# Auftragsverarbeitungsvertrag (AVV)

> Diese Auftragsverarbeitungsvereinbarung (AVV) gilt für alle Vereine und Organisationen, die fillQR nutzen. Sie ist Bestandteil unserer Nutzungsbedingungen (§ 7). Beim Onboarding bestätigst du die Annahme dieser AVV — die zustimmungsrelevanten Daten (Datum, Version, IP-Adresse) werden in unserem Audit-Log gespeichert.

AVV als PDF herunterladen (Version 1.0)

## Präambel und Vertragsparteien

Dieser Auftragsverarbeitungsvertrag (nachfolgend „AVV") wird geschlossen zwischen dem jeweiligen Verein oder der jeweiligen Organisation, die fillQR nutzt (nachfolgend **„Verantwortlicher"**), und

| Partei | Daten |
|---|---|
| **Auftragsverarbeiter** | **ERP Buddy**, Jacqueline Bergmann, Ellhornstraße 13, 27628 Hagen im Bremischen, E-Mail: info@erp-buddy.de |
| **Verantwortlicher** | Der jeweilige Verein oder die jeweilige Organisation, die fillQR über das Onboarding-Formular oder auf manuellem Wege in Betrieb genommen hat und die im fillQR-System hinterlegten Stammdaten als Identifikationsgrundlage dienen. |

Nachfolgend werden Auftragsverarbeiter und Verantwortlicher gemeinsam als **„Parteien"** bezeichnet.

Der Verantwortliche betreibt fillQR als digitales Werkzeug zur Datenerfassung (z. B. Mitgliedsanträge, Formulare, QR-Code-basierte Abläufe). Dabei verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag und nach Weisung des Verantwortlichen. Dieser AVV regelt die datenschutzrechtlichen Anforderungen dieser Auftragsverarbeitung gemäß Art. 28 DSGVO.

## § 1 Gegenstand und Dauer der Verarbeitung

**Gegenstand:** Der Auftragsverarbeiter stellt dem Verantwortlichen die fillQR-SaaS-Plattform zur Verfügung. Im Rahmen dieser Leistungserbringung verarbeitet der Auftragsverarbeiter personenbezogene Daten, die der Verantwortliche über die Plattform erfasst, speichert oder verarbeitet — insbesondere im Rahmen des Produkts **VereinsBuddy** (digitaler Mitgliedsantrag, Mitgliederverwaltung, Kommunikation mit Mitgliedern).

**Dauer:** Dieser AVV gilt für die Dauer des Nutzungsvertrags zwischen den Parteien. Er endet automatisch mit Kündigung oder Beendigung des Nutzungsvertrags. Die Regelungen zur Löschung und Rückgabe von Daten (§ 9) gelten über das Vertragsende hinaus bis zur vollständigen Erfüllung.

## § 2 Art und Zweck der Verarbeitung

**Art der Verarbeitung:** Erhebung, Speicherung, Übermittlung, Strukturierung, Abfrage, Verwendung, Anpassung, Löschung und Vernichtung personenbezogener Daten.

**Zweck:** Die Verarbeitung erfolgt ausschließlich zur Erbringung der vertraglich vereinbarten SaaS-Leistungen von fillQR. Dazu gehören insbesondere:

- Entgegennahme und Verwaltung von digitalen Mitgliedsanträgen (VereinsBuddy)
- Verwaltung der Mitgliederdaten (Status, Beitragsarten, Abteilungen, SEPA-Mandate)
- Versand transaktionaler E-Mails (Eingangsbestätigung, Willkommens-Mail, Passwort-Reset)
- Bereitstellung des Admin-Dashboards und der Auswertungsfunktionen
- Betrieb der technischen Infrastruktur (Server, Datenbank, Backup)
- Technische Wartung und Weiterentwicklung der Plattform

Eine Verarbeitung zu anderen Zwecken — insbesondere zu eigenen Zwecken des Auftragsverarbeiters, zu Werbezwecken oder zur Weitergabe an Dritte ohne Weisung des Verantwortlichen — findet nicht statt.

## § 3 Art der personenbezogenen Daten

Gegenstand der Verarbeitung können folgende Datenkategorien sein:

- **Stammdaten:** Vorname, Nachname, Geburtsdatum, Geschlecht, Anschrift (Straße, PLZ, Ort)
- **Kontaktdaten:** E-Mail-Adresse, Telefonnummer
- **Mitgliedschaftsdaten:** Mitgliedsnummer, Eintrittsdatum, Status, Mitgliedstyp, Abteilungen (Sparten), Austrittsdatum
- **Bankdaten (optional):** IBAN, BIC, Kontoinhaber, SEPA-Mandatsreferenz (sofern SEPA-Lastschrift aktiviert)
- **Daten Minderjähriger:** Geburtsdatum (zur Erkennung der Minderjährigkeit), ggf. Daten der Erziehungsberechtigten (Vor-/Nachname, E-Mail, Telefon, Anschrift)
- **Zusatzfelder (optional, je Tenant-Konfiguration):** Fotoeinwilligung, Newsletter-Anmeldung, Ehrenamt-Opt-in, Spendenbereitschaft, Empfehlungsquelle
- **Fotos (optional):** Profilbild, sofern vom Verantwortlichen aktiviert
- **Technische Daten:** IP-Adressen (für Rate-Limiting, 7 Tage Retention), Session-Daten, Log-Einträge (scrubbed, max. 7 Tage)
- **Login-Daten:** E-Mail-Adresse und bcrypt-gehashtes Passwort der Admin-Nutzer des Vereins

