ja, es existiert eine Benutzerverwaltung, welche die Festlegung von Gruppen und Berechtigungen für einzelne Operationen zulässt. Die Administration stellt eine weitestgehende Beschränkung des Zugangs sicher.

Wird das Verfahren selbst oder durch Dritte verwaltet?

Das Verfahren wird durch Dritte verwaltet, anders könnten die weitreichenden Anforderungen der GoBD und Kassenverordnung nicht eingehalten werden.

Liegt ein Vertrag über die Auftragsverarbeitung mit dem Anbieter vor?

Es besteht ein Vertrag mit dem Anbieter.

Wie ist das Verfahren gegen unbefugte Zugriffe und Datenverlust geschützt?

Die im ADV-Vertrag festgelegten TOM stellen Zugriffsschutz und Integrität sicher. Durch eine strenge Benutzerverwaltung und häufige Sicherheitsupdates wird der Zugriffsschutz zusätzlich verstärkt. Die Anwendung sind einzeln durch eine eigene Benutzerverwaltung geschützt; die Datenbank ist verschlüsselt.

Gibt der Hersteller Hinweise zur Konformität mit den Vorschriften der DSGVO?

Die allgemeinen Empfehlungen zur IT-Sicherheit werden berücksichtigt. Weiterhin werden die Empfehlungen des Herstellers berücksichtigt und umgesetzt. Der Hersteller garantiert die DSGVO-Konformität.

Sind kritische Funktionen (Statistik, Tracking, Drittanbieter-Plugins etc.) bekannt?

Nein.

Sind Sicherheitslücken, Risiken oder sonstige Probleme bekannt?

Nein.

Anbieter	Webseite	Dokumentation
tickettoaster GmbH	https://tickettoaster.de/	nur intern verfügbar

Was ist Zweck des Einsatzes?

1. Vertrieb von Tickets
2. Abwicklung von Gutscheinen, Stornierungen, Umbuchungen und sonstiger Daten
3. Erstellen anonymisierter Statistiken
4. Export in die Finanzbuchhaltung

Welche Arten von Daten werden gespeichert oder verarbeitet?

- Namen, E-Mailadresse und Anschrift der Kunden

Findet eine automatisierte Datenverarbeitung statt?

Ja, Daten werden mittels elektronischer Einrichtungen editiert und gespeichert.

Werden Zugriffe beschränkt?

Ja, es existiert eine Benutzerverwaltung, welche die Festlegung von Gruppen und Berechtigungen für einzelne Operationen zulässt. Die Administration stellt eine weitestgehende Beschränkung des Zugangs sicher.

Wird das Verfahren selbst oder durch Dritte verwaltet?

Das Verfahren wird vom Anbieter verwaltet.

Liegt ein Vertrag über die Auftragsverarbeitung mit dem Anbieter vor?

Es besteht ein Vertrag mit dem Anbieter.

Wie ist das Verfahren gegen unbefugte Zugriffe und Datenverlust geschützt?

Die im ADV-Vertrag festgelegten TOM stellen Zugriffsschutz und Integrität sicher. Durch eine strenge Benutzerverwaltung und häufige Sicherheitsupdates wird der Zugriffsschutz zusätzlich verstärkt.

Gibt der Hersteller Hinweise zur Konformität mit den Vorschriften der DSGVO?

Es sind keine Hinweise vorhanden. Die allgemeinen Empfehlungen zur IT-Sicherheit werden berücksichtigt.

Sind kritische Funktionen (Statistik, Tracking, Drittanbieter-Plugins etc.) bekannt?

Nein.

Sind Sicherheitslücken, Risiken oder sonstige Probleme bekannt?

Die Angabe einer Telefonnummer ist laut Hersteller verpflichtend. Besucher werden darauf hingewiesen, dass sie eine ungültige Nummer angeben dürfen.

Anbieter	Hoster	Webseite	Dokumentation
WordPress	Hetzner Online GmbH	https://wordpress.org/	https://codex.wordpress.org/de:Hauptseite

Was ist Zweck des Einsatzes?

