

Vertrag über Rechenzentrumsleistungen

zwischen

[Name, Anschrift, Steuernummer],

im Folgenden: **Betreiber**

und

dem Musterverein e.V., vertreten durch den Vorstand, Musterstr. 12, 00000
Musterhausen, Vereinsregister Musterstadt, VR 0000, USt-IdNr. 00000000000,

im Folgenden: **Verein.**

Der Betreiber betreibt Server in einem Rechenzentrum und erbringt hierauf bezogene Leistungen. Der Verein beabsichtigt, diese Leistungen für den Betrieb der Mitgliederverwaltungssoftware MIA zu beziehen. Dieser Vertrag regelt Bereitstellung, Betrieb und Qualität der Leistungen, Verantwortlichkeiten, Sicherheitsanforderungen, Vergütung und Haftung sowie den Datenschutz.

§ 1 Vertragsgegenstand, Vertragsbestandteile, Leistungsänderungen

1. Vertragsgegenstand ist die entgeltliche Erbringung von Rechenzentrumsleistungen gemäß Anlage 1 durch den Betreiber für den Betrieb der Mitgliederverwaltungssoftware MIA.
2. Bestandteile dieses Vertrages sind
 - dieser Vertragstext,
 - Anlage 1: Leistungsbeschreibung,
 - Anlage 2: Service-Level-Vereinbarung,
 - Anlage 3: Sicherheitskonzept,
 - Anlage 4: Auftragsverarbeitungsvereinbarung (AVV).
3. Wünscht der Verein Änderungen am Leistungsumfang, an Schnittstellen, Parametern, Service-Level-Vereinbarung oder Sicherheitsanforderungen, teilt er dem Betreiber diese mit. Der Betreiber prüft die Änderungswünsche und teilt dem Verein innerhalb von **[14]** Tagen Auswirkungen auf Preis, Zeitplan, Verfügbarkeit, Sicherheit und Risiken mit. Änderungen werden erst mit der Bestätigung durch beide Parteien wirksam; die Bestätigung bedarf der Textform.

§ 2 Bereitstellung, Mitwirkung des Kunden

1. Der Betreiber stellt die Leistungen innerhalb der in Anlage 1 festgelegten Bereitstellungsfristen bereit.
2. Der Verein stellt alle zur Leistungserbringung erforderlichen Informationen, Zugänge, Ansprechpartner, IP-Adressierungen, Konfigurationsvorgaben und Freigaben rechtzeitig bereit. Der Verein ist für die Kompatibilität seiner Systeme, Software und Konfigurationen verantwortlich, soweit nicht ausdrücklich Managed Services vereinbart sind.
3. Verzögerungen aufgrund unterlassener oder verspäteter Mitwirkungen des Vereins gehen zu Lasten des Vereins; vereinbarte Termine verlängern sich angemessen.

§ 3 Service Levels, Support, Störungsmanagement

1. Die Zielverfügbarkeit und die Messmethode ergeben sich aus Anlage 2.
2. Nicht als Ausfallzeiten gelten insbesondere:
 - Wartungsfenster gemäß Anlage 2;
 - Ausfälle durch Störungen, die aus der Sphäre des Vereins stammen;
 - Ausfälle durch höhere Gewalt gemäß § 13.
3. Für Supportanfragen, Störungs- und Fehlermeldungen steht dem Verein die Plattform <https://mieterbund.zendesk.com> zur Verfügung.
4. Der Verein ist verpflichtet, Störungen und Fehler unverzüglich in nachvollziehbarer Form unter Angabe der für die Erkennung der Störung oder des Fehlers zweckdienlichen Informationen zu melden (Fehlerbeschreibung, betroffene Systeme, Dringlichkeit, Logs, Ansprechpartner) und den Betreiber bei der Analyse angemessen zu unterstützen.
5. Servicezeiten, Priorisierung (P1–P4), Reaktionszeiten ergeben sich aus Anlage 2.

§ 4 Sicherheitsanforderungen, physische Sicherheit, Betrieb

1. Der Betreiber betreibt die IaaS-Plattform nach dem in Anlage 3 beschriebenen Sicherheitskonzept. Der Betreiber greift auf Vorprodukte von anderen Dienstleistern zurück; diese sind in Anlage 3 aufgeführt.
2. Der Betreiber setzt angemessene organisatorische und technische Maßnahmen zur Sicherung gegen unbefugten Zutritt, Zugriff, Veränderung und Verlust ein.

3. Soweit Managed Services vereinbart sind, gelten die Patchzyklen, Freigabeprozesse und Verantwortlichkeiten gemäß Anlage 1 und 2.
4. Der Betreiber protokolliert betriebs- und sicherheitsrelevante Ereignisse im erforderlichen Umfang. Zugriffsrechte werden rollenbasiert nach dem Prinzip der geringsten Privilegien vergeben; privilegierte Zugriffe werden protokolliert und – soweit möglich – zeitlich befristet.

§ 5 Datenschutz und Auftragsverarbeitung

1. Bei der Erbringung der Leistungen verarbeitet der Betreiber personenbezogene Daten im Auftrag des Vereins und handelt insoweit als Auftragsverarbeiter im Sinne des Art. 28 DS-GVO. Hierfür schließen die Parteien vor Beginn der Verarbeitung die Auftragsverarbeitungsvereinbarung (AVV) gemäß Anlage 4.
2. Der Einsatz von Unterauftragsverarbeitern richtet sich nach Anlage 4. Der Betreiber stellt sicher, dass Unterauftragsverarbeiter mindestens gleichwertige Datenschutzpflichten übernehmen.
3. Speicher- und Verarbeitungsorte ergeben sich aus Anlage 1. Drittlandtransfers erfolgen nur unter den Voraussetzungen der DS-GVO.

