Auftragsverarbeitervereinbarung

vom

dd.mm.yyyy

zwischen

Max Mustermann
(im Folgenden „Verantwortlicher“)

und

Max Mustermann-Auftragnehmer GmbH
(im Folgenden „Auftragsverarbeiter“)

Der Auftragsverarbeiter hat sich verpflichtet, die in Anlage 1 beschriebenen Datenverarbeitungen gegenüber dem Verantwortlichen zu erbringen. Für die Zwecke dieser Vereinbarung gelten die Begriffsdefinitionen der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679).

1. **Weisungsrecht.**
Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen — auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation — sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

2. **Vertraulichkeit.**
Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

3. **Datensicherheit.**
Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er ausreichende Sicherheitsmaßnahmen ergriffen hat, um zu verhindern, dass Daten ordnungswidrig verwendet oder Dritten unbefugt zugänglich werden. Außerdem erklärt der Auftragsverarbeiter, dass er alle gemäß Artikel 32 Datenschutz-Grundverordnung erforderlichen Maßnahmen ergreift. Diese Maßnahmen schließen im Besonderen die in Anlage 2 beschriebenen Maßnahmen ein.

4. **Meldung einer Verletzung des Schutzes personenbezogener Daten.**
Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über eine Verletzung des Schutzes personenbezogener Daten, die der Auftragsverarbeiter im Auftrag des Verantwortlichen verarbeitet. Diese Meldung soll zumindest beschreiben:

   a. die Art der Verletzung des Schutzes personenbezogener Daten, einschließlich der Kategorien und der Zahl der betroffenen Personen und der Zahl der betroffenen Datensätze;

   b. die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

   c. die vom Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten sowie gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen Auswirkungen.

Im Falle einer Verletzung des Schutzes personenbezogener Daten unterstützt der Auftragsverarbeiter den Verantwortlichen dabei, Maßnahmen zur Wiederherstellung der Datensicherheit zu treffen sowie die Verletzung zu beenden.

5. **Sub-Auftragsverarbeitung.**
Die Hinzuziehung neuer oder die Ersetzung bestehender Sub-Auftragsverarbeiter bedarf/bedürfen der vorhergehenden ausdrücklichen schriftlichen Zustimmung des Verantwortlichen. Nimmt der Auftragsverarbeiter einen anderen Sub-Auftragsverarbeiter in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem Sub-Auftragsverarbeiter im Wege eines schriftlichen Vertrags dieselben Datenschutzpflichten auferlegt, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen des anwendbaren Datenschutzrechts erfolgt. Außerdem überprüft der Auftragsverarbeiter regelmäßig die Einhaltung der Datenschutzpflichten durch den Sub-Auftragsverarbeiter und teilt dem Verantwortlichen jede etwaige Verletzung dieser Pflichten unverzüglich mit. Der Auftragsverarbeiter hat in einem solchen Fall die Sub-Auftragsverarbeitung zu beenden, wenn dies vom Verantwortlichen verlangt wird. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

6. **Unterstützung.**
Der Auftragsverarbeiter unterstützt den Verantwortlichen durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung der Pflichten des Verantwortlichen bei Anträgen auf Wahrnehmung der Betroffenenrechte gemäß Kapitel III (Information, Auskunft, Berichtigung, Löschung ….) der Datenschutz-Grundverordnung. Der Auftragsverarbeiter stellt seine Unterstützung innerhalb von zehn Arbeitstagen ab Anfrage des Verantwortlichen beim Auftragsverarbeiter bezüglich eines Antrages einer betroffenen Person auf Wahrnehmung ihrer Betroffenenrechte zur Verfügung. Darüber hinaus unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung seiner Pflichten gemäß dem anwendbaren Datenschutzrecht, einschließlich Artikel 32 bis 36 Datenschutz-Grundverordnung (Verarbeitungsicherheit, Meldung von Datenschutz-verletzungen, …).

7. **Rückgabe / Löschung von personenbezogenen Daten.**
Der Auftragsverabeiter ist nach Abschluss der Erbringung der Verarbeitungsleistungen verpflichtet, den letztgültigen Datenstand in elektronischem, strukturierten, üblicherweise gebrauchten und widerverwendbaren Format an den Verantwortichen zu übermitteln – dies nur dann, falls der Verantwortliche über den letztgültigen Datenstand nicht verfügt. Der Auftragsverarbeiter löscht in einem weiteren Schritt nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

8. **Überprüfung.**
Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten unentgeltlich zur Verfügung und ermöglicht Überprüfungen, einschließlich Inspektionen, die von dem Verantwortlichen oder einem anderen von diesem beauftragen Prüfer durchgeführt werden.

Im Namen des Verantwortlichen	Im Namen des Auftragsverarbeiters
Ort, Datum, Unterschrift	Ort, Datum, Unterschrift

Anlage 1 (Kurzbeschreibung der Datenverarbeitung)

Allgemeine Beschreibung der beauftragten Datenverarbeitung, Verarbeitungszweck, Verarbeitungsmaßnahmen
Versand der Vereinszeitung, Aufdruck der Mitgliederadressen
Von der Verarbeitung betroffener Personenkreis:
Vereinsmitlieder
Kategorien von Daten Die übermittelten personenbezogenen Daten gehören zu folgenden Datenkategorien (bitte genau angeben):
Name + Postadresse

Anlage 2 – Technisch-organisatorische Maßnahmen

(1.1.a) **Vertraulichkeit**

☒ **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B.: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen;

☒ **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung, z.B.: Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

☒ **Zugriffskontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Standard-Berechtigungsprofile auf „need to know-Basis“, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten;

☒ **Pseudonymisierung**: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.

☒ **Klassifikationsschema für Daten:** Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

(1.1.b) **Integrität**

☒ **Weitergabekontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

☒ **Eingabekontrolle**: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement

(1.1.c) **Verfügbarkeit und Belastbarkeit**

☒ **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern;

☒ Rasche **Wiederherstellbarkeit**;

☒ **Löschungsfristen**: Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.

(1.1.d) **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**

☒ Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen

☒ Incident-Response-Management;

☒ Datenschutzfreundliche Voreinstellungen;

☒ **Auftragskontrolle:** Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters, Vorabüberzeugungspflicht, Nachkontrollen.