Datenschutzrichtlinie des Bayerischen Schützenbundes e.V.

(Stand 05.12.2018)

1. Geltungsbereich

Der Schutz personenbezogener Daten ist dem Bayerischen Schützenbund e.V. (BSSB) ein wichtiges Anliegen. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Deshalb verarbeitet der BSSB die personenbezogenen Daten unserer hauptamtlichen und ehrenamtlichen Mitarbeiter, unmittelbaren Mitglieder (Vereine) und mittelbaren Mitglieder (Vereinsmitglieder) sowie von Dritten in Übereinstimmung mit den anwendbaren Rechtsvorschriften zum Schutz personenbezogener Daten und zur Datensicherheit. Ebenso beziehen sie alle Arten von Betroffenen (Kunden, Lieferanten etc.) in ihren Geltungsbereich mit ein.

Diese Richtlinie hat Gültigkeit für jeglichen Umgang mit personenbezogenen Daten unabhängig, ob diese elektronisch oder in Papierform vonstattengeht.

Sie gilt persönlich und richtet sich an

- die Personen oder Bereiche, die über den Einsatz/die Bereitstellung von Verarbeitungsprozessen und der entsprechenden Anwendungssysteme entscheiden (Landesschützenmeisteramt, Gremien, Geschäftsführer);
- die Personen oder Bereiche, die über die Nutzung von personenbezogenen Daten für die Erfüllung ihrer Aufgaben entscheiden (Gremien des Bayerischen Schützenbundes e.V. sowie Vorstände von unselbständigen Untergliederungen des Bayerischen Schützenbundes e.V., die rechtlich nicht eigenständig sind);
- haupt- und ehrenamtliche Mitarbeiter bzw. Benutzer, d.h. diejenigen, die das zur Verfügung gestellte Anwendungssystem für die Erledigung ihrer betrieblichen Aufgaben nutzen.

2. Erhebung/Verarbeitung von personenbezogenen Daten

2.1 Die Erhebung und Verarbeitung personenbezogener Daten darf nur im Rahmen des rechtlich Zulässigen und insbesondere im Rahmen der Satzung des BSSB erfolgen. Grundsätzlich dürfen nur solche Informationen verarbeitet und genutzt werden, die zur betrieblichen Aufgabenerfüllung erforderlich sind und in Zusammenhang mit dem Verarbeitungszweck stehen.

2.2 Vor Einführung neuer Arten von Erhebungen ist die Zulässigkeit bestimmende Zweckbestimmung der Daten durch den für die Anwendung Verantwortlichen schriftlich zu dokumentieren. Grundsätzlich ist eine Zweckänderung nur dann zulässig, wenn die Verarbeitung mit denjenigen Zwecken vereinbar ist, für die die Daten ursprünglich erhoben worden sind. Die im Rahmen der Zweckänderung genutzten Abwägungskriterien sind einzeln zu prüfen. Die Prüfung ist darüber hinaus auch zu einem ordnungsgemäßen Nachweis zu dokumentieren.

Eine Zweckänderung ist auch zulässig, wenn eine Einwilligung der betroffenen Person durch den Verantwortlichen eingeholt wird. Gleichzeitig hat der für die Verarbeitung Verantwortliche vor der Erhebung bzw. der Speicherung von Daten schriftlich festzulegen, ob und in welcher Art und Weise der gesetzlichen Benachrichtigungspflicht des Betroffenen zu genügen ist.

2.3 Falls andere Stellen Informationen über Betroffene anfordern, dürfen diese ohne Einwilligung des Betroffenen nur gegeben werden, wenn hierfür eine gesetzliche Verpflichtung oder ein die Weitergabe rechtfertigendes legitimes Interesse des BSSB besteht und die Identität des Anfragenden zweifelsfrei feststeht. Im Zweifel ist der Datenschutzbeauftragte kontaktieren.

2.4 Werden personenbezogene Daten nicht beim Betroffenen erhoben, sondern werden beispielsweise bei einer anderen Stelle beschafft, ist der Betroffene nachträglich und umfassend über den Umgang mit seinen Daten zu informieren. Dies gilt auch für die Änderung einer Ziel- und Zweckbestimmung der Datenverarbeitung.

