Auftragsverarbeitungsvertrag

gemäß Art. 28 Abs. 3 DSGVO

Fassung 1.0 · Stand 25.10.2026

VERANTWORTLICHER (AUFTRAGGEBER)

[Name des Vereins]
[Anschrift des Vereins]
nachfolgend „Verein“ oder „Verantwortlicher“

AUFTRAGSVERARBEITER (AUFTRAGNEHMER)

vereinigo IT OG
Gaislöd 1/18, 6067 Absam, Österreich
Firmenbuchnummer FN 686216 t, Landesgericht Innsbruck · UID ATU83571109
vertreten durch die Gesellschafter Thomas Pittl und Matteo Höllrigl
E-Mail: kontakt@vereinigo.at
nachfolgend „vereinigo“ oder „Auftragsverarbeiter“

MUSTER ohne Angaben zu einem bestimmten Verein. Der Vertrag kommt zustande, wenn der Verein bei der Registrierung die Nutzungsbedingungen einschließlich dieses Auftragsverarbeitungsvertrags akzeptiert. Nach Vertragsabschluss steht er mit den Angaben des Vereins im Nutzerkonto dauerhaft zum Abruf bereit. Der Vertrag ist Bestandteil der Nutzungsbedingungen von vereinigo (§ 7.3) und wird gemäß Art. 28 Abs. 9 DSGVO elektronisch geschlossen. Eine Unterschrift ist nicht erforderlich.

§ 1 Gegenstand, Dauer und Rollen

1.1 Dieser Vertrag regelt die Verarbeitung personenbezogener Daten durch vereinigo im Auftrag des Vereins bei der Bereitstellung der Plattform vereinigo (Web-Anwendung und Mitgliederapp) auf Grundlage der Nutzungsbedingungen von vereinigo (nachfolgend „Hauptvertrag“).

1.2 Der Verein ist Verantwortlicher im Sinne von Art. 4 Z 7 DSGVO, vereinigo ist Auftragsverarbeiter im Sinne von Art. 4 Z 8 DSGVO. Für die Stammdaten des Nutzerkontos sowie für Abrechnung, Support und die Sicherheit der Plattform ist vereinigo selbst Verantwortlicher; darauf bezieht sich dieser Vertrag nicht (siehe Datenschutzerklärung von vereinigo).

1.3 Der Vertrag beginnt mit dem Abschluss des Hauptvertrags und gilt für dessen Dauer. Er endet, wenn der Hauptvertrag beendet und die Daten nach § 11 zurückgegeben bzw. gelöscht sind. Pflichten, die ihrer Natur nach fortwirken (insbesondere Vertraulichkeit und Löschung), bleiben bestehen.

1.4 Gegenstand, Art und Zweck der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen ergeben sich aus Anlage 1.

§ 2 Weisungen des Vereins

2.1 vereinigo verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Vereins – auch in Bezug auf die Übermittlung in ein Drittland –, es sei denn, vereinigo ist nach dem Recht der Union oder eines Mitgliedstaats zur Verarbeitung verpflichtet. In diesem Fall teilt vereinigo dem Verein diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

2.2 Dokumentierte Weisungen sind dieser Vertrag samt Anlagen, die Nutzungsbedingungen sowie die Eingaben und Einstellungen, die berechtigte Personen des Vereins (insbesondere Administrator:innen) in der Plattform vornehmen, etwa das Anlegen, Ändern, Exportieren und Löschen von Daten oder das Aktivieren von Modulen. Darüber hinausgehende Einzelweisungen erteilt der Verein in Textform an kontakt@vereinigo.at; vereinigo bestätigt sie. Weisungen, die den vereinbarten Leistungsumfang überschreiten, behandeln die Parteien wie Änderungswünsche zum Hauptvertrag.

2.3 vereinigo informiert den Verein unverzüglich, wenn eine Weisung nach seiner Auffassung gegen die DSGVO oder andere Datenschutzvorschriften verstößt. vereinigo darf die Ausführung dieser Weisung aussetzen, bis der Verein sie bestätigt oder ändert.

