Vereinbarung zur Datenverarbeitung und zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DS-GVO)

(Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO)

Zwischen dem

Bund Bayerischer Jagdaufseher e.V.

Seehühle 13

86477 Adelsried

- Im Weiteren „BBJa e.V.“ genannt-

Und

Vorname Nachname

Straße XX

PLZ Wohnort

- Im Weiteren „Beschäftigter“ genannt-

Der Beschäftigte (im Sinne der DSGVO), hat die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten, wenn er im Namen des BBJa personenbezogene Daten erhebt, verarbeitet oder nutzt.

Beschäftigte im Sinne dieser Vereinbarung sind Funktionsträger des Vereins, die dauerhaft und regelmäßig mit der Verarbeitung von Daten beauftragt sind, sowie Bezirksvorsitzende, Übungsleiter (Referenten, Lehrgangsleiter, Organisatoren von Veranstaltungen, etc.) und Projektmitarbeiter, die vorübergehend mit der Verarbeitung von Daten zu einem bestimmten Zweck betraut sind.

Die hier genannten Regelungen gelten für die Verarbeitung der Daten mit Datenverarbeitungsanlagen und für die physikalische Verarbeitung von Daten in schriftlicher Form.

Der Beschäftigte erfüllt diesen Anspruch mindestens durch folgende Maßnahmen:

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

1.1. Zutrittskontrolle

Der Beschäftigte ergreift Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Unterlagen und Datenverarbeitungsanlagen (Computer, Drucker, Speicher, etc.), mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahme zur Zutrittskontrolle müssen Unterlagen und der Computer in einem für Dritte unzugänglichen, verschlossenen Bereich aufbewahrt werden.

1.2. Zugangskontrolle

Der Beschäftigte ergreift Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer, Speicher, etc.) von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Der Beschäftigte ergreift dazu folgende Maßnahmen: Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort.

Die eingesetzten Datenverarbeitungssysteme müssen zudem über einen aktuellen Anti-Virenschutz verfügen. Der Zugriff in und aus dem Internet muss durch eine geeignete Firewall abgesichert sein. Eingesetzte Speichermedien müssen verschlüsselt und mit einem Passwort abgesichert sein.

Passwörter müssen mindestens 8 Zeichen lang sein, aus einer Kombination von Buchstaben und Sonderzeichen bestehen. Passwörter müssen spätestens alle 8 Wochen geändert werden.

1.3. Zugriffskontrolle

Der Beschäftigte ergreift 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. Die Zugriffskontrolle wird unter anderem gewährleistet durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Er wird diese Zugriffeinschränkungen regelmäßig kontrollieren und auf den aktuellen Stand bringen. Darüber hinaus wird der Beschäftigte organisatorische Maßnahmen treffen, um eine unbefugte Einsichtnahme zu verhindern. Unterlagen, Speichermedien und Datenverarbeitungsanlagen müssen in einem für Dritte unzugänglichen Bereich aufbewahrt werden. Dafür eignen sich abgeschlossene Räumlichkeiten, oder verschlossene Schränke mit ausreichendem Aufbruchschutz.

1.4. Trennungskontrolle

Der Beschäftigte ergreift Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Dazu verwendet der Beschäftigte unterschiedliche Berechtigungen auf seinen Datenverarbeitungssystemen für private und Vereinszwecke. Daten für private und Vereinszwecke werden nicht gleichzeitig auf denselben mobilen Datenträgern gespeichert.

1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten ist möglichst in einer Weise zu anonymisieren, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Bei der Verarbeitung und Weitergabe von Daten sind ausschließlich die zwingend benötigten Daten zu verwenden. Darüberhinausgehende Daten oder Informationen dürfen nicht verwendet werden. Daten sind nach Wegfall des Zweckes Ihrer Erhebung ebenfalls möglichst zu anonymisieren und zu löschen, so dass die jeweilige Speicherung nur noch Ihrem weiter bestehenden Zweck dient.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1. Weitergabekontrolle

Der Beschäftigte ergreift 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. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung. Der Beschäftigte ist verantwortlich für eine datenschutzgerechte Vernichtung von Datenträgern, einfaches Löschen der Daten ist nicht ausreichend. Jegliche Datenübermittlung ist zu dokumentieren (Anlass, Zweck, Empfänger, Datum, Inhalt).

2.2. Eingabekontrolle

Der Beschäftigte ergreift Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1. Verfügbarkeitskontrolle

Der Beschäftigte ergreift Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Dazu legt der Beschäftigte regelmäßig (monatlich) Sicherungen der von ihm verarbeiteten Daten an und bewahrt diese an einem sicheren Ort (unzugänglich für andere, örtlich getrennt von den Datenverarbeitungssystemen) auf.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.1. Datenschutz-Management

Der Beschäftigte führt jährlich eine Überprüfung der Wirksamkeit dieser Technischen Schutzmaßnahmen durch.

4.2. Incident-Response-Management Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Der Beschäftigte meldet Sicherheitsvorfälle, wie Datenverluste, Verlust von Datenträgern, Datenpannen (unberechtigte Empfänger erhalten Zugriff auf Daten ohne angemessenen Zweck), Virenbefall der Datenverarbeitungssysteme, Festgestellte Abweichungen von den oben genannten Regelungen umgehend an die zuständige Stelle (Vorstand, Datenschutzbeauftragter).