§ 6 Rechte an Daten, Systemen, Software

1. Alle Rechte an den Daten des Vereins verbleiben beim Verein.
2. Der Betreiber verarbeitet Daten des Vereins ausschließlich zur Vertragserfüllung und nur im vereinbarten Umfang.
3. Soweit der Betreiber Konfigurationen, Skripte oder Dokumentationen speziell für den Verein erstellt („Arbeitsergebnisse“), erhält der Verein ein nicht ausschließliches und nicht übertragbares, zeitlich auf die Vertragslaufzeit beschränktes Nutzungsrecht, soweit dies zur Nutzung der Leistungen erforderlich ist.
4. Rechte an standardisierten Tools, Templates, Betriebsprozessen und Know-how des Betreibers verbleiben beim Betreiber.

§ 7 Vergütung, Abrechnung, Preisanpassung

1. Der Verein zahlt für den Rechenzentrumsbetrieb, beginnend mit der Bereitstellung von MIA im Rechenzentrum, ein monatliches Bereitstellungsentgelt in Höhe von 145 Euro inkl. einer Speicherplatzkapazität von 50 GB. Die monatlichen Preise für zusätzliche Speicherkapazitäten ergeben sich aus der online unter <https://mia->

doku.des-mia.de/docs/preiserechenzentrum/ zur Verfügung gestellten Preisliste, die als Vertragsbestandteil vereinbart wird. Die Preise sonstiger Leistungen richten sich ebenfalls nach der vorgenannten Preisliste.

2. Das Bereitstellungsentgelt und sämtliche übrigen Preise sind Nettopreise. Hinzu kommt die jeweils geltende gesetzliche Mehrwertsteuer, z.Zt.19%.
3. Der Betreiber rechnet monatlich ab. Das Bereitstellungsentgelt und die Kosten für zusätzliche Speicherkapazitäten sind monatlich im Voraus zum 01. des Monats fällig. Zahlungen erfolgen per SEPA-Firmen-Lastschrift (B2B), in begründeten Ausnahmefällen per SEPA-Basislastschrift (CORE).
4. Der Betreiber kann die Preise anpassen, wenn und soweit sich seine Kosten nachweislich verändern und die Anpassung zur Abbildung der Kostenentwicklung erforderlich ist. Kostenminderungen sind in gleicher Weise zu berücksichtigen. Die Anpassung ist auf den Umfang der tatsächlichen Kostenänderung begrenzt.
5. Der Betreiber kündigt Preisanpassungen mindestens **[6]** Wochen vorher in Textform an und erläutert die Grundlagen der Anpassung in nachvollziehbarer Form. Erhöht sich der Preis um mehr als 30 % innerhalb von **[12]** Monaten, steht dem Verein ein Sonderkündigungsrecht zum Datum der Wirksamkeit der Anpassung zu.

§ 8 Gewährleistung, Störungs- und Fehlermeldungen

1. Der Betreiber gewährleistet die vertragsgemäße Erbringung der Leistungen nach Maßgabe der gesetzlichen Bestimmungen.
2. Der Verein hat dem Betreiber Störungen und Fehler unverzüglich in nachvollziehbarer Form unter Angabe der für die Erkennung der Störung oder des Fehlers zweckdienlichen Informationen zu melden (Fehlerbeschreibung, betroffene Systeme, Dringlichkeit, Logs, Ansprechpartner) und den Betreiber bei der Analyse angemessen zu unterstützen.
3. Für die Meldung steht dem Verein die Plattform <https://mieterbund.zendesk.com> zur Verfügung.

§ 9 Haftung auf Schadensersatz

1. Der Betreiber haftet unbeschränkt für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit sowie für Schäden, die auf Vorsatz oder grober Fahrlässigkeit beruhen.

2. Bei einfacher Fahrlässigkeit haftet der Betreiber nur bei der Verletzung wesentlicher Vertragspflichten (Kardinalpflichten). In diesem Fall ist die Haftung auf den vertragstypischen, vorhersehbaren Schaden begrenzt.
3. Die Haftung nach Absatz 2 ist je Schadensfall auf 1.000.000 EUR und für alle Schadensfälle eines Versicherungsjahres auf 2.000.000 EUR begrenzt. Der Betreiber unterhält hierfür eine entsprechende Betriebshaftpflichtversicherung.
4. Eine weitergehende Haftung für entgangenen Gewinn, mittelbare Schäden, Folgeschäden oder reine Vermögensschäden ist bei einfacher Fahrlässigkeit ausgeschlossen, soweit gesetzlich zulässig.
5. Die Haftung nach dem Produkthaftungsgesetz sowie sonstige zwingende gesetzliche Haftungsvorschriften bleiben unberührt.

§ 10 Vertragslaufzeit, Kündigung

1. Der Vertrag beginnt am **[Datum]** und wird auf unbestimmte Zeit geschlossen.
2. Der Vertrag kann von beiden Parteien mit einer Frist von sechs Monaten gekündigt werden, erstmals zum Ablauf von 12 Monaten nach Vertragsabschluss. Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.
3. Die Kündigung bedarf der Textform, sofern nicht gesetzlich zwingend eine strengere Form vorgeschrieben ist.
4. Erklärungen in Textform gelten erst mit ihrem Zugang bei der anderen Vertragspartei als zugegangen. Der Absender trägt die Beweislast für den Zugang. Kann der Zugang einer per E-Mail übermittelten Erklärung nicht nachgewiesen werden, gilt sie als nicht zugegangen.
5. Sofern der Verein mehrere Leistungen bezieht, können Leistungen separat gekündigt werden, sofern diese technisch und wirtschaftlich trennbar sind. Kündigt der Verein eine Leistung, bleiben Entgelte für verbleibende Leistungen unberührt; einmalige Setup-Kosten werden nicht erstattet, sofern nichts Abweichendes vereinbart ist.