3. Teilnahme an Veranstaltungen des BSSB

Mit der Meldung zu Veranstaltungen des BSSB erklären sich die Teilnehmer aus organisatorischen Gründen mit der Verarbeitung der wettkampfrelevanten personenbezogenen Daten, unter der Angabe von Name, Vereinsname, Verbandszugehörigkeit, Alter, Klasse, Wettkampfbezeichnung, Startnummer, Startzeiten und erzielten Ergebnissen einverstanden. Sie willigen ebenfalls in die Veröffentlichung der Start- und Ergebnislisten, sowie der Erstellung und Veröffentlichung von Fotos in Aushängen, im Internet, in Sozialen Medien und in weiteren Publikationen des BSSB sowie dessen Untergliederungen ein. Aufgrund des berechtigten Interesses des Ausrichters an diesen Ergebnislisten sowie Fotos vom Wettbewerb und / oder Siegertreppchen für die Dokumentation bzw. Bewerbung des Sports in der Öffentlichkeit, besteht auch im Nachhinein kein Anspruch der Teilnehmer zur Löschung ihrer persönlichen Daten aus diesen Ergebnislisten bzw. von Fotos, die im Zusammenhang mit dem Wettkampf gefertigt und veröffentlicht wurden.

4. Datenschutzorganisation

4.1 Der BSSB hat nach Maßgabe des Artikels 37 DS-GVO einen betrieblichen Datenschutzbeauftragten bestellt. Die Kontaktdaten des Datenschutzbeauftragten werden auf der Homepage des BSSB und den offiziellen Printmedien veröffentlicht.

4.2 Der Datenschutzbeauftragte nimmt die ihm kraft Gesetzes und aus dieser Richtlinie zugewiesenen Aufgaben bei weisungsfreier Anwendung seines Fachwissens sowie seiner datenschutzrechtlichen Qualifikation war.

4.3 Der Datenschutzbeauftragte berät das Landesschützenmeisteramt und die Geschäftsführung sowie die Beschäftigten (haupt- und ehrenamtlich) hinsichtlich ihrer Datenschutzpflichten.

4.4 Ihm obliegt die Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien des Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der Mitarbeiter.

4.5 Im Falle risikoreicher Datenverarbeitungen steht der Datenschutzbeauftragte dem Verantwortlichem beratend bei der Abschätzung des Risikos zur Seite.

4.6 Der Datenschutzbeauftragte berichtet unmittelbar der Geschäftsleitung.

4.7 Der Datenschutzbeauftragte wird frühzeitig in allen Datenschutzfragen eingebunden und wird sowohl von der Geschäftsleitung als auch den Beschäftigten bei der Erfüllung seiner Aufgaben unterstützt.

4.8 Die Geschäftsleitung überträgt die Aufgabe des Führens eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DS-GVO) und ggf. des Erteilens von Auskünften (Art. 15 DS-GVO) auf den Datenschutzbeauftragten.

4.9 Für Meldungen, Auskünfte etc. gegenüber den Datenschutzaufsichtsbehörden liegt die bearbeitende Zuständigkeit bei dem Datenschutzbeauftragten.

4.10 Die Bereiche stellen die hierfür erforderlichen Informationen, Unterlagen etc. zur Verfügung. Gleiches gilt für Anfragen, Beschwerden oder Auskunftsersuchen Betroffener.

4.11 Jeder Mitarbeiter kann sich unmittelbar mit Hinweisen, Anregungen oder Beschwerden an den Datenschutzbeauftragten wenden, wobei absolute Vertraulichkeit gewahrt wird.

4.12 Der Datenschutzbeauftragte berichtet dem BSSB über stattgefundene Prüfungen, Beanstandungen und ggf. noch zu beseitigende Organisationsmängel.

5. Beschaffung/Hard- und Software

5.1 Die DV-Hard- und Software sind ausschließlich für betriebliche Aufgaben zu verwenden und gegen Verlust und Manipulation zu sichern.

Eine Nutzung für private Zwecke bedarf der ausdrücklichen Genehmigung.

