DATENSCHUTZKONZEPT

DER PONY EVENTS FEDERATION E.V.

Revision 2.0
19.04.2022

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 führt hierzu ein Verzeichnis der Zugänge und Benutzerkonten, welches regelmäßig kritisch geprüft wird. 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,
- Webseiten,
- Social-Media- und Nachrichtendienste einschließlich Foren- und Wiki-Lösungen und
- übrige Anwendersoftware sowie
- Add-Ins, Plug-Ins oder sonstige Erweiterungen zu obengenannten Lösungen,

unabhängig davon, ob diese auf eigener Hardware (On-Premise), auf gemieteter aber selbst gewarteter Hardware (Hosting, vServer) oder auf gemieteter und (teilweise) fremd verwalteter Hardware (Managed Hosting) betrieben oder als Cloud-Dienst bzw. Software as a Service in Anspruch genommen wird.

PRÜFUNG UND AUSWAHL

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, sicherer Hardware,
- ein Online-Dienst auf einem selbstverwalteten Server oder Webspace oder
- ein weniger automatisiertes bzw. analoges Verfahren oder
- ein Verfahren mit geringerer Datenerhebung

mit einem höheren Schutzniveau zur Verfügung stehen und wirtschaftlich genutzt werden können. Cloud-Dienste und Drittanbieterdienste sind jedoch zu bevorzugen, soweit diese – etwa durch bessere TOM, professionellere Administration oder sicherere Hardware – Vorteile gegenüber selbst betriebenen Verfahren bieten.

INFRASTRUKTUR, WARTUNG UND SICHERHEIT

Vor der Einführung wird jede Lösung einer Stufe innerhalb eines Infrastruktur-Sicherheitskonzeptes zugeordnet. Die Einstufung orientiert sich daran, wie Aufgaben und Verantwortlichkeiten für Absicherung, Wartung, Aktualisierung und Integrität der Lösung zwischen der PEF und einem eventuellen Anbieter oder Hoster verteilt sind.

Hierbei werden Software und die Hardware, auf welcher diese installiert und ausgeführt wird, stets als eine Einheit betrachtet.

Die Einstufung erfolgt, falls vorhanden, anhand des vorliegenden ADV-Vertrages sowie sonstiger Verträge, welche die Verantwortlichkeiten und Aufgaben von PEF und Betreiber regeln. Bei den Stufen 4 bis 6 erfolgt die Einstufung nach Rücksprache mit den Administratoren bzw. Entwicklern der Lösung. Die Einstufung nimmt der Datenschutzbeauftragte gemeinsam mit den Administratoren der Lösung vor.

Bei der Einstufung ist hauptsächlich die Installation der Lösung relevant und weniger der Ort der Ausführung. Wird z.B. ein Fachverfahren als Cloud-Lösung genutzt, aber auf eigener und selbstverwalteter Hardware eingesetzt, gilt die Stufe 1 und nicht die Stufe 4. Dies entspringt der Annahme, dass der Ort der Ausführung solcher Fremdlösungen irrelevant ist, da die Integrität durch die Integrität des aufrufenden Clients selbst nicht berührt ist. Hiervon wird daher abgewichen, wenn der Client doch unmittelbar Auswirkungen auf die Integrität der Lösung haben kann.

Stufe	Bedeutung
1	Fremdverfahren (Cloud-Produkte, Software as a Service (SaaS) o.ä.) Es handelt sich um eine Lösung auf fremder Hardware, welches die PEF als Endverbraucher nutzt. Die PEF hat außer Benutzerverwaltung und einfache Konfiguration keine Möglichkeiten, Einfluss zu nehmen und hat keinen Zugriff auf die Hardwareebene. Die Verantwortung für Sicherheit, Funktion und Wartung liegt beim Anbieter.
2	Gemietete fremdgewartete Hardware (Managed Hosting) Es handelt sich um eine Lösung auf fremder Hardware. Die PEF hat umfassende Konfigurationsmöglichkeiten, allerdings garantiert der Anbieter für Sicherheit und Wartung auf Hardware- und Betriebssystemebene (einschließlich Absicherung der Hardware gegen Angriffe), ggf. auch grundlegend für die Lösung an sich. Die PEF hat mindestens die Verantwortung für Teile der Lösung, die von eigenen Einstellungen oder Anpassungen betroffen sind.