## § 4 Kategorien betroffener Personen

Von der Verarbeitung können folgende Personengruppen betroffen sein:

- **Vereinsmitglieder:** Personen, die einen Mitgliedsantrag gestellt haben oder als Mitglied geführt werden
- **Antragsteller:** Personen, die einen Mitgliedsantrag ausgefüllt haben, aber noch keinen abgeschlossenen Mitgliedsstatus haben

- **Erziehungsberechtigte:** Eltern oder gesetzliche Vertreter minderjähriger Antragsteller
- **Admin-Nutzer des Vereins:** Mitarbeiter oder Funktionsträger des Vereins, die das Admin-Dashboard nutzen
- **Kontaktpersonen:** Personen, die über das Kontaktformular der Landingpage eine Anfrage gestellt haben (betrifft ERP Buddy als Verantwortlichen, nicht diesen AVV)

## § 5 Pflichten des Auftragsverarbeiters

### 5.1 Weisungsgebundenheit

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Auftrag und auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach dem Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, zur Verarbeitung verpflichtet. 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.

Weisungen werden in der Regel durch die Konfiguration und Nutzung der fillQR-Plattform durch den Verantwortlichen erteilt. Darüber hinaus können schriftliche Weisungen per E-Mail an info@erp-buddy.de erteilt werden.

### 5.2 Vertraulichkeit

Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeitsverpflichtung besteht auch nach Beendigung des Vertrags fort.

### 5.3 Technische und organisatorische Maßnahmen (TOM)

Der Auftragsverarbeiter trifft alle erforderlichen Maßnahmen gemäß Art. 32 DSGVO. Die konkret umgesetzten Maßnahmen sind in Anlage 1 (TOM) zu diesem AVV beschrieben. Es werden ausschließlich tatsächlich umgesetzte und aktiv betriebene Maßnahmen aufgeführt.

### 5.4 Unterstützung bei Betroffenenrechten

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung der Pflicht des Verantwortlichen, Anträge auf Wahrnehmung der Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch) zu beantworten.

Die fillQR-Plattform stellt technisch sicher, dass:

- Mitgliedsdaten durch Admin-Nutzer exportiert werden können (CSV-Export)
- Mitgliedsdaten durch Admin-Nutzer gelöscht werden können (Hard-Delete mit Audit-Log, Art. 17 DSGVO)
- Alle Daten eines Tenants auf Antrag gelöscht werden können (Tenant-Löschung mit 30-Tage-Karenz, vollständige Datenlöschung inkl. Uploads)

### 5.5 Meldepflicht bei Datenpannen (48-Stunden-Frist)

Bei Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten (Datenpanne) nach Art. 33 DSGVO informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, spätestens jedoch innerhalb von **48 Stunden** nach Bekanntwerden per E-Mail an die im fillQR-System hinterlegte Admin-E-Mail-Adresse des Verantwortlichen. Diese verkürzte interne Frist ermöglicht es dem Verantwortlichen, seine eigene **72-Stunden-Meldefrist** gegenüber der Aufsichtsbehörde nach Art. 33 Abs. 1 DSGVO einzuhalten.

Die Meldung enthält soweit möglich: Art der Verletzung, betroffene Datenkategorien und betroffene Personengruppen (ca. Anzahl), wahrscheinliche Folgen, ergriffene oder vorgeschlagene Abhilfemaßnahmen.

### 5.6 Datenschutz-Folgenabschätzung

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Durchführung von Datenschutz-Folgenabschätzungen (DSFA) sowie bei vorherigen Konsultationen der Aufsichtsbehörden, sofern der Verantwortliche dazu verpflichtet ist.

## § 6 Rechte und Pflichten des Verantwortlichen

Der Verantwortliche trägt die alleinige Verantwortung für die Rechtmäßigkeit der Datenverarbeitung im Sinne der DSGVO. Er hat insbesondere sicherzustellen, dass:

- die Verarbeitung der personenbezogenen Daten über fillQR auf einer Rechtsgrundlage nach Art. 6 DSGVO beruht;
- betroffene Personen vor der Datenerhebung über die Verarbeitung informiert werden (Art. 13 DSGVO), insbesondere über den Einsatz von fillQR als Auftragsverarbeiter;
- bei der Erfassung von Daten Minderjähriger die erforderlichen Einwilligungen der Erziehungsberechtigten vorliegen;
- dem Auftragsverarbeiter nur solche personenbezogenen Daten zur Verarbeitung übermittelt werden, die zur Zweckerfüllung notwendig sind (Datensparsamkeit);
- der Verantwortliche den Auftragsverarbeiter unverzüglich informiert, wenn bei einer Prüfung oder im Betrieb Fehler oder Unregelmäßigkeiten in Bezug auf datenschutzrechtliche Bestimmungen festgestellt werden.

