Technische und organisatorische Maßnahmen der kgl. priv. Schützengesellschaft Arnstein (SG Arnstein) gemäß § 64 Absatz 3 BDSG

Maßnahme	Umsetzung der Maßnahme
Zugangskontrolle Unbefugten ist der Zuritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	*Die analogen Daten liegen in abgeschlossenen Schränken im Schützenhaus, zu denen nur die Vorstandschaft einen Schlüssel besitzt.* *Der Rechner der SG ist passwortgeschützt, und nicht mit dem Internet verbunden. Er steht im Schützenhaus, zu dem nur Berechtigte Zutritt haben.*
Zugriffskontrolle Es ist zu 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 Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	*Zugriff auf die Mitgliederverwaltung bzw. auf personenbezogene Daten der Mitglieder ist nur mit der erweiterten Kennung am Rechner der SG möglich.* *Soweit Daten auf privaten Endgeräten verarbeitet werden (Mitgliederverwaltung, Finanzdaten), sind diese Geräte sowie die einzelnen Datenbanken durch entsprechende Zugangsdaten/Passwörter gegen unbefugten Zugriff geschützt.* *Alle mit dem Internet verbundenen Geräte verfügen über aktuelle Sicherheitsupdates, einen aktuellen Virenschutz und sind durch einen Router (Firewall) vor Zugriffen aus dem Internet geschützt.*

Transportkontrolle Es ist zu gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.	*Die Kommunikation mit dem Webauftritt erfolgt verschlüsselt mittels Https. Dies gilt auch für das Kontaktformular.* *Daten der Mitgliederverwaltung werden verschlüsselt mit Programminternen Schnittstellen aus dem Programm ZMI an die zentralen Systeme des BSSB übertragen.* *Die Übertragung von Beitragsdaten an die Finanzinstitute erfolgt über entsprechend verschlüsselte und geschützte Webseiten der Anbieter.*
Übertragungskontrolle Es ist zu gewährleisten, dass überprüft und festgestellt werden kann, an welchen Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können	*Berechtigungskonzept für unterschiedliche Rollen in dem System selbst (z.B. ZMI).* *Aufzeichnung von Zugriffen auf die Datenbank durch das System bzw. die Programme (z.B. ZMI)*
Datenträgerkontrolle Es ist zu verhindern dass Datenträger unbefugt gelesen, kopiert, verändert oder gelöscht werden.	*Bearbeitung in nicht der Öffentlichkeit zugänglichen Büroräumen / Privaträumen.* *Daten werden auf Datenträgern verschlüsselt transportiert.*
Benutzerkontrolle Es ist zu verhindern, dass Unbefugte automatisierte Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung nutzen.	*Reduzierte Zahl der Zugriffsberechtigten (nur Vorstandschaft).* *Berechtigungskonzept für unterschiedliche Rollen in dem System selbst.* *Bearbeitung in nicht der Öffentlichkeit zugänglichen Büroräumen / Privaträumen.*
Eingabekontrolle Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	*Eingabeprotokoll der Software (ZMI)*

Wiederherstellbarkeit Es ist zu gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.	*Die Daten auf den Endgeräten der SG werden regelmäßig gesichert (ca. alle 6 Wochen da wenig Veränderung).* *Die Daten aus der zentralen Mitgliederverwaltung werden bei Veränderung täglich gesichert und stehen im Wesentlichen auch jederzeit über den BSSB zur Wiederherstellung zur Verfügung.*
Zuverlässigkeit Es ist zu gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.	*Updates werden regelmäßig aufgespielt.* *Bei Störung oder Problemen wird das zuständige Mitglied informiert*
Datenintegrität Es ist zu gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.	*Updates werden regelmäßig aufgespielt.* *Funktion wird regemäßig geprüft.*
Auftragskontrolle Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.	*Vereinbarung zur Auftragsverarbeitung und Kontrolle mit Hostinganbieter „All-inkl.com“ abgeschlossen.* *Sonst keine Auftragsverarbeitungen*
Verfügbarkeitskontrolle Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	*Automatisches Backup des Mitgliederdatenbestanden bei Veränderung.* *Tägliche Sicherung der Daten der Mitgliederverwaltung.* *Zusätzlich Daten auch über BSSB wieder abrufbar.*
Trennungskontrolle Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	*Logische Trennung der Daten über Tabellen und Mandate*