Stufe	Bedeutung
3	Gemietete selbstgewartete Hardware (Hosting, vServer) Die PEF mietet einen (virtuellen) Server oder eine ähnliche (virtuelle) Hardware und betreibt diese wie eigene Hardware. Es werden eine oder mehrere Lösungen hierauf installiert, welche ebenfalls vollständig selbstgewartet werden. Die Verantwortlichkeit für Wartung, Sicherheit und Funktion liegt bis zur Betriebssystemebene vollständig bei der PEF. Der Anbieter hat unter Umständen auch keinen Zugriff auf die Hardware (außer im Rahmen von Notfallarbeiten) und garantiert nur für die Integrität der Hardware selbst.
4	Eigene selbstgewartete Hardware, lokale Installation Die PEF installiert eine Software auf eigener Hardware, die Software ist allerdings nur lokal nutzbar. Eine Internetverbindung kann bestehen; die Hardware tritt jedoch nicht als Server, sondern rein als Client auf. Die PEF ist für Hardware-, Betriebssystem- und Softwareebene selbst verantwortlich.
5	Eigene selbstgewartete Hardware, serverartige Nutzung Die PEF installiert eine Software auf eigener Hardware; die Software kann als Server in einem lokalen Netzwerk oder im Internet auftreten. Die PEF ist für Hardware-, Betriebssystem- und Softwareebene vollständig selbst verantwortlich.
6	Eigene selbstgewartete Hardware besonderer Art (IoT, Embedded Systems o.ä.) Die PEF installiert eine Software auf eigener Hardware, welche auch als Server in einem lokalen Netzwerk oder im Internet auftreten kann. Es handelt sich hierbei nicht um einen klassischen PC, sondern einen Computer, der typischerweise im IoT-Umfeld eingesetzt wird (Raspberry Pi, Arduino etc.), und in der Regel andere Hardware steuert, oder um ein ähnlich funktionierendes Gerät. Hierunter fallen u.a. Einrichtungen zur automatischen Eintrittskartenkontrolle oder steuerbare Anzeigegeräte. Die PEF ist für Hardware-, Betriebssystem- und Softwareebene vollständig selbst verantwortlich.

Es gelten für die einzelnen Stufen folgende regelmäßig auszuführende Aufgaben für die Administration:

Stufe	Aufgaben
1	Die Administration informiert sich regelmäßig über Sicherheit, Integrität und Funktion der Lösung. Sie lässt sich durch den Anbieter über geeignete Kanäle über Zwischenfälle und Probleme informieren, abonniert etwa einen Newsletter oder hinterlegt eine E-Mailadresse für Notfälle.
2	Über die Aufgaben nach Stufe 1 hinaus: Die Administration informiert sich in regelmäßigen Abständen selbstständig über mögliche Probleme, insbesondere solche, die die gemachten Einstellungen und vorgenommenen Anpassungen berühren. Sie informiert sich regelmäßig, ob es bekannte Konflikte oder hierdurch verursachte Sicherheitslücken gibt und ob die eigenen Anpassungen oder Einstellungen ggf. obsolet sind. Die Administration reagiert bei Bekanntwerden von Zwischenfällen oder Problemen unmittelbar nach dem unten beschriebenen Ablaufplan, wobei der Anbieter unmittelbar informiert und um Abhilfe gebeten wird, sofern seine Verantwortlichkeit berührt ist. Es wird regelmäßig geprüft, ob Updates vorliegen.
3	Wie Stufe 2, wobei sich die proaktive Recherche auf die Betriebssystemebene und dort gemachte Einstellungen und Anpassungen ausweitet.
4	Wie Stufe 3, wobei sich die proaktive Recherche auf die Hardwareebene (insbesondere Treiber) ausweitet. Zusätzlich ist geeignete Software zur Absicherung der Hardware zu nutzen.

Stufe	Aufgaben
5	Über die Aufgaben nach Stufe 4 hinaus: Es sind Werkzeuge zur Überwachung der Integrität des Systems und zur Früherkennung von Angriffen zu nutzen. Die Integrität der Netzwerkverbindungen ist regelmäßig zu prüfen.
6	Die Administration legt vor jeder Inbetriebnahme im Einvernehmen mit dem Datenschutzbeauftragten fest, welche Maßnahmen erforderlich sind, um die Integrität der Lösung zu gewährleisten und setzt diese um.

VERFAHRENSVERZEICHNIS

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
- Einstufung in das mehrstufige Infrastruktur-Sicherheitskonzept

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

Der Vorstand identifiziert bei der Prüfung der Freigabe Risiken und datenschutzrelevante Problematiken und wägt ab, ob diese angesichts der übrigen Vorteile der Lösung vertretbar sind. In jedem Fall werden solche Risiken in das Verfahrensverzeichnis aufgenommen und es werden geeignete Maßnahmen definiert, welche negative Auswirkungen auf den Datenschutz bestmöglich einschränken.