Private Hard-und Software dürfen nicht zur Verarbeitung personenbezogener Daten Verwendung finden.

Jeder Vorgesetzte ist in seinem Verantwortungsbereich für die Umsetzung der Richtlinie verantwortlich. Die Einhaltung muss von ihm regelmäßig kontrolliert werden.

Die für die Verarbeitungen der eingesetzten Systeme Verantwortlichen stellen sicher, dass ihre Mitarbeiter über diese Richtlinie informiert werden; das gilt auch für temporär Beschäftigte, ehrenamtliche Tätige, Praktikanten und Werkstudenten.

5.2 Die Beschaffung von Hard-und Software erfolgt grundsätzlich auf Anforderung durch den Bayerischen Schützenbund e.V.

Bereits bei der Auswahl von Hard-und Software wird der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen als ein tragendes Kriterium beachtet.

5.3 Falls mit der Beschaffung ein neues Verfahren der Verarbeitung personenbezogener Daten eingeführt werden soll, ist der Datenschutzbeauftragte rechtzeitig vorab zu informieren.

Die Beschaffung erfolgt erst nach Durchführung der Datenschutz-Folgeabschätzung und Stellungnahme des Datenschutzbeauftragten.

Im Zweifel entscheidet die Geschäftsleitung.

5.4 Der BSSB führt ein Verzeichnis der auf Landesebene eingesetzten Hardware und der verwendeten Anwendungsprogramme.

5.5 Bei Verdacht des Diebstahls von Hard-und Software, des unbefugten Zugriffs auf personenbezogene Daten, von Sabotage etc. sind der BSSB und der Datenschutzbeauftrage unverzüglich zu informieren.

6. Verfügbarkeit, Vertraulichkeit und Integrität von Daten

6.1 In Abhängigkeit der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit hat für jedes Verfahren eine dokumentierte Schutzbedarfsfeststellung und Analyse hinsichtlich der Risiken für Betroffene zu erfolgen.

6.2 Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität von Daten wird ein allgemeines Sicherheitskonzept in Abhängigkeit der Schutzbedarfsfeststellung und Risikoanalyse erstellt, das für alle Verfahren verbindlich ist. Hierin ist insbesondere der Stand der Technik ebenso zu berücksichtigen, wie Mittel und Maßnahmen zur Verschlüsselung und Datensicherung. Das Sicherheitskonzept ist hinsichtlich der Wirksamkeit der dort vorgesehenen technisch-organisatorischen Maßnahmen regelmäßig zu überprüfen, zu bewerten und zu evaluieren.

6.3 Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Wirksame Maßnahmen zur Zugangskontrolle an Geräten müssen vorhanden und aktiviert sein. Systemzugänge sind in Abwesenheit stets zu sperren.

6.4 Passwörter ermöglichen einen Zugang zu Systemen und den darin gespeicherten personenbezogenen Daten. Sie stellen eine persönliche Kennung des Nutzers dar und sind nicht übertragbar. Es ist sicherzustellen, dass Passwörter stets unter Verschluss gehalten werden. Passwörter müssen entsprechend dem Sicherheitskonzept angepasst werden.

6.5 Zugriffe auf personenbezogene Daten sollen nur diejenigen Personen erhalten, die im Zuge ihrer Aufgabenwahrnehmung Kenntnis von den jeweiligen Daten erhalten müssen. Zugriffsberechtigungen müssen genau und vollständig festgelegt und dokumentiert sein.

6.6 Datenübertragungen durch öffentliche Netze sind nach Möglichkeit zu verschlüsseln. Eine Verschlüsselung hat zwingend zu erfolgen, falls der Schutzbedarf der personenbezogenen Daten dies erfordert.

6.7 Zu unterschiedlichen Zwecken erhobene personenbezogene Daten sind getrennt voneinander zu verarbeiten. Die Trennung von Daten ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen.

6.8 Wartungsarbeiten an Systemen oder Telekommunikationseinrichtungen durch externe Dienstleister sind zu beaufsichtigen. Ferner ist zu gewährleisten, dass Dienstleister nicht unbefugt auf personenbezogene Daten zugreifen können. Fernwartungszugänge sind nur im Einzelfall zu gewähren und müssen dem Prinzip der minimalen Rechtevergabe folgen. Fernwartungsaktivitäten sind nach Möglichkeit aufzuzeichnen oder zu protokollieren.