2.4 vereinigo verarbeitet die Daten nicht für eigene Zwecke, insbesondere nicht zu Werbezwecken, zur Profilbildung oder zum Training von Systemen künstlicher Intelligenz.

§ 3 Pflichten des Vereins

3.1 Der Verein ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für das Vorliegen einer Rechtsgrundlage nach Art. 6 DSGVO (bei besonderen Kategorien zusätzlich nach Art. 9 DSGVO), und für die Wahrung der Betroffenenrechte. Er stellt sicher, dass Betroffene nach Art. 13 und 14 DSGVO informiert werden und – wo erforderlich – wirksame Einwilligungen vorliegen, bei minderjährigen Mitgliedern etwa jene der Erziehungsberechtigten.

3.2 Der Verein vergibt Rollen und Berechtigungen in der Plattform nach dem Grundsatz der Erforderlichkeit, hält Zugangsdaten geheim und entzieht Berechtigungen ausgeschiedener Funktionär:innen rechtzeitig. Besondere Kategorien personenbezogener Daten erfasst er nur, wenn dafür eine Rechtsgrundlage besteht; die Plattform enthält dafür keine eigenen Felder, Freitextfelder und hochgeladene Dokumente können solche Daten aber enthalten.

3.3 Der Verein informiert vereinigo unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

§ 4 Vertraulichkeit

4.1 vereinigo stellt sicher, dass die zur Verarbeitung befugten Personen (Gesellschafter, Mitarbeitende und Beauftragte) zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Datengeheimnis, § 6 DSG). Die Verpflichtung besteht auch nach Beendigung der Tätigkeit fort.

4.2 Auf Daten des Vereins greifen nur Personen zu, die dies zur Erfüllung des Hauptvertrags benötigen (Betrieb, Wartung, Fehlerbehebung, Support). Zugriffe im Rahmen des Supports erfolgen anlassbezogen.

§ 5 Technische und organisatorische Maßnahmen

5.1 vereinigo trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie des Risikos für die Rechte und Freiheiten der Betroffenen.

5.2 Die Maßnahmen unterliegen dem technischen Fortschritt. vereinigo darf alternative, angemessene Maßnahmen umsetzen, sofern das Schutzniveau dadurch nicht unterschritten wird. Wesentliche Änderungen dokumentiert vereinigo; die jeweils aktuelle Fassung dieses Vertrags samt Anlagen steht im Nutzerkonto bereit.

§ 6 Weitere Auftragsverarbeiter

6.1 Der Verein erteilt vereinigo die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) einzusetzen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in Anlage 3 aufgeführt.

6.2 Beabsichtigt vereinigo, einen Unterauftragsverarbeiter hinzuzufügen oder zu ersetzen, informiert vereinigo den Verein mindestens 30 Tage vorher in Textform (E-Mail an die hinterlegte Adresse oder Hinweis in der Plattform). Der Verein kann innerhalb von 14 Tagen nach Zugang aus einem wichtigen datenschutzrechtlichen Grund widersprechen. Kommt keine einvernehmliche Lösung zustande, kann der Verein den Hauptvertrag zum Zeitpunkt des geplanten Einsatzes außerordentlich kündigen.

6.3 vereinigo schließt mit jedem Unterauftragsverarbeiter einen Vertrag, der diesem im Wesentlichen dieselben Datenschutzpflichten auferlegt wie dieser Vertrag, und haftet gegenüber dem Verein für dessen Einhaltung. Auf Verlangen stellt vereinigo dem Verein eine Kopie der Vereinbarung zur Verfügung, wobei Geschäftsgeheimnisse unkenntlich gemacht werden dürfen.

§ 7 Übermittlung in Drittländer

7.1 Die Verarbeitung findet grundsätzlich in Österreich bzw. innerhalb der EU/des EWR statt. Hosting, Datenbank, Dateispeicher und E-Mail-Versand erfolgen bei einem Anbieter mit Serverstandort in Österreich.