1. Bereitstellen statischer und dynamischer Informationen über den Verein und seine Veranstaltungen
2. Ermöglichung der Kontaktaufnahme über Formulare
3. Ermöglichung der Registrierung für Vereinsveranstaltungen über Formulare

Welche Arten von Daten werden gespeichert oder verarbeitet?

- E-Mailadresse und Namen von Benutzern
- Zustimmung zur Verarbeitung von Cookies
- IP-Adressen im Log des Hosting-Anbieters
- Bei Formularübermittlungen i.d.R. Name, E-Mailadresse und Anschrift sowie weitere dort benannte Daten

Findet eine automatisierte Datenverarbeitung statt?

Ja, ADV-Vertrag liegt vor. Es erfolgt eine Weiterleitung von Formularantworten an vereinseigene E-Mailadressen.

Werden Zugriffe beschränkt?

Ja, es existiert eine Benutzerverwaltung, welche die Festlegung von Gruppen und Berechtigungen für einzelne Operationen zulässt. Die Administration stellt eine weitestgehende Beschränkung des Zugangs sicher.

Wird das Verfahren selbst oder durch Dritte verwaltet?

Das Verfahren wird selbst auf einem eigenen Webspace bzw. vServer verwaltet.

Liegt ein Vertrag über die Auftragsverarbeitung mit dem Anbieter vor?

Es besteht ein Vertrag mit dem Hosting-Anbieter.

Wie ist das Verfahren gegen unbefugte Zugriffe und Datenverlust geschützt?

Die im ADV-Vertrag festgelegten TOM stellen Zugriffsschutz und Integrität sicher. Durch eine strenge Benutzerverwaltung und häufige Sicherheitsupdates wird der Zugriffsschutz zusätzlich verstärkt.

Gibt der Hersteller Hinweise zur Konformität mit den Vorschriften der DSGVO?

Es sind keine unmittelbaren Hinweise vorhanden. Gemäß allgemeiner Hinweise wird ein Plug-In zur Herstellung der DSGVO-Konformität verwendet.

Sind kritische Funktionen (Statistik, Tracking, Drittanbieter-Plugins etc.) bekannt?

Alle bisher bekannten kritischen Funktionen wurden sukzessive deaktiviert, Risiken sind somit behoben. Die Administratoren prüfen regelmäßig das System selbst sowie alle Plug-Ins auf Sicherheitsupdates und Risiken.

Es werden folgende WordPress-Plugins eingesetzt, über welche personenbezogene Daten verarbeitet werden:

- Quforms für Formularantworten
- Contact Form 7 für die allgemeine Kontaktaufnahme
- EU Cookie Law

Hierbei erhalten Hersteller oder andere Dritte keinen Zugriff auf die verarbeiteten Daten.

Tracking-Funktionen und Analysetools sind ausgeschaltet oder anonymisieren statistische Daten.

Sind Sicherheitslücken, Risiken oder sonstige Probleme bekannt?

Folgende Risiken sind bekannt:

- Das Plugin QForms speichert gesendete Anfragen in der Datenbank zwischen. Die PR-Mitarbeiter sind angewiesen, die Formulare möglichst so einzustellen, dass keine Daten auf der Datenbank gespeichert werden. Die Datenbank ist regelmäßig zu leeren.

Anbieter	Hoster	Webseite	Dokumentation
Zammad	Hetzner Online GmbH	https://zammad.com/de	https://docs.zammad.org/en/latest/

Was ist Zweck des Einsatzes?

1. Interner Workflow
2. Abwicklung von Kundenanfragen

Welche Arten von Daten werden gespeichert oder verarbeitet?

- E-Mailadresse und Namen von Benutzern
- Anliegen von Kunden und Geschäftspartnern, die per E-Mail oder Twitter eingereicht werden
- Namen, E-Mailadresse und Anschrift sowie weitere dort benannte Daten aus Formularen (Bewerbungen, Panels, Musiker, Künstler, Gäste etc.)
- Sonstige betriebswirtschaftliche Daten

Findet eine automatisierte Datenverarbeitung statt?

Ja, Daten werden mittels elektronischer Einrichtungen editiert und gespeichert.

Werden Zugriffe beschränkt?

Ja, es existiert eine Benutzerverwaltung, welche die Festlegung von Gruppen und Berechtigungen für einzelne Operationen zulässt. Die Administration stellt eine weitestgehende Beschränkung des Zugangs sicher.