7. Transparenz der Datenverarbeitung

7.1 Über Verfahren, die den Umgang mit personenbezogenen Daten betreffen, führt der Datenschutzbeauftragte ein Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 DS-GVO. Gleiches gilt für Veränderungen.

7.2 Unabhängig von dieser Meldung ist der Datenschutzbeauftragte bei der Planung der Einführung neuer Anwendungen bzw. der Veränderung bestehender Verfahren über Zweck und Inhalt der Anwendung und die Erfüllung der Benachrichtigungspflicht zu informieren.

Bei standardisierten Erhebungen (z.B. Eingabefelder auf der Internet-Homepage) ist der Erhebungsbogen dem Datenschutzbeauftragten zur Abstimmung vorzulegen.

7.3 Sollte gem. Art. 9 DS-GVO eine Verarbeitung besonderer Kategorien personenbezogener Daten erfolgen (z. B. Klassifizierung) ist bei jeder Einführung bzw. Veränderung bestehender Verfahren eine Datenschutz-Folgenabschätzung erforderlich.

7.4 Es ist sicherzustellen, dass dem Betroffenen seine Daten auf Wunsch in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden können.

8. Beschwerden

8.1 Jeder Betroffene hat das Recht, sich über eine Verarbeitung seiner Daten zu beschweren, sollte er sich hierdurch in seinen Rechten verletzt fühlen. Ebenso können Beschäftigte Verstöße gegen diese Richtlinie jederzeit anzeigen.

8.2 Die zuständige Stelle für die oben genannten Beschwerden ist der Datenschutzbeauftragte.

9. Datenpanne

9.1 Sollten personenbezogene Daten unrechtmäßig Dritten zugänglich gemacht worden sein, ist darüber unverzüglich die Geschäftsführung und der Datenschutzbeauftragte zu informieren.

9.2 Die Meldung hat alle relevanten Informationen zur Aufklärung des Sachverhalts zu umfassen, insbesondere die empfangende Stelle, die betroffenen Personen sowie Art und Umfang der übermittelten Daten.

9.3 Die Erfüllung einer etwaigen Informationspflicht gegenüber der Aufsichtsbehörde erfolgt durch den Datenschutzbeauftragten. Betroffene werden durch die Geschäftsleitung informiert, wobei der Datenschutzbeauftragte beratend hinzugezogen wird.

10. Datenhaltung/Versand/Löschung

10.1 Die Speicherung von Daten erfolgt grundsätzlich auf den hierzu von Seiten des BSSB zur Verfügung gestellten Netz-/Serverlaufwerken. Eine Speicherung auf mobilen Datenträgern zu dienstlichen Zwecken ist nur in verschlüsselter Form zulässig. Eine Speicherung auf externe Datenspeicher (z.B. Cloud) bedarf der Genehmigung durch den BSSB.

10.2 Soweit technisch bedingt ein anderer Speicherort zwingend erforderlich ist (z.B. Notebook, Desktop-PC) ist der jeweilige Benutzer für die Durchführung der Datensicherung selbst verantwortlich. Ist ein Netzzugang möglich (z.B. bei Notebook mit WLAN, Tablet), ist zumindest einmal wöchentlich der aktuelle Datenbestand auf das für den Benutzer reservierte Netzlaufwerk zu überspielen. Die gewählten Datensicherungsmaßnahmen sind in dem Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren.

10.3 Gesetzliche Aufbewahrungsfristen und Löschungstermine sind von dem über die Verarbeitung der Daten Entscheidenden in seiner Verantwortung zu beachten. Über die Anwendung ZMI gespeicherte personenbezogene Daten werden 5 Jahre nach Beendigung der Mitgliedschaft vorgehalten und automatisch nach Ablauf dieser Frist gelöscht. Daten zur waffenrechtlichen Erlaubnis haben eine Aufbewahrungsfrist von 10 Jahren nach Beendigung der Mitgliedschaft.