7.2 Eine Übermittlung in ein Drittland erfolgt nur, wenn die Voraussetzungen des Kapitels V DSGVO erfüllt sind. Nach dem derzeitigen Stand betrifft das ausschließlich die Zustellung von Push-Benachrichtigungen über die Dienste von Apple und Google (Anlage 3), und nur soweit Mitglieder Benachrichtigungen auf ihrem Gerät zugelassen haben. Sie stützt sich auf die Standardvertragsklauseln der EU-Kommission bzw. einen gleichwertigen Mechanismus der Anbieter.

§ 8 Unterstützung des Vereins

8.1 vereinigo unterstützt den Verein durch geeignete technische und organisatorische Maßnahmen bei der Beantwortung von Anträgen betroffener Personen nach Kapitel III DSGVO. Dafür stehen Administrator:innen unter anderem Funktionen zum Einsehen, Berichtigen, Exportieren und Löschen von Daten zur Verfügung. Wendet sich eine betroffene Person unmittelbar an vereinigo, leitet vereinigo das Anliegen unverzüglich an den Verein weiter und beantwortet es nicht selbst.

8.2 vereinigo unterstützt den Verein unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO (Sicherheit der Verarbeitung, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung und vorherige Konsultation der Aufsichtsbehörde).

8.3 Unterstützung im Rahmen der Standardfunktionen der Plattform ist im Entgelt enthalten. Darüber hinausgehenden erheblichen Aufwand kann vereinigo nach vorheriger Information angemessen vergütet verlangen.

§ 9 Verletzung des Schutzes personenbezogener Daten

9.1 vereinigo meldet dem Verein jede Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Z 12 DSGVO, die Daten des Vereins betrifft, unverzüglich, spätestens binnen 72 Stunden nach Bekanntwerden, an die im Nutzerkonto hinterlegte E-Mail-Adresse.

9.2 Die Meldung enthält, soweit bekannt: die Art der Verletzung, die Kategorien und die ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen sowie die ergriffenen oder vorgeschlagenen Maßnahmen. Fehlende Angaben reicht vereinigo schrittweise nach.

9.3 vereinigo ergreift unverzüglich Maßnahmen zur Eindämmung und Behebung. Die Meldung an die Aufsichtsbehörde (Art. 33 DSGVO) und die Benachrichtigung der Betroffenen (Art. 34 DSGVO) obliegen dem Verein; vereinigo nimmt sie nur auf Weisung des Vereins vor.

§ 10 Nachweis- und Kontrollrechte

10.1 vereinigo stellt dem Verein alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung, insbesondere Auskünfte und die Dokumentation der technischen und organisatorischen Maßnahmen.

10.2 Der Verein ist berechtigt, die Einhaltung dieses Vertrags zu überprüfen oder durch einen zur Verschwiegenheit verpflichteten Prüfer überprüfen zu lassen, in der Regel zunächst anhand von Dokumentation und Auskünften. Eine Prüfung vor Ort findet nur aus begründetem Anlass nach mindestens 14 Tagen Vorankündigung zu den üblichen Geschäftszeiten statt, ohne den Betrieb unverhältnismäßig zu stören und unter Wahrung der Vertraulichkeit sowie der Rechte anderer Kunden von vereinigo; Zugang zu Daten anderer Vereine besteht nicht.

10.3 Jede Partei trägt ihre eigenen Kosten der Prüfung. Für darüber hinausgehenden erheblichen Aufwand kann vereinigo eine angemessene Vergütung verlangen.

§ 11 Rückgabe und Löschung

11.1 Der Verein kann seine Daten während der Vertragslaufzeit jederzeit über die Exportfunktionen der Plattform abrufen. Das gilt als Rückgabe der Daten.

11.2 Beantragt der Verein die Deaktivierung oder Kündigung seines Kontos, steht ihm eine Frist von 30 Tagen zur Verfügung, in der er seine Daten noch einsehen und sichern kann. Mit der Beendigung des Hauptvertrags löscht vereinigo die Daten des Vereins einschließlich der hochgeladenen Dateien und bestätigt dies auf Verlangen in Textform. Eine Deaktivierung ohne Kündigung führt nicht zur Löschung; die Daten bleiben dann bis zur Kündigung oder bis zu einer Löschweisung des Vereins gespeichert.