Wird das Verfahren selbst oder durch Dritte verwaltet?

Das Verfahren wird selbst auf einem eigenen Webspace bzw. vServer verwaltet.

Liegt ein Vertrag über die Auftragsverarbeitung mit dem Anbieter vor?

Es besteht ein Vertrag mit dem Hosting-Anbieter.

Wie ist das Verfahren gegen unbefugte Zugriffe und Datenverlust geschützt?

Die im ADV-Vertrag festgelegten TOM stellen Zugriffsschutz und Integrität sicher. Durch eine strenge Benutzerverwaltung und häufige Sicherheitsupdates wird der Zugriffsschutz zusätzlich verstärkt.

Gibt der Hersteller Hinweise zur Konformität mit den Vorschriften der DSGVO?

Es sind keine speziellen Hinweise vorhanden. Die allgemeinen Empfehlungen zur IT-Sicherheit werden berücksichtigt.

Sind kritische Funktionen (Statistik, Tracking, Drittanbieter-Plugins etc.) bekannt?

Nein.

Sind Sicherheitslücken, Risiken oder sonstige Probleme bekannt?

Die Löschung von Daten muss manuell erfolgen. Die Administratoren sind angewiesen, in regelmäßigen Abständen geschlossene Tickets und inaktive Benutzer zu löschen.

Anbieter	Hoster	Webseite	Dokumentation
Hetzner Online GmbH	Hetzner Online GmbH	https://www.hetzner.de/	https://www.hetzner.de/rechtliches/datenschutz

Was ist Zweck des Einsatzes?

Allgemeine Kommunikation per E-Mail.

Welche Arten von Daten werden gespeichert oder verarbeitet?

- grundsätzlich jede Form betrieblicher personenbezogener Daten

Findet eine automatisierte Datenverarbeitung statt?

Ja, Daten werden mittels elektronischer Einrichtungen editiert und gespeichert.

Werden Zugriffe beschränkt?

Ja, es existiert eine Benutzerverwaltung, welche die granulare Festlegung von Berechtigungen zulässt. Die Administration stellt eine weitestgehende Beschränkung des Zugangs sicher. Benutzer haben nur Zugriff auf ihre eigenen sowie Gruppen-E-Mails.

Wird das Verfahren selbst oder durch Dritte verwaltet?

Die Verwaltung erfolgt über den eigenen Webspace.

Liegt ein Vertrag über die Auftragsverarbeitung mit dem Anbieter vor?

Es liegt ein Vertrag mit dem Anbieter vor.

Wie ist das Verfahren gegen unbefugte Zugriffe und Datenverlust geschützt?

Die im ADV-Vertrag festgelegten und im Datenschutzkonzept beschriebenen TOM stellen Zugriffsschutz und Integrität sicher. Durch eine strenge Benutzerverwaltung und häufige Sicherheitsupdates wird der Zugriffsschutz zusätzlich verstärkt. Die virtuelle Maschine selbst und die Anwendung sind einzeln durch eine eigene Benutzerverwaltung geschützt; die Datenbank ist verschlüsselt.

Gibt der Hersteller Hinweise zur Konformität mit den Vorschriften der DSGVO?

Die allgemeinen Empfehlungen zur IT-Sicherheit werden berücksichtigt. Weiterhin werden die Empfehlungen des Herstellers berücksichtigt und umgesetzt.

Sind kritische Funktionen (Statistik, Tracking, Drittanbieter-Plugins etc.) bekannt?

Nein.

Sind Sicherheitslücken, Risiken oder sonstige Probleme bekannt?

Nein.

Anbieter	Webseite	Dokumentation
Alphabet Inc.	https://cloud.google.com/	https://cloud.google.com/security/compliance/gdpr/?hl=de

Was ist Zweck des Einsatzes?

Allgemeine Kommunikation per E-Mail. *Es ist vorgesehen, das Verfahren aufzugeben und vollständig auf Hetzner-E-Mail umzusteigen.*

Welche Arten von Daten werden gespeichert oder verarbeitet?

- grundsätzlich jede Form betrieblicher personenbezogener Daten

Findet eine automatisierte Datenverarbeitung statt?

