Datenschutzkonzept

der Pony Events Federation e.V.

GELTUNGSBEREICH

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

Sie richtet sich insbesondere an:

- Vorstandsmitglieder
- Veranstaltungsmitarbeiter
- 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.

BEGRIFFSDEFINITIONEN

PERSONENBEZOGENE DATEN

Einzelangaben über persönliche oder sachliche Verhältnisse einer natürlichen Person (Betroffener). Beispiele: Name, Vorname, Geburtstag, Adressdaten, Bestelldaten, E-Mail-Inhalte.

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.

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

Der Vorstand führt ein Verzeichnis der Verarbeitungstätigkeiten, in welchem er das 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.

Der Vorstand evaluiert das Verzeichnis regelmäßig, mindestens ein Mal 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

Zugang zu personenbezogenen Daten erhält nur, wer auf das Datengeheimnis verpflichtet wurde und die Daten zur Erfüllung seiner Aufgaben benötigt.

Der Vorstand führt hierzu ein Verzeichnis der Zugänge und Benutzerkonten, welches regelmäßig kritisch geprüft wird. Wird ein Zugang nicht mehr benötigt, ist dieser unverzüglich zu löschen.

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.

IT-FACHVERFAHREN, HARD- UND SOFTWARE

IT-Fachverfahren, Cloud-Dienste, Hosting-Dienste, übrige Online-Dienste sowie Soft- und Hardware werden vor der Nutzung bzw. Auswahl nach Datenschutzbelangen geprüft.

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.

Es ist sichere Hardware zu verwenden, wobei wo möglich auf einen Internetzugang verzichtet werden soll.

Vereinstätigkeiten sollen nicht auf privater Hardware bzw. nur innerhalb eines geschützten Bereichs 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.

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 gehalten werden.

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.

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.

ÜBERGANGSZEIT

Zur Umsetzung der Anforderungen der DSGVO evaluiert der Vorstand die Gesamtheit der Vereinstätigkeiten und trifft geeignete Maßnahmen, um die Vorgaben der DSGVO umzusetzen und darüber hinaus einen transparenten und kundenorientierten Umgang mit personenbezogenen Daten zu etablieren.

Bis zum Inkrafttreten der DSGVO sind alle Prozesse und eingesetzten (IT-) Verfahren zu dokumentieren, zu überprüfen und ggf. zu optimieren.

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.
- Digitale Daten in Online- und Cloud-Speichern werden logisch gelöscht.
- Digitale Datenträger, welche nicht wiederverwendbar sind (CD-ROM, CD-R), werden so zerstört, dass sie mit üblichen Mitteln nicht mehr ausgelesen werden können (Zerkleinern, Verkratzen, Verbrennen). 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.

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.

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.

Behördenauskünfte werden durch den Datenschutzbeauftragten unverzüglich beantwortet.

Kamen, den 05.05.2018

- Der Vorstand -