11.3 Kopien in Datensicherungen verwendet vereinigo ausschließlich zur Wiederherstellung und löscht bzw. überschreibt sie im Rahmen des turnusmäßigen Sicherungszyklus.

11.4 Verlangt das Recht der Union oder eines Mitgliedstaats die weitere Speicherung, informiert vereinigo den Verein und beschränkt die Verarbeitung auf diesen Zweck. Gesetzliche Aufbewahrungspflichten des Vereins (etwa für Buchhaltungsunterlagen nach § 132 BAO) trägt der Verein selbst; er exportiert aufbewahrungspflichtige Unterlagen rechtzeitig vor der Löschung.

§ 12 Haftung

12.1 Für die Haftung der Parteien gelten die Haftungsbestimmungen der Nutzungsbedingungen. Die Haftung gegenüber betroffenen Personen nach Art. 82 DSGVO bleibt unberührt.

§ 13 Schlussbestimmungen

13.1 Bei Widersprüchen zwischen diesem Vertrag und den Nutzungsbedingungen geht dieser Vertrag in Fragen des Datenschutzes vor.

13.2 Änderungen und Ergänzungen bedürfen der Textform. Anpassungen, die wegen einer geänderten Rechtslage, behördlicher Vorgaben oder höchstgerichtlicher Rechtsprechung erforderlich sind, teilt vereinigo dem Verein mindestens 30 Tage vor Wirksamkeit in Textform mit; der Verein kann den Hauptvertrag in diesem Fall außerordentlich kündigen.

13.3 Rechtswahl und Gerichtsstand richten sich nach den Nutzungsbedingungen (anwendbar ist österreichisches Recht). Ist eine Bestimmung dieses Vertrags unwirksam, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt; die Parteien ersetzen die unwirksame Bestimmung durch eine wirksame, die ihrem Zweck am nächsten kommt.

13.4 Ansprechstelle für Datenschutzfragen auf Seiten von vereinigo: kontakt@vereinigo.at.

ANLAGE 1

Beschreibung der Verarbeitung

Gegenstand und Zweck

- Bereitstellung und Betrieb der vom Verein gebuchten Funktionen der Plattform vereinigo als Software-as-a-Service für die Vereinsverwaltung.
- Je nach gebuchtem Paket: Mitgliederverwaltung, Termine und Veranstaltungen (inkl. Zu-/Absagen, Anwesenheit, Sitzungsprotokolle), Nachrichten und Chat, Neuigkeiten, Aufgaben, Dokumentenablage, Notizen, Fotogalerie, Buchhaltung, Rechnungen, Ressourcen- und Raumreservierung, Flohmarkt, Kantinenverkauf, Social-Media-Planer (Planung und Veröffentlichung von Beiträgen auf Facebook und Instagram), digitaler Mitgliedsausweis, Support sowie die zugehörige Mitgliederapp (iOS und Android).

Art der Verarbeitung

- Erheben und Erfassen (Eingabe durch Berechtigte, Import, Selbsteingabe durch Mitglieder), Speichern, Ordnen, Abfragen, Verwenden (Anzeige, Auswertung, Export), Offenlegen durch Übermittlung an berechtigte Nutzer:innen sowie per E-Mail und Push-Benachrichtigung, bei Nutzung des Social-Media-Planers auf Weisung des Vereins an Meta zur Veröffentlichung auf Facebook und Instagram, Berichtigen, Einschränken, Löschen und Sichern.