ALLGEMEINE IT-SICHERHEITSVORKEHRUNGEN

Der (parallele) Einsatz anderer 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 allgemein 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.

Die mit der Betreuung von Hard- oder Software betrauten Personen abonnieren den Bürger-CERT-Newsletter des BSI und prüfen regelmäßig einschlägige Online-Quellen, ob für sie relevante Sicherheitslücken gemeldet wurden. Weiterhin informieren sie sich regelmäßig beim Anbieter einer Lösung, ob dieser Zwischenfälle oder Sicherheitslücken gemeldet hat. Wenn möglich, lassen sich diese vom Anbieter aktiv informieren.

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.

Hiernach erfolgt, soweit rechtlich erforderlich, eine Information der betroffenen Personen und/oder der zuständigen Datenschutzbehörde.

IT-SICHERHEITSVORFÄLLE

Bei IT-Sicherheitsvorfällen gilt der folgende Ablaufplan neben der Meldekette bei Datenschutzvorfällen. Der Plan tritt in Kraft, sobald

- eine Sicherheitslücke oder ein sicherheitsrelevanter Zwischenfall von einem Anbieter o.ä. gemeldet oder selbst festgestellt wurden,
- eine entsprechende (allgemeine) Meldung Anlass zur Sorge gibt, dass es zu einem sicherheitsrelevanten Zwischenfall kommen könnte oder
- ein vergleichbarer Zwischenfall eintritt oder gemeldet wird.

Es ist wie folgt zu verfahren:

<table>
<tr><td colspan="2">Eingang einer Meldung bzw. Bekanntwerden eines Zwischenfalls</td></tr>
<tr><td colspan="2">Es wird geprüft, ob tatsächlich ein Sicherheitsrisiko besteht und wer für dessen Behebung verantwortlich ist.</td></tr>
<tr><td colspan="2">Es werden möglichst viele Informationen über den Vorfall gesammelt und lokal gesichert. Ggf. wird ein Backup angefertigt.</td></tr>
<tr><td colspan="2">Es wird geprüft, ob als erste Gegenmaßnahme
1. eine Sperrung des Zugriffs auf die Software,
2. eine Sperrung des Zugriffs auf die Hardware,
3. das Versetzen von Software oder Hardware in einen unveränderlichen Zustand,
4. die Isolation der Soft- oder Hardware (trennen vom Netzwerk, sperren von Ports) oder
5. die Abschaltung der Soft- oder Hardware
sinnvoll und erforderlich sind. Falls nötig, wird die geeignete Gegenmaßnahme getroffen. Die Entscheidung trifft der zuständige Administrator, ggf. nach Rücksprache mit dem Datenschutzbeauftragten.</td></tr>
<tr><td>PEF ist verantwortlich</td><td>Anbieter ist verantwortlich</td></tr>
<tr><td>Es wird recherchiert, wie das Problem gelöst werden kann, eventuell durch die Installation von Updates oder eine Konfigurationsänderung. Kann das Problem nicht selbst gelöst werden, wird ggf. die</td><td>Der Anbieter wird informiert.</td></tr>
</table>

Unterstützung des Anbieters oder einer Fachfirma hinzugezogen.	
Kontrolle des Ergebnisses	
Es wird geprüft, ob das Problem behoben wurde.	
Das Problem wurde behoben	Das Problem kann nicht behoben werden
Die Ursachen für das Problem sowie die Lösung werden aufbereitet und dokumentiert.	Es wird nach endgültigem Scheitern der Reparaturversuche im Einvernehmen mit dem Datenschutzbeauftragten eine Lösung gesucht. Ein Ersatz für die Lösung ist in Betracht zu ziehen.
Die Lösung wird wieder in Betrieb genommen.	Die Lösung bleibt außer Betrieb.

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).

Soweit Daten nicht ständig im Zugriff sein müssen oder nur vorübergehend benötigt werden, werden sie ausschließlich in Papierform oder auf Offline-Datenträgern aufbewahrt.

Für die Dauer und Art der Aufbewahrung ist im Übrigen das Löschkonzept maßgeblich.

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.

Bei Dokumenten oder Daten, für die keine gesetzliche Aufbewahrungsfrist gilt, legt der Ersteller individuell eine Aufbewahrungsfrist fest, welche unter Berücksichtigung der Geschäftsinteressen möglichst kurz zu halten ist. Die Daten werden ausschließlich auf Papier- oder Offline-Datenträgern gespeichert.