Ja, Daten werden mittels elektronischer Einrichtungen editiert und gespeichert.

Werden Zugriffe beschränkt?

Ja, es existiert eine Benutzerverwaltung, welche die granulare Festlegung von Berechtigungen zulässt. Die Administration stellt eine weitestgehende Beschränkung des Zugangs sicher. Benutzer haben nur Zugriff auf ihre eigenen sowie Gruppen-E-Mails.

Wird das Verfahren selbst oder durch Dritte verwaltet?

Die Verwaltung erfolgt durch eigenes Personal.

Liegt ein Vertrag über die Auftragsverarbeitung mit dem Anbieter vor?

Es liegt ein Vertrag mit dem Anbieter vor.

Wie ist das Verfahren gegen unbefugte Zugriffe und Datenverlust geschützt?

Die im ADV-Vertrag festgelegten und im Datenschutzkonzept beschriebenen TOM stellen Zugriffsschutz und Integrität sicher. Durch eine strenge Benutzerverwaltung und häufige Sicherheitsupdates wird der Zugriffsschutz zusätzlich verstärkt. Die virtuelle Maschine selbst und die Anwendung sind einzeln durch eine eigene Benutzerverwaltung geschützt; die Datenbank ist verschlüsselt.

Gibt der Hersteller Hinweise zur Konformität mit den Vorschriften der DSGVO?

Die allgemeinen Empfehlungen zur IT-Sicherheit werden berücksichtigt. Weiterhin werden die Empfehlungen des Herstellers berücksichtigt und umgesetzt. Der Hersteller garantiert für die DSGVO-Konformität.

Sind kritische Funktionen (Statistik, Tracking, Drittanbieter-Plugins etc.) bekannt?

Nein.

Sind Sicherheitslücken, Risiken oder sonstige Probleme bekannt?

Nein.

Anbieter	Hoster	Webseite	Dokumentation
DokuWiki	Hetzner Online GmbH	https://www.dokuwiki.org/dokuwiki	https://www.dokuwiki.org/manual

Was ist Zweck des Einsatzes?

1. Abwicklung von Helferbewerbungen und -verträgen
2. Speicherung von Daten über zurückliegende Helfertätigkeiten

Welche Arten von Daten werden gespeichert oder verarbeitet?

- E-Mailadresse und Namen von Benutzern
- Namen, E-Mailadresse und Anschrift von Helfern und Bewerbungen
- Angaben zu Tätigkeiten und Ausbildung
- Angaben zu Leistungen bei früheren Helfertätigkeiten

Findet eine automatisierte Datenverarbeitung statt?

Ja, Daten werden mittels elektronischer Einrichtungen editiert und gespeichert.

Werden Zugriffe beschränkt?

Ja, es existiert eine Benutzerverwaltung, welche die Festlegung von Gruppen und Berechtigungen für einzelne Bereiche zulässt. Die Administration stellt eine weitestgehende Beschränkung des Zugangs sicher.

Es handelt sich um einen technisch besonders geschützten Bereich innerhalb der DokuWiki-Installation, auf welchen nur Vorstandsmitglieder und besonders bevollmächtigte Helfermanager Zugriff haben.

Wird das Verfahren selbst oder durch Dritte verwaltet?

Das Verfahren wird selbst auf einem eigenen Webspace bzw. vServer verwaltet.

Liegt ein Vertrag über die Auftragsverarbeitung mit dem Anbieter vor?

Es besteht ein Vertrag mit dem Hosting-Anbieter.

Wie ist das Verfahren gegen unbefugte Zugriffe und Datenverlust geschützt?

Die im ADV-Vertrag festgelegten TOM stellen Zugriffsschutz und Integrität sicher. Durch eine strenge Benutzerverwaltung und häufige Sicherheitsupdates wird der Zugriffsschutz zusätzlich verstärkt.

Gibt der Hersteller Hinweise zur Konformität mit den Vorschriften der DSGVO?

Es sind keine Hinweise vorhanden. Die allgemeinen Empfehlungen zur IT-Sicherheit werden berücksichtigt.

Sind kritische Funktionen (Statistik, Tracking, Drittanbieter-Plugins etc.) bekannt?