§ 11 Vertraulichkeit

1. Die Vertragsparteien verpflichten sich, alle ihnen im Rahmen des Vertrages zugänglich gemachten sowie bei Gelegenheit der Zusammenarbeit erlangten Informationen über Angelegenheiten der anderen Partei, die als vertraulich gekennzeichnet sind, bei einer mündlichen Übermittlung als vertraulich bezeichnet

werden oder aus Sicht eines objektiven Beobachters als vertraulich erkennbar sind sowie Geschäfts- und Betriebsgeheimnisse vertraulich zu behandeln.

2. Die Vertraulichkeitsverpflichtung gilt über die Beendigung dieses Vertrages hinaus.
3. Vertrauliche Informationen dürfen ohne schriftliche Einwilligung der anderen Vertragspartei zu einem anderen als dem zur vertragsgemäßen Aufgabenerfüllung vorgesehenen Zweck nicht verwertet, Dritten zugänglich gemacht oder sonst genutzt werden.

§ 12 Audit- und Informationsrechte

1. Der Verein kann nach angemessener Vorankündigung und höchstens **[1]** Mal pro Jahr auf eigene Kosten Audits durchführen oder durchführen lassen, soweit dies erforderlich ist, um die Einhaltung vertraglicher Sicherheits- und Datenschutzpflichten zu prüfen.
2. Audits erfolgen während üblicher Geschäftszeiten, unter Wahrung der Sicherheitsanforderungen des Rechenzentrums und ohne Störung des Betriebs.
3. Der Betreiber kann statt Vor-Ort-Audits geeignete Nachweise vorlegen (z. B. Zertifikate, Auditberichte, Penetrationstest-Zusammenfassungen), sofern diese gleichwertig sind.

§ 13 Höhere Gewalt

1. Keine Partei haftet für Leistungsstörungen, die durch Ereignisse außerhalb ihres Einflussbereichs verursacht werden (z. B. Naturkatastrophen, Krieg, Streik, staatliche Maßnahmen, flächendeckende Energie-/Netzausfälle), sofern die Partei das Ereignis nicht zu vertreten hat.
2. Die betroffene Partei informiert die andere Partei unverzüglich und unternimmt zumutbare Maßnahmen zur Schadensminderung.

§ 14 Compliance, Exportkontrolle

1. Die Parteien verpflichten sich zur Einhaltung der anwendbaren Gesetze, insbesondere IT-Sicherheits-, Datenschutz- und Exportkontrollvorschriften.
2. Der Verein ist für die Rechtmäßigkeit der von ihm betriebenen Inhalte und Anwendungen verantwortlich.

§ 15 Abtretung

Der Verein darf Rechte und Pflichten aus diesem Vertrag nur mit vorheriger Zustimmung des Betreibers abtreten, wobei der Betreiber die Zustimmung nicht unbillig verweigern darf.

§ 16 Schlussbestimmungen

1. Änderungen und Ergänzungen dieses Vertrages bedürfen der Textform, soweit nicht gesetzlich eine strengere Form vorgesehen ist. Dies gilt auch für die Änderung dieser Textformklausel.
2. Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Ort, Datum

Ort, Datum

Unterschrift Betreiber

Unterschrift Verein

Anlage 1: Leistungsbeschreibung

1. Bereitgestellte Infrastruktur

Der Betreiber stellt dem Verein die für den Betrieb der Mitgliederverwaltungssoftware MIA erforderliche virtuelle Serverinfrastruktur einschließlich Betriebssystem bereit.

Die Bereitstellung erfolgt auf einer durch den Betreiber administrierten Virtualisierungsplattform in einem durch einen beauftragten Dienstleister betriebenen Rechenzentrum.

Ein Anspruch auf Bereitstellung bestimmter physischer Hardware oder auf Zuordnung zu einem bestimmten physischen Server besteht nicht.

2. Speicher

Im monatlichen Bereitstellungsentgelt sind 50 GB Speicherplatz enthalten.

Zusätzlicher Speicherplatz wird gemäß der jeweils geltenden Preisliste berechnet.

3. Netzwerk

Der Betreiber stellt die für den Betrieb von MIA erforderliche Netzwerkanbindung und Internetkonnektivität bereit.

4. Betriebssystem und Systembetrieb

Der Betreiber übernimmt Installation, Konfiguration, Wartung und Sicherheitsaktualisierung des Betriebssystems sowie der von ihm verantworteten Infrastrukturkomponenten.

5. Datensicherung

Die Aufbewahrungsrotation umfasst 7 tägliche, 4 wöchentliche, 6 monatliche und 1 jährliche Sicherungsstände sowie den jeweils letzten Sicherungsstand. Änderungen der Aufbewahrungsrotation sind zulässig, sofern hierdurch das vereinbarte Schutzniveau nicht wesentlich vermindert wird.

Ältere Sicherungsstände werden im Rahmen der festgelegten Rotation automatisch aus der Sicherung entfernt.

Die Wiederherstellung eines verfügbaren Sicherungsstandes kann vom Verein über das Supportsystem angefordert werden.

6. Verantwortungsgrenze

Die Verantwortlichkeit des Betreibers umfasst die bereitgestellte virtuelle Infrastruktur einschließlich Betriebssystem bis zum vereinbarten Übergabepunkt. Die Anwendung

MIA einschließlich Installation, Betrieb, Administration, Konfiguration, Aktualisierung und fachlicher Nutzung liegt nicht im Verantwortungsbereich des Betreibers.

Anlage 2: Service-Level-Vereinbarung

1. Geltungsbereich und Verfügbarkeit

Diese Service-Level-Vereinbarung bezieht sich ausschließlich auf die vom Betreiber gemäß Anlage 1 bereitgestellte und verantwortete virtuelle Server- und Systeminfrastruktur.

Die Zielverfügbarkeit dieser Infrastruktur beträgt **99,5 % pro Kalenderjahr**.