Kategorien betroffener Personen

- Mitglieder des Vereins, auch minderjährige Mitglieder
- Funktionär:innen, Trainer:innen und sonstige Nutzer:innen der Plattform
- Interessenten, Gäste, Teilnehmer:innen und Kontaktpersonen (z. B. Erziehungsberechtigte)
- Kunden, Lieferanten und sonstige Geschäftspartner des Vereins (Buchhaltung, Rechnungen, Kantine)
- Personen, die in Beiträgen des Social-Media-Planers genannt oder abgebildet sind

Arten personenbezogener Daten

- Stammdaten: Name, Anschrift, Kontaktdaten, Geburtsdatum, Mitgliedsnummer, Eintritts- und Austrittsdatum, Funktion und Gruppenzugehörigkeit, Foto
- Zugangsdaten: Login-E-Mail-Adresse, Passwort (nur als Hashwert), Angaben zur Zwei-Faktor-Anmeldung
- Kommunikationsinhalte: Chat- und Gruppennachrichten, Rundmails, Statusmeldungen, Kommentare, Rückfragen
- Termindaten: Zu- und Absagen, Anwesenheiten, Aufgabenzuteilungen, Umfrageantworten
- Inhalte des Vereins: Dokumente, Notizen, Fotos und andere hochgeladene Dateien
- Social-Media-Planer: Beitragstexte und -bilder, Planungszeitpunkte und Veröffentlichungsstatus, Name bzw. Kennung der verbundenen Facebook-Seite oder des Instagram-Kontos sowie das (verschlüsselt gespeicherte) Zugangstoken dieser Konten
- Finanzdaten: Mitgliedsbeiträge, Buchungen, Rechnungen, Bankverbindungen, Verkaufsdaten
- Gerätekennungen für Push-Benachrichtigungen; Standortdaten nur, wenn der Verein „Ereignisse in der Nähe“ nutzt und das Mitglied am Gerät zustimmt
- Technische Nutzungsdaten: IP-Adresse und Zeitpunkte in Server-Protokollen, Sicherheitsereignisse

Besondere Kategorien (Art. 9 DSGVO)

- Nicht vorgesehen. Die Plattform enthält keine Felder dafür; Freitexte und Dokumente können solche Daten enthalten, wenn der Verein sie dort ablegt (siehe § 3.2).

Dauer der Verarbeitung und Ort

- Für die Dauer des Hauptvertrags; Rückgabe und Löschung nach § 11.
- Verarbeitung in Österreich (Hosting) bzw. in der EU/im EWR; Ausnahmen nur nach § 7 und Anlage 3.

ANLAGE 2

Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

1. Vertraulichkeit

- Zugangskontrolle: Anmeldung mit persönlichem Konto (E-Mail-Adresse und Passwort). Passwörter werden ausschließlich als Hashwert gespeichert; eine Passwort-Richtlinie (Mindestlänge, Ablehnung häufiger und leicht erratbarer Muster) gilt an allen Stellen, an denen ein Passwort gesetzt wird. Fehlversuche bei der Anmeldung werden gedrosselt (Schutz vor Brute-Force). Eine Zwei-Faktor-Anmeldung (TOTP) steht Administrator:innen, Bearbeiter:innen und dem Betreiberteam zur Verfügung.
- Sitzungsschutz: serverseitige Sitzungen mit gesichertem Cookie (HttpOnly, Secure, SameSite), begrenzter Gesamt- und Inaktivitätsdauer; getrennte Sitzungsspeicher für Produktiv- und Testumgebung.
- Zugriffskontrolle: Rollenkonzept (Administrator:in, Bearbeiter:in, Mitglied) mit modulbezogenen Freigaben und konfigurierbaren App-Berechtigungen je Mitgliederklasse; sensible Aktionen (z. B. Kündigung oder Deaktivierung des Kontos, Änderung der Umsatzsteuerbefreiung) verlangen zusätzlich das aktuelle Passwort. Das Verbinden und Trennen von Social-Media-Konten sowie das Planen und Veröffentlichen von Beiträgen steht nur Administrator:innen und Bearbeiter:innen mit Modulfreigabe zur Verfügung.
- Mandantentrennung: Jede Abfrage und jeder Dateizugriff ist an die Vereinsinstanz des angemeldeten Benutzers gebunden; die Trennung wird in wiederkehrenden Sicherheitsprüfungen kontrolliert.
- Verschlüsselung: durchgehend verschlüsselte Übertragung (TLS, HSTS); Chat-Nachrichten, Bankverbindungen in den Rechnungseinstellungen und Zugangsdaten zu angebundenen Diensten (darunter die Zugangstoken verbundener Facebook- und Instagram-Konten) werden verschlüsselt gespeichert (AES-256-GCM); der digitale Mitgliedsausweis verwendet einen signierten, nur kurz gültigen QR-Code.
- Dateizugriff: Dokumente und Anhänge werden ausschließlich über authentifizierte, mandantengeprüfte Abrufe ausgeliefert; hochgeladene Dateien durchlaufen eine Typ- und Inhaltsprüfung.
- Datensparsamkeit: keine Werbe- oder Tracking-Dienste; Inhalte fremder Server werden nur eingebunden, soweit eine Funktion es erfordert (Kartenansicht über OpenStreetMap, Bezahlung von Rechnungen von vereinigo über PayPal oder Stripe - siehe Anlage 3); ein einziges technisch notwendiges Cookie. Die eigene Kopie eines Beitragsbilds wird nach der vollständigen Veröffentlichung gelöscht; zur Anzeige im Redaktionsplan abgerufene Bilder werden höchstens zehn Minuten auf dem Server zwischengespeichert.