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

DATEN MIT KURZER AUFBEWAHRUNGSDAUER

Daten und Dokumente, die nur für einen kurzen, absehbaren Zeitraum (i.d.R. bis zu einem Jahr) aufbewahrt werden sollen, werden unmittelbar mit ihrem Ablaufdatum beschriftet und auf einem Papier- oder Offline-Datenträger einer gesonderten Ablage zugeführt, welche regelmäßig (mind. einmal pro Monat) durchgesehen wird. Bei Überschreiten der Aufbewahrungsfrist werden die Daten und Dokumente unmittelbar vernichtet.

LÖSCHVORMERKUNG

Die mit der Vorgangsbearbeitung beauftragten Mitarbeiter sind angehalten, jederzeit zu prüfen, ob die erstellten oder bearbeiteten Daten und Dokumente noch (für die angegebene Dauer) benötigt werden und ob diese gelöscht oder mit einer Löschvormerkung versehen werden können. Im Zweifelsfall benachrichtigen sie ein Vorstandsmitglied, welches über die Löschung oder Löschvormerkung entscheidet.

Bei Dokumenten, deren Aufbewahrungsdauer bereits bei Ablage feststeht (z.B. Buchhaltungsbelege), werden diese unmittelbar mit dem vorgesehenen Löschdatum versehen. Bei Sammelablagen (Ordnern) kann auch die gesamte Ablage mit einem Löschdatum versehen werden (z.B. Ordner mit allen Buchhaltungsbelegen eines Geschäftsjahres).

Sofern sich die Aufbewahrungsdauer erst zu einem bestimmten Zeitpunkt oder bei Eintritt eines bestimmten Ereignisses ergibt (z.B. Beendigung der Tätigkeit eines Mitarbeiters, Austritt eines Mitglieds), ist das Löschdatum bei Eintritt dieses Ereignisses bzw. Zeitpunktes anzubringen.

Bei elektronischen Daten wird sichergestellt, dass in zusätzlichen Datenfeldern ein Löschdatum angebracht ist (z.B. zusätzliches Datenbankfeld „Löschdatum“ oder „Aufbewahrungsfrist“) oder sich die Aufbewahrungsdauer aus einem anderen Datenfeld ergibt (z.B. bei Buchhaltungsdatum Geschäftsjahr oder Bestelleingang).

Administratoren oder Verfahrensbeauftragte stellen sicher, dass durch regelmäßige Lösch- bzw. Auswertungsläufe, welche zu nach Art der Daten und Systemeigenschaften sinnvollen Zeitpunkten einzuplanen sind, Löschvormerkungen angebracht und zu löschende Datensätze rechtzeitig identifiziert werden können.

Sollte sich ein Löschzeitpunkt technisch nicht speichern oder ableiten lassen, werden die Datensätze regelmäßig im Rahmen der Dateninventur überprüft.

DATENINVENTUR

Mindestens einmal im Jahr überprüft der Vorstand sämtliche Datenträger, Dokumente und Ablagen und identifiziert zu löschende, zu archivierende oder zur Löschung vorzumerkende Datensätze und Dokumente.

Bei der Dateninventur sind insbesondere Dokumente, Systeme und Datenträger zu überprüfen, die über kein festgelegtes Löschdatum verfügen oder bei denen technisch die Anbringung oder Ableitung eines Löschdatums nicht möglich ist.

LÄNGERE AUFBEWAHRUNG BEI REVISION ODER RECHTSSTREIT

Soweit Daten im Rahmen einer gesetzlich vorgeschriebenen oder von Behörden eingeleiteten Prüfung oder im Rahmen eines Rechtsstreits länger als ursprünglich vorgesehen werden, werden diese aus den regulären Verzeichnissen oder Ablagen ausgesondert und, ohne diese Daten zu duplizieren, in einer Fallakte zusammengeführt.

Die Löschung erfolgt, sobald dies nach den Umständen des Einzelfalls möglich ist. Bei Festlegung dieser verlängerten Aufbewahrungsdauer sind gesetzliche Anforderungen sowie Vorgaben von Behörden maßgeblich.

Ungeachtet der längeren Aufbewahrungsdauer ist die Überführung auf Offline-Datenträger zu prüfen.

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 – 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,*	- Nutzer-Berechtigungskonzept - Verwaltung der Nutzerrechte durch Systemadministrator - Anzahl der Administratoren auf das Notwendigste reduziert - Verwenden einer Passwortrichtlinie - Protokollierung von Zugriffen auf kritische Anwendungen

kopiert, verändert oder entfernt werden können.)	- 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 UND VERFAHREN

Die einzelnen Verarbeitungstätigkeiten, Rollenkonzepte und Verfahren werden in einem gesonderten Verzeichnis aufgeführt.