Die Anwendung MIA sowie deren Betrieb, Funktionsfähigkeit und Verfügbarkeit sind nicht Gegenstand dieser Service-Level-Vereinbarung und liegen nicht im Verantwortungsbereich des Betreibers.

Nicht als Ausfallzeiten im Rahmen der Verfügbarkeitsberechnung gelten insbesondere:

- angekündigte Wartungsfenster und erforderliche Wartungsmaßnahmen;
- Störungen und Ausfälle der Anwendung MIA oder sonstiger Systeme und Anwendungen außerhalb des Verantwortungsbereichs des Betreibers;
- Störungen, die aus der Sphäre des Vereins, seiner Nutzer oder von ihm eingesetzter Systeme stammen;
- Störungen und Ausfälle von Telekommunikations-, Netzwerk-, Rechenzentrums-, Hosting- oder sonstigen Vorleistungsdienstleistern, soweit die Ursache außerhalb des Einfluss- und Verantwortungsbereichs des Betreibers liegt;
- Störungen aufgrund höherer Gewalt gemäß § 13 des Hauptvertrags;
- Störungen aufgrund von Angriffen Dritter oder sonstigen externen Ereignissen, soweit der Betreiber diese nicht zu vertreten hat.

Die Infrastruktur gilt als verfügbar, wenn die vom Betreiber bereitgestellte virtuelle Server- und Systeminfrastruktur einschließlich des Betriebssystems sowie die vom Betreiber betriebene zentrale Netzwerk- und VPN-Infrastruktur grundsätzlich betriebsbereit sind. Nicht maßgeblich für die Feststellung der Verfügbarkeit sind Störungen oder Ausfälle von Internet- und Telekommunikationsverbindungen des Vereins sowie von an den Standorten des Vereins eingesetzten Netzwerk-, VPN- oder Security-Geräten, insbesondere Sophos RED Devices, und sonstigen Endgeräten. Die Funktionsfähigkeit der auf der Infrastruktur betriebenen Anwendung MIA ist für die Feststellung der Verfügbarkeit ebenfalls nicht maßgeblich.

2. Wartungsmaßnahmen

Planbare Wartungsmaßnahmen, bei denen mit einer Beeinträchtigung der Verfügbarkeit zu rechnen ist, werden nach Möglichkeit mindestens 48 Stunden vor Beginn angekündigt.

Wartungsmaßnahmen zur Behebung kritischer Störungen, zur Abwehr konkreter Sicherheitsrisiken oder zur kurzfristig erforderlichen Installation sicherheitsrelevanter Aktualisierungen können ohne Einhaltung der vorgenannten Ankündigungsfrist durchgeführt werden.

Der Betreiber bemüht sich, planbare Wartungsmaßnahmen so durchzuführen, dass die Nutzung der bereitgestellten Infrastruktur möglichst wenig beeinträchtigt wird.

3. Störungsmeldungen

Störungen sind über das im Hauptvertrag bezeichnete Supportsystem zu melden.

Die Störungsmeldung soll alle für die Bearbeitung erforderlichen Informationen enthalten, insbesondere eine Beschreibung der Störung, die betroffenen Systeme, den Zeitpunkt der Feststellung und, soweit vorhanden, relevante Fehlermeldungen oder Protokollinformationen.

Die Priorisierung einer Störung richtet sich nach den tatsächlichen Auswirkungen auf die vom Betreiber verantwortete Infrastruktur. Störungen der Anwendung MIA werden bei der Priorisierung nur berücksichtigt, soweit ihre Ursache in der vom Betreiber verantworteten Infrastruktur liegt.

4. Prioritäten und Reaktionszeiten

Priorität	Beschreibung	Reaktionszeit
P1 Kritisch	Vollständiger Ausfall der vom Betreiber verantworteten virtuellen Server- oder Systeminfrastruktur oder vergleichbare schwerwiegende Störung	4 Stunden
P2 Hoch	Erhebliche Beeinträchtigung der vom Betreiber verantworteten Infrastruktur, wobei ein eingeschränkter Betrieb weiterhin möglich ist	Innerhalb von 24 Stunden
P3 Normal	Sonstige Störung der Infrastruktur ohne erhebliche Beeinträchtigung des laufenden Betriebs	Innerhalb von 2 Arbeitstagen
P4 Niedrig	Geringfügige Beeinträchtigungen ohne relevante Auswirkung auf die Arbeitsfähigkeit.	Innerhalb von 4 Arbeitstagen

Reaktionszeit bezeichnet den Zeitraum zwischen Eingang einer gemäß Ziffer 3 ausreichend qualifizierten Störungsmeldung und dem Beginn der Störungsanalyse durch den Betreiber. Sie stellt keine Wiederherstellungs-, Behebungs- oder Lösungszeit dar.

Die angegebenen Reaktionszeiten gelten innerhalb der vereinbarten Servicezeiten. Außerhalb der Servicezeiten beginnt die Reaktionszeit mit Beginn der nächsten

Servicezeit, soweit für die betreffende Priorität keine abweichende Vereinbarung getroffen wurde.

Allgemeine technische Anfragen, Beratungsanfragen sowie Änderungs- und Erweiterungswünsche stellen keine Störungen im Sinne dieser Service-Level-Vereinbarung dar und unterliegen nicht den vorstehenden Reaktionszeiten.

5. Wiederherstellung und Entstörung

Der Betreiber wird Störungen in seinem Verantwortungsbereich nach Maßgabe ihrer Priorität und im Rahmen der technischen und betrieblichen Möglichkeiten bearbeiten.

Bestimmte Wiederherstellungs-, Behebungs- oder Lösungszeiten werden nicht zugesichert. Die Dauer der Entstörung kann insbesondere von der Art und Ursache der Störung sowie von erforderlichen Leistungen eingesetzter Infrastruktur- oder Vorleistungsdienstleister abhängig sein.

