**Muster:**

**KI-Governance-Ordnung**

**MUSTER für eine vereinsinterne „Governance-Ordnung – digitale Werkzeuge und KI“**

**§ 1 Zweck und Geltungsbereich**

Diese Geschäftsordnung legt fest, wie der Verein digitale Werkzeuge – insbesondere Systeme mit künstlicher Intelligenz (KI) – auswählt, einsetzt und kontrolliert. Sie gilt für alle Vorstandsmitglieder, Beauftragte, Beschäftigte und sonstige Personen, die im Auftrag des Vereins tätig sind.

Gesetzliche Vorgaben, wie sie insbesondere in der Datenschutz-Grundverordnung (DSGVO), im Bürgerlichen Gesetzbuch (BGB) und im Vereinsrecht stehen, haben immer Vorrang.

**§ 2 Wichtige Begriffe**

**KI-Werkzeug**: Ein System, das Inhalte oder Entscheidungen automatisch erzeugt, unterstützt oder bewertet (z. B. Text-KI, Chatbots, automatische Datenanalysen).

**Personenbezogene Daten**: Alle Informationen, die sich auf eine bestimmte Person beziehen lassen (Name, Adresse, E-Mail, Geburtsdatum, Bankdaten etc.).

**Auftragsverarbeitungsvertrag** (AV-Vertrag): Vertrag mit einem externen Dienstleister, der personenbezogene Daten im Auftrag des Vereins verarbeitet (Art. 28 DSGVO).

**§ 3 Grundprinzipien beim Einsatz von KI**

Beim Einsatz von künstlicher Intelligenz gelten in unserem Verein folgende Grundprinzipien:

1. **Zweckbindung und Datenminimierung**: Wir nutzen KI nur für Vereinsaufgaben und verarbeiten nur so viele Daten wie unbedingt nötig.
2. **Transparenz und Nachvollziehbarkeit**: Ergebnisse müssen prüfbar sein. Wichtige Arbeitsschritte dokumentieren wir.
3. **Menschliche Entscheidung**: Entscheidungen mit erheblicher Wirkung, z. B. Ausschlüsse, Mahnungen oder Personalfragen, werden immer von einer Person final geprüft.
4. **Sicherheit als Standard**: Wir setzen auf sichere Passwörter, Zwei-Faktor-Anmeldung und klare Zugriffsrechte.
5. **Keine besonders sensiblen Daten in offene KI-Dienste**: Gesundheitsdaten, Religion, politische Meinungen usw. laden wir nicht in frei zugängliche KI-Systeme hoch.

**§ 4 Zuständigkeiten**

Damit der Einsatz von digitalen Werkzeugen und KI reibungslos funktioniert, hat jede Rolle klare Aufgaben:

**Vorstand gesamt**: legt die Strategie fest, genehmigt den Einsatz neuer Tools und überprüft jährlich deren Nutzen und Sicherheit.

**Vorsitzender**: Gesamtverantwortung, entscheidet bei Problemen oder Sicherheitsvorfällen.

**Schatzmeister**: prüft Kosten, Lizenzen und Freigaben z. B. für automatisierte Mahnverfahren.

**IT-Beauftragte/r oder externer Fachmann**: prüft neue Tools technisch, richtet sie sicher ein, verwaltet Benutzerrechte.

**Datenschutzbeauftragte/r oder -koordinator/in**: stellt sicher, dass alle gesetzlichen Datenschutzregeln eingehalten werden, prüft AV-Verträge, führt Verzeichnisse und Löschkonzepte.

**Fachverantwortliche** (z. B. Leiter/in Mitgliederverwaltung): prüfen die inhaltliche Qualität der Ergebnisse und achten darauf, dass die KI-Ausgaben korrekt sind.

**§ 5 Datenarten – Ampelprinzip**

Damit wir immer wissen, welche Daten wie geschützt werden müssen, teilen wir sie in drei Kategorien ein:

1. **Rot (streng geschützt – nie in offene KI-Dienste hochladen)**: z. B. Gesundheitsdaten, Religion, Daten von Minderjährigen, Bank- oder Spendenkontodaten, Strafdaten. Diese dürfen nur in speziell gesicherten, vertraglich abgesicherten Systemen verarbeitet werden.
2. **Gelb (geschützt – nur unter Auflagen)**: z. B. Namen, Adressen, Mitgliedsnummern, Teilnahme- oder Beitragsdaten. Nur in sicheren Systemen mit AV-Vertrag und Speicherort in der EU/EWR.
3. **Grün (unproblematisch)**: z. B. anonymisierte Listen, öffentlich zugängliche Vereinsinformationen. Frei nutzbar.

**§ 6 Einführung neuer Tools**

Bevor ein digitales Werkzeug oder eine KI genutzt wird, wird folgender Prozess durchlaufen:

1. **Antrag stellen**: Die Person, die das Tool nutzen möchte, beschreibt den Zweck, die Art der Daten (Ampelfarbe), den Anbieter, den Speicherort und die Kosten.
2. **Prüfung**: IT-Beauftragter und Datenschutzbeauftragter prüfen Technik und Datenschutz, der Schatzmeister die Kosten.
3. **Testphase**: Wir testen mit anonymisierten oder fiktiven Daten.
4. **Vorstandsbeschluss**: Der Vorstand entscheidet, ob das Tool offiziell eingeführt wird (Freigabe meist für 12 Monate, dann erneute Prüfung).
5. **Dokumentation**: Das Tool wird in einer internen Liste („Toolkataster“) erfasst.