2. Integrität

- Weitergabekontrolle: Daten werden nur über verschlüsselte Verbindungen übertragen; Exporte stehen nur berechtigten Rollen zur Verfügung; Datenbanksicherungen sind dem Betreiberteam vorbehalten. Beiträge werden nur nach ausdrücklicher Aktion einer berechtigten Person (Planung oder Sofort-Veröffentlichung) an Facebook bzw. Instagram übermittelt, die Häufigkeit solcher Aktionen ist begrenzt; Bilder stellt vereinigo Meta nur über eine nicht erratbare Adresse bereit. Beim Trennen eines Kontos wird das Zugangstoken gelöscht und, soweit technisch möglich, bei Meta widerrufen.
- Eingabe- und Angriffsschutz: parametrisierte Datenbankabfragen, Schutz vor Cross-Site-Request-Forgery bei allen schreibenden Anfragen, Bereinigung von Benutzereingaben bei der Ausgabe, Sicherheits-Header (u. a. Content-Security-Policy, X-Frame-Options, X-Content-Type-Options).
- Nachvollziehbarkeit: Buchhaltungsrelevante Vorgänge werden mit fortlaufender Nummer, Zeitstempel und Benutzerbezug abgelegt, abgeschlossene Zeiträume sind gesperrt; sicherheitsrelevante Ereignisse werden protokolliert und dem Betreiberteam gemeldet.

3. Verfügbarkeit und Belastbarkeit

- Datensicherung: tägliche automatisierte Sicherung der Datenbank als konsistenter Schnappschuss mit Prüfsumme und Protokoll; Ablage auf von vereinigo selbst betriebenen Systemen mit Snapshots und Replikation an einen zweiten Standort; gesonderte Sicherung hochgeladener Dateien. Fehlgeschlagene oder ausbleibende Sicherungen lösen eine Warnung aus.

- Wiederherstellung: dokumentiertes Wiederherstellungsverfahren (Runbook) mit regelmäßiger Wiederherstellungsübung.
- Betrieb: Überwachung des Systemzustands (Status-Prüfungen, Fehlerprotokoll), Begrenzung der Anfragehäufigkeit zum Schutz vor Überlastung und Missbrauch, geordnete Wartungsfenster.

4. Regelmäßige Überprüfung und Bewertung

- Wiederkehrende, dokumentierte Sicherheitsprüfungen von Programmcode, Konfiguration und Mandantentrennung; Prüfung der eingesetzten Software-Bibliotheken auf bekannte Schwachstellen; zeitnahes Einspielen von Sicherheitsaktualisierungen.
- Entwicklung und Test getrennt von der Produktivumgebung; Änderungen werden in einer Versionsverwaltung nachvollzogen.

5. Organisatorische Maßnahmen

- Verpflichtung aller zugriffsberechtigten Personen zur Vertraulichkeit; Zugriff nur nach dem Erforderlichkeitsprinzip, Support-Zugriffe anlassbezogen.
- Verfahren für Datenschutzverletzungen mit Meldung an den Verein innerhalb von 72 Stunden (§ 9).
- Auftragskontrolle: Unterauftragsverarbeiter werden vertraglich gebunden (§ 6, Anlage 3).
- Löschkonzept: Rückgabe und Löschung nach § 11, einschließlich hochgeladener Dateien.