6. Servicezeiten

Die regulären Servicezeiten sind Montag bis Freitag von 08:00 Uhr bis 17:00 Uhr, ausgenommen gesetzliche Feiertage am Sitz des Betreibers.

Die in Ziffer 4 genannten Reaktionszeiten gelten ausschließlich innerhalb der regulären Servicezeiten. Außerhalb der Servicezeiten eingehende Störungsmeldungen gelten für die Berechnung der Reaktionszeit mit Beginn der nächsten regulären Servicezeit als eingegangen.

Außerhalb der regulären Servicezeiten besteht kein Anspruch auf Bearbeitung von Störungen, soweit nicht ausdrücklich etwas Abweichendes vereinbart wurde.

Für außerhalb der regulären Servicezeiten erbrachte Leistungen können abweichende Vereinbarungen und Vergütungen gelten.

Anlage 3: Sicherheitskonzept

1. Grundsätze

Der Betreiber setzt für die von ihm verantwortete Server-, System- und Netzwerkinfrastruktur angemessene technische und organisatorische Sicherheitsmaßnahmen ein.

Art und Umfang der Maßnahmen richten sich nach dem Schutzbedarf der verarbeiteten Daten, dem Stand der Technik sowie den technischen und betrieblichen Gegebenheiten.

Die Sicherheitsinfrastruktur und die eingesetzten Sicherheitsmaßnahmen werden regelmäßig überprüft und unter Berücksichtigung technischer Entwicklungen, erkannter Risiken und betrieblicher Erfordernisse fortentwickelt und, soweit angemessen, erweitert. Sicherheitsmaßnahmen können angepasst oder durch gleichwertige oder höherwertige Maßnahmen ersetzt werden, sofern das vereinbarte Sicherheitsniveau hierdurch nicht wesentlich vermindert wird.

2. Physische Sicherheit und Rechenzentrum

Die für den Betrieb erforderliche physische Infrastruktur wird durch vom Betreiber beauftragte Rechenzentrums- und Infrastrukturdienstleister bereitgestellt.

Die physischen Sicherheitsmaßnahmen, insbesondere

- Zutrittskontrolle,
- Schutz der Rechenzentrumsflächen,
- Brandschutz und Branddetektion,
- Stromversorgung und unterbrechungsfreie Stromversorgung,
- gegebenenfalls Notstromversorgung,
- physischer Schutz der Server-, Speicher- und Netzwerkinfrastruktur

werden durch die jeweiligen Rechenzentrums- und Infrastrukturdienstleister umgesetzt.

Der Betreiber hat keinen unmittelbaren physischen Zugriff auf die eingesetzten Serversysteme und Rechenzentrumsflächen.

Die jeweils eingesetzten Unterauftragsverarbeiter und Infrastrukturdienstleister ergeben sich aus der gemäß Anlage 4 § 8 geführten aktuellen Liste.

3. Server- und Virtualisierungsinfrastruktur

Die für die Vereine bereitgestellten Systeme werden als virtuelle Systeme auf einer durch den Betreiber administrierten Virtualisierungsinfrastruktur betrieben.

Der Betreiber trifft angemessene Maßnahmen zum Schutz der von ihm verantworteten Systeme gegen unberechtigten Zugriff und unberechtigte Veränderungen.

Administrative Zugriffsrechte werden auf die für den Betrieb erforderlichen Personen beschränkt.

Die Systeme und die eingesetzte Infrastruktur werden im Rahmen der betrieblichen Erfordernisse gewartet und mit sicherheitsrelevanten Aktualisierungen versorgt.

4. Netzwerk- und Kommunikationssicherheit

Der Betreiber betreibt die zentrale Netzwerk- und Sicherheitsinfrastruktur einschließlich der zentralen Firewall- und VPN-Infrastruktur.

Der administrative Zugriff auf die vom Betreiber verantworteten Systeme erfolgt über hierfür vorgesehene und angemessen geschützte Zugangswege.

Netzwerke und Systeme werden entsprechend ihrer Funktion und ihres Schutzbedarfs getrennt oder segmentiert, soweit dies technisch und betrieblich erforderlich ist.

Datenübertragungen über öffentliche Netze werden, soweit technisch vorgesehen und erforderlich, durch geeignete Verschlüsselungsverfahren geschützt.

Die Internet- und Telekommunikationsanschlüsse der Vereine sowie an deren Standorten eingesetzte Netzwerk-, VPN-, Security- und sonstige Endgeräte, insbesondere Sophos RED Devices, liegen außerhalb der vom Betreiber verantworteten zentralen Infrastruktur.

5. Zugangs- und Zugriffsschutz

Administrative Zugänge zur vom Betreiber verantworteten Infrastruktur werden auf berechtigte Personen beschränkt.

Soweit technisch verfügbar und für den jeweiligen Zugang angemessen, werden zusätzliche Authentifizierungsmaßnahmen, insbesondere Mehrfaktor-Authentifizierung, eingesetzt.

Berechtigungen werden nach dem Prinzip der geringsten erforderlichen Rechte vergeben.

Administrative und sicherheitsrelevante Ereignisse werden, soweit von den jeweiligen Systemen technisch unterstützt und betrieblich erforderlich, protokolliert. Relevante Protokolldaten werden überwiegend über eine zentrale Syslog-Infrastruktur erfasst und vorgehalten.

Nicht mehr erforderliche Berechtigungen werden entzogen.

6. Protokollierung und Überwachung

Betriebs- und sicherheitsrelevante Ereignisse der vom Betreiber verantworteten Infrastruktur werden im technisch und betrieblich erforderlichen Umfang protokolliert.

Relevante Protokolldaten werden, soweit technisch möglich und sinnvoll, zentral erfasst und für die Erkennung und Analyse von Störungen und Sicherheitsereignissen vorgehalten.

Die Protokollierung dient insbesondere der Erkennung und Analyse von Störungen, Sicherheitsereignissen, fehlgeschlagenen Zugriffsversuchen und unberechtigten Zugriffen.