**§ 7 Regeln für den Umgang mit KI**

Beim Umgang mit künstlicher Intelligenz in der alltäglichen Arbeit gelten folgende Regeln:

**Keine sensiblen Daten hochladen:** Streng geschützte (rot) und geschützte Daten (gelb) werden nur mit Genehmigung und Sicherheitsmaßnahmen verwendet.

**Vier-Augen-Prinzip**: Bei wichtigen Inhalten wie Rechtstexten, Finanzen oder offiziellen Schreiben prüft eine zweite Person das KI-Ergebnis.

**Kennzeichnung**: Automatisch erstellte Texte werden intern mit „KI-assistiert“ gekennzeichnet.

**Kein Alleingang der KI**: Entscheidungen mit Folgen für Mitglieder trifft immer ein Mensch, die KI darf nur vorbereiten.

**§ 8 Automatisierte Abläufe (z. B. Mahnungen)**

Automatisierungen dürfen eingesetzt werden, wenn:

* eine Rechtsgrundlage besteht (z. B. Mitgliedsvertrag, Satzung),
* die Textbausteine vorher geprüft wurden,
* bei Härtefällen eine manuelle Endkontrolle erfolgt,
* der Versand über die zulässigen Kanäle erfolgt (z. B. E-Mail oder Brief laut Satzung),
* alle Vorgänge protokolliert werden (Datum, Empfänger, verantwortliche Person).

**§ 9 Sicherheit und Zugriffsrechte**

(1) Zugriffsrechte werden nur so weit wie nötig („Need-to-know-Prinzip“) eingeräumt und jährlich überprüft.

(2) Eine Zwei-Faktor-Anmeldung, die Verwendung sicherer Passwörter und die Nutzung eines Passwort-Managers sind Pflicht.

(3) Geräte müssen verschlüsselt und gesperrt sein, Protokolle werden zwölf Monate aufbewahrt.

(4) Beim Austritt aus dem Verein oder Ausscheiden aus einer Funktion werden Zugriffsrechte sofort entzogen.

**§ 10 Verträge mit Anbietern und Datenübermittlung ins Ausland**

(1) Vor der Nutzung eines externen Anbieters muss ein Auftragsverarbeitungsvertrag (Art. 28 DSGVO) abgeschlossen werden.

(2) Datenübermittlungen in Länder außerhalb der EU/EWR sind nur mit besonderen Schutzmaßnahmen erlaubt (z. B. Standardvertragsklauseln) und müssen vom Vorstand genehmigt werden.

**§ 11 Aufbewahrung und Löschung**

(1) Für jede Datenart gibt es feste Löschfristen, orientiert an gesetzlichen Vorgaben (z. B. Mitglieder-, Kassen- oder Veranstaltungsdaten).

(2) Wenn möglich, wird verhindert, dass KI-Anbieter Vereinsdaten zum Training ihrer Systeme verwenden.

(3) Regelmäßige Backups und Exportmöglichkeiten werden geprüft.

**§ 12 Umgang mit Vorfällen**

(1) Sicherheitsvorfälle oder Datenpannen müssen sofort an den Vorsitz und die Datenschutzbeauftragte gemeldet werden.

(2) Innerhalb von 72 Stunden erfolgt eine Bewertung, ggf. eine Meldung an die Aufsichtsbehörde und betroffene Personen.

(3) Der Vorfall wird dokumentiert.

**§ 13 Transparenz und Information**

Im Beitrittsformular und in der Datenschutzerklärung wird kurz erläutert, wie der Verein KI nutzt. Der Vorstand berichtet darüber hinaus einmal im Jahr der Mitgliederversammlung über eingesetzte Tools, deren Zweck, wichtige Änderungen und eventuelle Vorfälle (ohne persönliche Daten).

**§ 14 Schulung**

Neue Verantwortliche erhalten eine Einweisung. Alle Nutzer von KI-Tools nehmen einmal im Jahr an einer kurzen Auffrischungsschulung (30–45 Minuten) teil.

**§ 15 Inkrafttreten und Überprüfung**

Diese Geschäftsordnung tritt am … in Kraft.

Der Vorstand prüft sie mindestens einmal jährlich oder wenn sich Gesetze oder die genutzten Tools ändern.

**Impressum**

Verlag PROmedia ein Verlagsbereich der Verlag für die Deutsche Wirtschaft AG,

Theodor-Heuss-Straße 2-4 D-53177 Bonn

Großkundenpostleitzahl: D-53095 Bonn

Tel.: (0228) 95 50 130

Fax: (0228) 36 96 480

Internet: www.vnr.de

E-Mail: kundendienst@vnr.de

Vorstand: Richard Rentrop

Redaktionell Verantwortliche: Kathrin Righi,

VNR Verlag für die Deutsche Wirtschaft AG,

Adresse siehe oben

Alle Angaben wurden mit Sorgfalt ermittelt und überprüft.

Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Eine Gewähr kann deshalb nicht übernommen werden.

Copyright 2025: Vervielfältigungen jeder Art sind nur mit ausdrücklicher Genehmigung des Verlags gestattet.

Die Aufnahme in Online-Dienste und Internet sowie die Vervielfältigung auf Datenträger dürfen nur nach vorheriger schriftlicher Zustimmung des Verlags erfolgen.