10.4 Bei der Weiter-oder Rückgabe nicht mehr benötigter IT-Komponenten ist der Benutzer verpflichtet diese dem BSSB zurückzugeben. Der BSSB wird dafür sorgen, dass sämtliche Daten wirksam gelöscht oder entsprechend zertifizierte Dienstleister mit der Löschung beauftragt werden.

11. Verpflichtung/Schulung der Mitarbeiter

11.1 Jeder Mitarbeiter, der Umgang mit personenbezogenen Daten hat, ist auf einen vertraulichen Umgang mit personenbezogenen Daten und die Einhaltung dieser Richtlinie zu verpflichten.

11.2 Die Verpflichtung erfolgt unter Verwendung des hierzu vorgesehenen Formulars und unter Aushändigung eines Merkblatts durch den BSSB.

11.3 Der Datenschutzbeauftragte ist über die Verpflichtung von Mitarbeitern zwecks von ihr vorzunehmender weiterer Schulungen und die Feststellung evtl. Kontrollbedarfs zu informieren.

12. Externe Dienstleister/Auftragsverarbeitung/Wartung

12.1 Sollen externe Dienstleister erstmals mit der Verarbeitung personenbezogener Daten bzw. einzelnen Verarbeitungsschritten (z.B. Erhebung, Löschung = Entsorgung) bzw. mit Tätigkeiten (z.B. Wartung, Reparatur) beauftragt werden, bei denen sie die Möglichkeit der Kenntnis personenbezogener Daten bekommen, so ist der Datenschutzbeauftragte vor der Beauftragung unter Vorlage des den Anforderungen des Art. 28 DS-GVO genügenden Vertragsentwurfs und der Kriterien der erfolgten bzw. nachfolgend vorgesehenen Auftragskontrolle zu informieren.

12.2 Entsprechendes gilt, falls der BSSB entsprechende Tätigkeiten im Auftrag Dritter wahrnehmen will.

12.3 Der Dienstleister ist im Hinblick auf die mit ihm vertraglich vereinbarten technisch-organisatorischen Maßnahmen regelmäßig zu überprüfen. Das Ergebnis ist zu dokumentieren.

13. Sicherheit der Verarbeitung

13.1 Für jedes Verfahren ist eine dokumentierte Schutzbedarfsfeststellung sowie eine Analyse bzgl. der für den Betroffenen möglichen Risiken zu erstellen. Diese richten sich an der Art, dem Umfang, der Umstände und Zwecke der Verarbeitung sowie der Wahrscheinlichkeit des Eintritts einer solchen Gefahr.

13.2 Neben dieser Richtlinie bestehen technisch-organisatorische Regelungen, die insbesondere zur Realisierung der Datensicherungsgebote des Art. 32 DS-GVO zu treffende Maßnahmen betreffen.

14. Folgen von Verstößen

Ein fahrlässiger oder gar mutwilliger Verstoß gegen diese Richtlinie kann arbeitsrechtliche Maßnahmen nach sich ziehen, einschließlich einer fristlosen oder fristgerechten Kündigung. Ebenso kommen strafrechtliche Sanktionen und zivilrechtliche Folgen wie Schadenersatz in Betracht.

15. Rechenschafts- und Dokumentationspflicht

Die Einhaltung der Vorgaben, die sich aus dieser Richtlinie ergeben, muss jederzeit nachweisbar sein. Eine Nachweisbarkeit hat insbesondere durch eine schlüssige und nachvollziehbare schriftliche Dokumentation hinsichtlich getroffener Maßnahmen und dazugehöriger Abwägungen zu erfolgen.

16. Aktualisierung der Richtlinie; Nachweisbarkeit

16.1 Im Rahmen der Fortentwicklung des Datenschutzrechts sowie technologischer oder organisatorischer Veränderungen wird diese Richtlinie regelmäßig auf einen Anpassungs- oder Ergänzungsbedarf hin überprüft.

16.2 Änderungen an dieser Richtlinie sind formlos wirksam und nach Inkrafttreten zu veröffentlichen und den Mitarbeitern in geeigneter Weise kenntlich zu machen.

Landesschützenmeisteramt