Umfang und Aufbewahrungsdauer der Protokolldaten richten sich nach den betrieblichen und sicherheitstechnischen Erfordernissen sowie den gesetzlichen Vorgaben.

7. Datensicherung und Wiederherstellung

Die Datensicherung erfolgt gemäß Anlage 1 des Hauptvertrags.

Sicherungssysteme und Sicherungsdaten werden durch angemessene technische und organisatorische Maßnahmen gegen unberechtigten Zugriff geschützt.

Sicherungsstände werden entsprechend den in Anlage 1 festgelegten Aufbewahrungs- und Rotationszyklen vorgehalten und anschließend im Rahmen dieser Rotation entfernt.

Wiederherstellungen aus vorhandenen Sicherungsständen erfolgen nach Maßgabe der in Anlage 1 beschriebenen Leistungen.

8. Sicherheitsaktualisierungen und Wartung

Der Betreiber installiert für die von ihm verantworteten Systeme sicherheitsrelevante Aktualisierungen im Rahmen angemessener Wartungs- und Aktualisierungszyklen.

Bei kritischen Sicherheitslücken oder konkreten Sicherheitsrisiken können erforderliche Maßnahmen auch außerhalb regulärer Wartungsfenster durchgeführt werden.

Der Betreiber ist berechtigt, eingesetzte technische Systeme, Hard- und Software sowie Sicherheitskomponenten durch gleichwertige oder höherwertige Lösungen zu ersetzen, sofern das vereinbarte Sicherheitsniveau nicht wesentlich vermindert wird.

9. Sicherheitsvorfälle

Sicherheitsrelevante Ereignisse werden entsprechend ihrer Art und Schwere bewertet und im Rahmen der technischen und betrieblichen Möglichkeiten bearbeitet.

Soweit ein Sicherheitsvorfall personenbezogene Daten des Vereins betrifft, gelten ergänzend die Regelungen über Datenschutzverletzungen gemäß Anlage 4.

10. Verantwortungsabgrenzung

Das Sicherheitskonzept umfasst ausschließlich die vom Betreiber verantwortete Server-, Betriebssystem-, Virtualisierungs-, zentrale Netzwerk-, Firewall- und VPN-Infrastruktur.

Die Anwendung MIA einschließlich ihrer anwendungsspezifischen Administration, Konfiguration, Aktualisierung und fachlichen Nutzung liegt nicht im Verantwortungsbereich des Betreibers.

Ebenfalls nicht umfasst sind die lokalen IT-Systeme, Internet- und Telekommunikationsanschlüsse sowie die an den Standorten der Vereine eingesetzten Netzwerk-, VPN-, Security- und sonstigen Endgeräte.

Anlage 4: Auftragsverarbeitungsvereinbarung (AVV)

zwischen

dem Musterverein e.V., vertreten durch den Vorstand, Musterstr. 12, 00000 Musterhausen, Vereinsregister Musterstadt, VR 0000, USt-IdNr. 0000000000,

im Folgenden: **Verantwortlicher**,

und

[Name, Anschrift, Steuernummer],

im Folgenden: **Auftragsverarbeiter**.

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Pflichten der Parteien im Zusammenhang mit dem Vertrag über Rechenzentrumsleistungen vom **[Datum]**, im Folgenden: **Hauptvertrag**.

§ 1 Gegenstand, Dauer, Art und Zweck der Verarbeitung

1. Gegenstand ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Rahmen der Erbringung der Rechenzentrumsleistungen gemäß Hauptvertrag.
2. Die Verarbeitung erfolgt für die Dauer des Hauptvertrages sowie – soweit erforderlich – für die in § 10 genannten Exit-/Löschfristen.
3. Der Auftragsverarbeiter stellt die für den Betrieb der Mitgliederverwaltungssoftware MIA erforderliche Rechenzentrums- und Hosting-Infrastruktur bereit. Er speichert und sichert die in MIA verarbeiteten personenbezogenen Daten und verarbeitet technische Protokoll- und Metadaten, soweit dies für den sicheren Betrieb, die Fehleranalyse, die Datensicherung und die Wiederherstellung erforderlich ist.

Administrative Zugriffe auf Inhaltsdaten sind nur zulässig, soweit sie zur Durchführung dokumentierter Wartungs-, Support-, Wiederherstellungs- oder Sicherheitsmaßnahmen erforderlich sind. Art und Umfang der konkret beauftragten Leistungen und die jeweiligen Verantwortungsgrenzen ergeben sich aus Anlage 1 des Hauptvertrags.

4. Zweck der Verarbeitung ist die Bereitstellung und der Betrieb der vertraglich geschuldeten Leistungen einschließlich Sicherstellung von Verfügbarkeit, Integrität, Vertraulichkeit und Belastbarkeit.

§ 2 Kategorien betroffener Personen und Daten

1. Je nach der Nutzung des Verantwortlichen können folgende Personen betroffen sein:
 - Beschäftigte des Verantwortlichen,
 - Mitglieder des Verantwortlichen,
 - Lieferanten/Partner,
 - Nutzer der Systeme/Anwendungen des Verantwortlichen,
 - sonstige durch den Verantwortlichen definierte Personengruppen.
2. Je nach der Nutzung des Verantwortlichen können insbesondere folgende Daten verarbeitet werden:
 - Stammdaten (Name, Kontaktdaten),
 - Vertrags-/Abrechnungsdaten,
 - Nutzungsdaten, Logdaten, Metadaten,
 - Kommunikationsinhalte,
 - Authentifizierungsdaten (z. B. Hashes/Token),
 - Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO): nein.