Nein.

Sind Sicherheitslücken, Risiken oder sonstige Probleme bekannt?

Nein.

Anbieter	Hoster	Webseite	Dokumentation
WordPress	Hetzner Online GmbH	https://wordpress.org/	https://codex.wordpress.org/de:Hauptseite

Was ist Zweck des Einsatzes?

Bereitstellung einer E-Learning-Umgebung für Mitglieder und Mitarbeiter, insbesondere um Belehrungen online abwickeln zu können.

Sonstige Angaben

Benutzer werden einzeln auf Anfrage angelegt. Das WordPress-System ist isoliert, sodass diese keinen Zugriff auf personenbezogene Daten erhalten. Bei der Registrierung müssen die Datenschutzbedingungen anerkannt werden.

Es wird zusätzlich das WordPress-Plugin Sensei LMS eingesetzt. Dieses sendet keine Daten an Dritte und greift auf die WordPress-eigene Benutzerverwaltung zurück.

Das E-Learning-Angebot ist ein Zusatzangebot; es werden weiterhin Live-Schulungen und -Belehrungen angeboten. Es besteht keine Verpflichtung zur Nutzung der Plattform.

VERFAHRENSBESCHREIBUNG - CLUBDESK

Anbieter	Webseite	Dokumentation
reeweb AG	https://www.clubdesk.de/de/startseite.html	https://www.clubdesk.de/de/ihre-vorteile/haeufige-fragen.html

Was ist Zweck des Einsatzes?

- Verwaltung der Mitgliedsdaten und Mitarbeiterdaten
- Mitgliederkommunikation
- Nachhalten der Datenschutz- und Arbeitsschutzunterweisungen
- Nachhalten der Berechtigungen und Datenzugriffe über Rollen

Welche Arten von Daten werden gespeichert oder verarbeitet?

- Allgemeine Personendaten (Name, Anschrift, Geburtsdatum, E-Mailadresse) der Mitglieder
- Informationen zum Mitglieds- bzw. Mitarbeiterstatus (Eintritt, Austritt)
- Informationen zu Berechtigungen, Funktionen und Rollen innerhalb des Vereins

Findet eine automatisierte Datenverarbeitung statt?

Ja, Daten werden mittels elektronischer Einrichtungen editiert und gespeichert.

Werden Zugriffe beschränkt?

Ja, es existiert eine Benutzerverwaltung, welche die granulare Festlegung von Berechtigungen für einzelne Daten und Operationen zulässt. Die Administration stellt eine weitestgehende Beschränkung des Zugangs sicher.

Wird das Verfahren selbst oder durch Dritte verwaltet?

Es handelt sich um ein durch den Anbieter verwaltetes Verfahren auf dessen Cloud-Infrastruktur. Die direkte Administration erfolgt durch den Verein selbst.

Liegt ein Vertrag über die Auftragsverarbeitung mit dem Anbieter vor?

Es liegt ein Vertrag mit dem Anbieter vor.

Wie ist das Verfahren gegen unbefugte Zugriffe und Datenverlust geschützt?

Die im ADV-Vertrag festgelegten und im Datenschutzkonzept beschriebenen TOM stellen Zugriffsschutz und Integrität sicher. Durch eine strenge Benutzerverwaltung und häufige Sicherheitsupdates wird der Zugriffsschutz zusätzlich verstärkt. Die virtuelle Maschine selbst und

die Anwendung sind einzeln durch eine eigene Benutzerverwaltung geschützt; die Datenbank ist verschlüsselt.

Gibt der Hersteller Hinweise zur Konformität mit den Vorschriften der DSGVO?

Die allgemeinen Empfehlungen zur IT-Sicherheit werden berücksichtigt. Weiterhin werden die Empfehlungen des Herstellers berücksichtigt und umgesetzt (siehe Link in der Kopfzeile).

Der Hersteller garantiert für die Einhaltung der datenschutzrechtlichen Bestimmungen gemäß DSGVO.

Sind kritische Funktionen (Statistik, Tracking, Drittanbieter-Plugins etc.) bekannt?

Nein.

Sind Sicherheitslücken, Risiken oder sonstige Probleme bekannt?

Nein.