4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

Grundsätzlich dürfen nicht mehr personenbezogene Daten erhoben werden, als für den jeweiligen Zweck unbedingt erforderlich sind. Daten sind nur dann zu erheben, wenn sie unmittelbar dem Zweck des Vereins dienen, vereinsrechtlichen, anderen gesetzlichen oder steuerlichen Gründen benötigt werden. Die Weitergabe von Daten darf ausschließlich in Abstimmung mit dem Vorstand erfolgen, ausgenommen es gibt eine gesetzliche Verpflichtung zur Weitergabe. (Datensparsamkeit)

4.4. Auftragskontrolle (Outsourcing an Dritte)

Der Beschäftigte ergreift Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch insbesondere die Durchführung von Wartung und Systembetreuungsarbeiten an seinen Datenverarbeitungssystemen, sowohl vor Ort als auch per Fernwartung.

5. Löschen von Daten

5.1. Löschungspflicht

Wie im Art. 17 Abs. 1 DS-GVO vorgesehen, sind personenbezogene Daten auf Verlangen der betroffenen Person und/oder unter bestimmten Voraussetzungen ohne Verlangen der betroffenen Person eigenständig durch den Beschäftigten unverzüglich zu löschen. Art. 17 Abs. 1 DS-GVO benennt dazu folgende Fälle:

a) Die Notwendigkeit der Verarbeitung zur Zweckerreichung ist entfallen. Insbesondere:
    - wenn der Beschäftigte die Tätigkeit im Verein nicht mehr ausgeübt. Es sind in diesem Fall alle Daten an eine durch den Vorstand zu benennende Person auszuhändigen und anschließend wirksam zu löschen.
    - ein Mitglied aus dem Verein ausscheidet; Es sind alle Daten zu löschen, die nicht aus gesetzlichen Gründen aufbewahrt werden müssen (siehe auch Ausnahmen).
    - eine Veranstaltung oder ein Projekt, wofür Daten erhoben und verarbeitet wurden, abgeschlossen ist und keine gesetzliche Grundlage zur weiteren Aufbewahrung besteht (siehe auch Ausnahmen).

b) Die betroffene Person hat ihre Einwilligung widerrufen und es besteht auch keine sonstige Rechtsgrundlage.
Bekanntwerden eines Widerrufs ist umgehend dem geschäftsführenden Vorstand zu melden!

c) Die betroffene Person legt gem. Art. 21 Abs. 1 oder 2 DS-GVO Widerspruch gegen die Verarbeitung ein;
Bekanntwerden eines Widerrufs ist umgehend dem geschäftsführenden Vorstand zu melden!

d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
Bekanntwerden eines Widerrufs ist umgehend dem geschäftsführenden Vorstand zu melden!

5.2. Ausnahmen von der Löschungspflicht

Die Pflicht zur Löschung nach Art. 17 Abs. 1 und die Pflicht zur Information weiterer Verantwortlicher nach Art. 17 Abs. 2 DS-GVO entfallen, wenn gemäß Art. 17 Abs. 3 DS-GVO die Verarbeitung erforderlich ist

a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
b) zur Erfüllung einer rechtlichen Verpflichtung, zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder zur Ausübung öffentlicher Gewalt;
c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit;
d) für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gem. Art. 89 Abs. 1 DS-GVO, soweit die Löschung die Verwirklichung dieser Ziele ernsthaft beeinträchtigt;
e) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Allerdings berechtigen die benannten Ausnahmen nicht zu einer zeitlich unbegrenzten Verarbeitung der jeweiligen personenbezogenen Daten und zur Speicherung beim Beschäftigten. Diese Daten sind beim Schriftführer, und im Falle von Mitgliederdaten bei der Mitgliederverwaltung zu hinterlegen, der geschäftsführende Vorstand ist zu informieren, der Beschäftigte hat diese Daten anschließend zu löschen.

5.3. Löschverfahren

Der Beschäftigte stellt sicher, dass Daten im Sinne der DS-GVO sicher in einem geeigneten Verfahren gelöscht werden. Dazu werden Datenträger in einem geeigneten Verfahren (Überschreibeverfahren, „7-fach“) zu löschen und anschließend physikalisch zu zerstören. Unterlagen müssen mit einem geeigneten Aktenshredder vernichtet werden.

Die Löschung der Daten und das verwendete Verfahren ist zu dokumentieren.

6. Geltungsbereich

Verstöße gegen diese Vereinbarung können strafrechtlich geahndet werden und werden bei den entsprechenden Stellen gemeldet. Ein Verstoß kann zugleich eine Verletzung von vereinsrechtlichen Pflichten oder spezieller Geheimhaltungspflichten darstellen. Auch (zivilrechtliche) Schadenersatzansprüche können sich aus schuldhaften Verstößen gegen diese Vereinbarung ergeben. Diese Vereinbarung gilt auch nach Beendigung der Tätigkeit weiter.

Sollten einzelne Bestimmungen dieser Vereinbarung teilweise oder vollständig unwirksam, nichtig oder in sonstiger Weise undurchführbar sein oder werden, so berührt dies nicht die Wirksamkeit der Bestimmungen im Übrigen.

_____	_____	_____
Ort, Datum	Unterschrift des Verpflichteten	Unterschrift des Verantwortlichen