§ 3 Weisungsrecht des Verantwortlichen

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, sofern nicht eine gesetzliche Verpflichtung zur Verarbeitung besteht. In diesem Fall informiert der Auftragsverarbeiter den Verantwortlichen vor der Verarbeitung, soweit rechtlich zulässig.
2. Weisungen können in Textform erteilt werden. Weisungsberechtigt ist [_____].
3. Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen die DSGVO oder andere anwendbare Datenschutzbestimmungen verstößt, informiert er den Verantwortlichen unverzüglich. Er ist berechtigt, die Durchführung der betreffenden Weisung bis zu ihrer Bestätigung oder Änderung durch den Verantwortlichen auszusetzen. Offensichtlich rechtswidrige Weisungen muss der Auftragsverarbeiter nicht ausführen.
4. Standardisierte, im Hauptvertrag festgelegte Betriebsprozesse gelten als vorab dokumentierte Weisungen.

5. Weisungen dürfen den sicheren und ordnungsgemäßen Betrieb der Hosting- und Infrastrukturplattform sowie die Rechte anderer Kunden nicht beeinträchtigen. Soweit erforderlich, kann der Auftragsverarbeiter eine alternative datenschutzkonforme Umsetzung vorschlagen.

§ 4 Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich insbesondere:

- **Vertraulichkeit:** Personen, die unter seiner Verantwortung personenbezogene Daten verarbeiten, auf Vertraulichkeit zu verpflichten;
- **TOM:** geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DS-GVO umzusetzen (Details siehe § 7);
- **Unterstützung:** den Verantwortlichen bei der Erfüllung von Betroffenenrechten (§ 6), bei Datenschutz-Folgenabschätzungen (§ 9) und bei Meldungen von Verletzungen (§ 5) zu unterstützen;
- **Verzeichnis:** ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DS-GVO zu führen;
- **Nachweise:** die Einhaltung dieser AVV nach Maßgabe von § 11 nachzuweisen.

§ 5 Verletzungen des Schutzes personenbezogener Daten

1. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, spätestens innerhalb von **[24]** Stunden nach Kenntniserlangung über Verletzungen des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DS-GVO, soweit diese die Daten des Verantwortlichen betreffen. Die Meldung erfolgt über folgenden Kanal:
[_____].
2. Die Mitteilung umfasst – soweit verfügbar – insbesondere:
 - die Beschreibung der Art der Verletzung,
 - die betroffenen Datenkategorien und ungefähre Anzahl betroffener Personen/Datensätze,
 - die wahrscheinlichen Folgen,
 - die ergriffenen oder vorgeschlagenen Maßnahmen zur Abhilfe.
3. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung seiner Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DS-GVO.

4. Liegen bei der Erstmeldung noch nicht alle Informationen vor, übermittelt der Auftragsverarbeiter die verfügbaren Informationen unverzüglich und reicht weitere Erkenntnisse ohne unangemessene Verzögerung nach.

§ 6 Unterstützung bei Betroffenenrechten

1. Der Auftragsverarbeiter unterstützt den Verantwortlichen durch geeignete technische und organisatorische Maßnahmen dabei, Anträge betroffener Personen zu erfüllen (Art. 12 – 22 DS-GVO).
2. Erhält der Auftragsverarbeiter einen Antrag unmittelbar, leitet er diesen unverzüglich an den Verantwortlichen weiter, soweit er nicht gesetzlich zur Bearbeitung verpflichtet ist.

§ 7 Technische und organisatorische Maßnahmen (TOM) nach

Art. 32 DS-GVO

1. Die technischen und organisatorischen Maßnahmen (TOM) des Auftragsverarbeiters ergeben sich aus dem Sicherheitskonzept gemäß Anlage des Hauptvertrags und werden hiermit Bestandteil dieser AVV.
2. Soweit der Auftragsverarbeiter Leistungen durch Rechenzentrums- oder Infrastrukturdienstleister erbringen lässt, werden die physischen technischen und organisatorischen Maßnahmen, insbesondere Zutritts-, Gebäude-, Stromversorgungs- und Brandschutzmaßnahmen, durch diese Dienstleister umgesetzt. Der Auftragsverarbeiter stellt sicher, dass diese Dienstleister ein dem Vertrag und den Anforderungen des Art. 32 DSGVO entsprechendes Schutzniveau gewährleisten.
3. Der Auftragsverarbeiter kann die TOM weiterentwickeln, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen teilt er dem Verantwortlichen vorab mit.
4. Der Auftragsverarbeiter ist berechtigt, technische Systeme, Hard- und Software sowie Sicherheitsmaßnahmen fortlaufend weiterzuentwickeln oder zu ersetzen, sofern das datenschutzrechtliche Schutzniveau hierdurch nicht vermindert wird.

§ 8 Unterauftragsverarbeiter

1. Der Verantwortliche erteilt dem Auftragsverarbeiter eine allgemeine Genehmigung zum Einsatz von Unterauftragsverarbeitern.

2. Der Auftragsverarbeiter informiert den Verantwortlichen in Textform über beabsichtigte Änderungen (Hinzunahme/Ersetzung) von Unterauftragsverarbeitern mindestens **[30]** Tage im Voraus, soweit möglich. Die jeweils aktuelle Liste ist jederzeit unter der <https://www.gerbig.info> abrufbar.
3. Der Verantwortliche kann aus wichtigem Grund, insbesondere bei nachvollziehbaren Datenschutz-/Sicherheitsbedenken, innerhalb von **[14]** Tagen widersprechen. Können sich die Parteien nicht einigen, steht dem Verantwortlichen ein Sonderkündigungsrecht hinsichtlich der betroffenen Leistung zu.
4. Der Auftragsverarbeiter schließt mit Unterauftragsverarbeitern Verträge, die den Anforderungen von Art. 28 DS-GVO entsprechen und mindestens gleichwertige Pflichten enthalten. Der Auftragsverarbeiter bleibt gegenüber dem Verantwortlichen für die Erfüllung der Pflichten des Unterauftragsverarbeiters verantwortlich.
5. Der Einsatz von Rechenzentrums-, Hosting-, Netzwerk-, Backup-, Monitoring- und sonstigen Infrastrukturdienstleistern ist zulässig.
6. Die jeweils aktuelle Liste der Unterauftragsverarbeiter einschließlich der von ihnen erbrachten Leistungen, der Verarbeitungsorte und gegebenenfalls der eingesetzten geeigneten Garantien bei Drittlandübermittlungen wird auf der Internetseite des Auftragsverarbeiters unter **<https://www.gerbig.info>** veröffentlicht und ist Bestandteil dieser Vereinbarung.