ANLAGE 3

Unterauftragsverarbeiter

Zum Zeitpunkt der Fassung 1.0 (Stand 25.10.2026) setzt vereinigo folgende Unterauftragsverarbeiter ein:

Unterauftragsverarbeiter	Leistung	Verarbeitete Daten	Standort / Grundlage
World4You Internet Services GmbH Hafenstraße 47–51, 4020 Linz, Österreich	Hosting der Plattform: Webserver, Datenbank, Dateispeicher; E-Mail-Versand	Alle in der Plattform verarbeiteten Daten des Vereins, E-Mail-Adressen und Inhalte versandter Nachrichten	Serverstandort Österreich; AV-Vertrag nach Art. 28 DSGVO
Apple Distribution International Ltd. Hollyhill Industrial Estate, Cork, Irland	Zustellung von Push-Benachrichtigungen an die iOS-App (Apple Push Notification Service)	Gerätekennung und Text der Benachrichtigung	Übermittlung in die USA auf Grundlage der Standardvertragsklauseln der EU-Kommission bzw. eines gleichwertigen Mechanismus des Anbieters
Google Ireland Ltd. Gordon House, Barrow Street, Dublin 4, Irland	Zustellung von Push-Benachrichtigungen an die Android-App (Firebase Cloud Messaging)	Geräte-Token und Text der Benachrichtigung	Übermittlung in die USA auf Grundlage der Standardvertragsklauseln der EU-Kommission bzw. eines gleichwertigen Mechanismus des Anbieters

Keine Unterauftragsverarbeitung

- Eigene Infrastruktur von vereinigo: Die Ablage von Dokumenten und Datensicherungen sowie das Ticketsystem des Supports erfolgen auf Systemen, die vereinigo selbst betreibt. Es handelt sich nicht um Dienste Dritter.
- Kartenansicht in der Web-App und Kartenvorschau in der Android-App: Dabei ruft der Browser bzw. das Gerät des Nutzers Kartenkacheln direkt von der OpenStreetMap Foundation ab (technisch bedingt mit der IP-Adresse des Geräts und den Koordinaten des angezeigten Kartenausschnitts); darüber hinaus werden keine Daten des Vereins übermittelt.
- Zahlungsdienste (PayPal, Stripe): Sie dienen nur der Bezahlung von Rechnungen von vereinigo an den Verein; vereinigo ist dabei selbst Verantwortlicher. Sobald offene Rechnungen mit PayPal-Zahlungsmöglichkeit angezeigt werden, lädt der Browser das PayPal-Zahlungsmodul direkt von PayPal; bei Stripe erfolgt eine Weiterleitung auf die Zahlungsseite von Stripe. Mitgliederdaten werden nicht übermittelt.
- Funktionen auf Veranlassung des Vereins: Nutzt der Verein optionale Funktionen, die Daten an Dienste Dritter übertragen (z. B. die Veröffentlichung von Beiträgen auf Facebook oder Instagram), geschieht dies auf Weisung des Vereins; der jeweilige Dienst ist insoweit eigenständig verantwortlich.
- Social-Media-Planer: Verbindet der Verein ein Facebook- oder Instagram-Konto, übermittelt vereinigo auf Weisung des Vereins Beitragstext und Bild über die Schnittstelle von Meta an Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irland (Anmeldung über das vom Verein erteilte Zugangstoken). Meta verarbeitet die veröffentlichten Inhalte als eigenständig Verantwortlicher nach den eigenen Bedingungen; Meta ist der vom Verein gewählte Empfänger, kein Unterauftragsverarbeiter von vereinigo. Das Zugangstoken speichert vereinigo verschlüsselt und löscht es beim Trennen des Kontos. Für die Rechtmäßigkeit der veröffentlichten Inhalte (z. B. die Einwilligung abgebildeter Personen) ist der Verein verantwortlich.