§ 9 Unterstützung bei DSFA und Konsultation

1. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei Datenschutz-Folgenabschätzungen (Art. 35 DS-GVO) und ggf. bei der vorherigen Konsultation der Aufsichtsbehörde (Art. 36 DS-GVO), soweit die Verarbeitung dies erfordert und der Auftragsverarbeiter hierzu Informationen liefern kann.
2. Die zur Erfüllung der gesetzlichen Verpflichtungen des Verantwortlichen erforderliche Bereitstellung vorhandener und ohne besonderen Aufwand zugänglicher Informationen und Unterlagen ist mit der vereinbarten Vergütung abgegolten. Ein darüber hinausgehender Aufwand, insbesondere für individuelle Ermittlungen, Zusammenstellungen, Auswertungen oder Aufbereitungen sowie Beratungs-, Entwicklungs- oder Projektleistungen, kann nach vorheriger Vereinbarung gesondert vergütet werden. Gesetzlich zwingende unentgeltliche Unterstützungspflichten des Auftragsverarbeiters bleiben unberührt.

§ 10 Rückgabe, Löschung und Exit

1. Nach Vertragsende löscht oder gibt der Auftragsverarbeiter – nach Wahl des Verantwortlichen – alle personenbezogenen Daten zurück und löscht vorhandene Kopien, sofern keine gesetzliche Aufbewahrungspflicht besteht.
2. Der Verantwortliche teilt seine Entscheidung spätestens zum Vertragsende mit. Liegt zu diesem Zeitpunkt keine Weisung vor, hält der Auftragsverarbeiter die Daten für einen Übergangszeitraum von 30 Tagen ausschließlich zur Rückgabe bereit und löscht sie anschließend.
3. Eine Löschung muss innerhalb von **[30]** Tagen geschehen; der Auftragsverarbeiter bestätigt dem Verantwortlichen die Löschung in geeigneter Form.
4. Von der Löschung ausgenommen sind Sicherungskopien, soweit deren weitere Aufbewahrung technisch bedingt oder gesetzlich vorgeschrieben ist. Diese Daten dürfen ausschließlich zu Wiederherstellungszwecken verarbeitet werden und sind nach Ablauf der jeweiligen Aufbewahrungsfristen zu löschen.

§ 11 Nachweise, Audit, Informationsrechte

1. Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der Pflichten nach Art. 28 DSGVO nachzuweisen.
2. Audits/Inspektionen durch den Verantwortlichen oder einen zur Verschwiegenheit verpflichteten Prüfer sind nach Maßgabe des Hauptvertrags (Audit-Klausel § 12) zulässig.
3. Der Auftragsverarbeiter kann – soweit angemessen – statt Vor-Ort-Audits aktuelle Zertifikate, Auditberichte oder geeignete Prüfungsnachweise (z. B. ISO 27001, SOC-Report, BSI C5) vorlegen.
4. Die Beschränkung auf ein regelmäßiges Audit pro Kalenderjahr gilt nicht bei Datenschutzverletzungen, begründeten Zweifeln an der Vertragseinhaltung, wesentlichen Änderungen der Verarbeitung oder auf Verlangen einer zuständigen Aufsichtsbehörde. Geeignete Zertifikate und Prüfberichte können bei der Festlegung von Art und Umfang eines Audits berücksichtigt werden, schließen weitergehende Kontrollen bei berechtigtem Anlass jedoch nicht aus.

5. Ein Anspruch auf Zugang zu Rechenzenträumen oder sonstigen Einrichtungen von Unterauftragsverarbeitern oder Infrastrukturdienstleistern besteht nicht, soweit nicht zwingende gesetzliche Kontrollrechte entgegenstehen. Der Auftragsverarbeiter kann geeignete Nachweise oder Zertifizierungen dieser Dienstleister vorlegen.

§ 12. Datenübermittlungen in Drittländer

1. Eine Verarbeitung/Übermittlung in Drittländer außerhalb des EWR findet nur statt, wenn die Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.
2. Etwaige Drittlandverarbeitungen und Garantien sind in der Unterauftragsverarbeiterliste gemäß § 8 Ziffer 6 zu dokumentieren.

§ 13 Vertraulichkeit

Ergänzend gelten die Vertraulichkeitsregelungen des Hauptvertrages (§ 11).

§ 14 Haftung

1. Die Haftung richtet sich nach den Haftungsregelungen des Hauptvertrages.
2. Zwingende datenschutzrechtliche Haftungsregelungen (insbesondere Art. 82 DSGVO) bleiben unberührt.
3. Soweit gesetzlich zulässig, gelten die Haftungsbeschränkungen des Hauptvertrages auch für datenschutzrechtliche Pflichtverletzungen, soweit Art. 82 DSGVO oder andere zwingende gesetzliche Vorschriften dem nicht entgegenstehen.

§ 15 Schlussbestimmungen

1. Änderungen dieser AVV bedürfen der Textform, soweit nicht gesetzlich eine strengere Form vorgeschrieben ist.
2. Bei Widersprüchen zwischen dieser AVV und dem Hauptvertrag gehen die Regelungen dieser AVV vor, soweit sie Datenschutzpflichten nach Art. 28 DSGVO konkretisieren.

Ort, Datum

Ort, Datum

Unterschrift Verantwortlicher

Unterschrift Auftragsverarbeiter