Weisungen werden schriftlich oder in Textform (E-Mail an info@erp-buddy.de) erteilt. Mündliche Weisungen werden vom Verantwortlichen unverzüglich schriftlich bestätigt.

## § 7 Unterauftragsverarbeiter (Subprozessoren)

Der Auftragsverarbeiter setzt zur Leistungserbringung die in der Subprozessoren-Liste (Anlage dieser AVV) aufgeführten Unterauftragsverarbeiter ein. Diese Liste wird bei Änderungen aktualisiert.

Aktuell eingesetzte Subprozessoren mit wesentlicher Rolle:

- **Hetzner Online GmbH** (Deutschland) — Hosting, Datenbankbetrieb, Server-Infrastruktur sowie verschlüsselte Offsite-Backups (Hetzner StorageBox). AVV abgeschlossen.

- **Scaleway SAS** (Frankreich) — Transaktionaler E-Mail-Versand. DPA abgeschlossen.
- **Cloudflare, Inc.** (USA) — DNS-Auflösung (Grey-Cloud, kein Proxy) und Bot-Schutz (Turnstile). Customer DPA abgeschlossen, EU-US DPF + SCCs.
- **Variomedia AG** (Deutschland) — Mail-Empfang für Adressen unter `fillqr.de` und Tenant-Subdomains. AVV abgeschlossen.
- **Google LLC — Google Workspace** (USA) — Mail-Empfang für die Impressum-Adresse `info@erp-buddy.de`. DPA Bestandteil der Google-Workspace-Bedingungen, EU-US DPF + SCCs.

Der Verantwortliche erteilt hiermit eine allgemeine Genehmigung zur Beauftragung weiterer Unterauftragsverarbeiter. Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen (Hinzufügung oder Ersetzung von Unterauftragsverarbeitern) mindestens **30 Tage** im Voraus per E-Mail. Der Verantwortliche kann innerhalb dieser Frist Widerspruch einlegen. Bei begründetem Widerspruch suchen die Parteien gemeinsam nach einer Lösung.

Der Auftragsverarbeiter legt denselben Datenschutzpflichten, denen er selbst unterliegt, auch seinen Unterauftragsverarbeitern auf (Art. 28 Abs. 4 DSGVO).

## § 8 Technische und organisatorische Maßnahmen (TOM)

Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 DSGVO). Die konkret umgesetzten Maßnahmen sind in Anlage 1 zu diesem AVV dokumentiert.

Der Auftragsverarbeiter ist berechtigt, die TOM weiterzuentwickeln und anzupassen, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen, die das Schutzniveau beeinflussen könnten, werden dem Verantwortlichen vorab mitgeteilt.

## § 9 Löschung und Rückgabe von Daten bei Vertragsende

Nach Beendigung des Nutzungsvertrags (Kündigung, Ablauf, Konto-Deaktivierung) verfährt der Auftragsverarbeiter wie folgt:

- **Datenexport-Fenster (30 Tage):** Der Verantwortliche hat nach Vertragsende 30 Tage Zeit, seine Daten per CSV-Export aus dem Admin-Dashboard zu exportieren. Auf Anfrage stellt der Auftragsverarbeiter einen vollständigen Datenbankexport bereit.
- **Löschung:** Nach Ablauf der 30-Tage-Karenz werden alle personenbezogenen Daten des Verantwortlichen — einschließlich Mitgliederdaten, SEPA-Mandate, E-Mail-Logs, hochgeladene Dateien (Fotos, Dokumente), Admin-Zugangsdaten und Tenant-Konfiguration — unwiderruflich gelöscht.
- **Backups:** Automatische Backups (Hetzner Auto-Backup, PostgreSQL-Dumps) werden nach spätestens 7 Tagen nach vollständiger Löschung des Tenant-Datensatzes aus dem Backup-Rotation-Zyklus ausgeschlossen. Eine vollständige Löschung aus allen Backup-Schichten ist innerhalb von 30 Tagen nach der Tenant-Löschung abgeschlossen.
- **Löschbestätigung:** Auf Anfrage stellt der Auftragsverarbeiter eine schriftliche Bestätigung der vollständigen Datenlöschung aus.

## § 10 Audit- und Kontrollrechte

Der Verantwortliche hat das Recht, die Einhaltung dieses AVV und der geltenden Datenschutzvorschriften durch den Auftragsverarbeiter zu überprüfen. Das Kontrollrecht kann wahrgenommen werden durch:

- **Dokumentationsanfragen:** Anforderung von Nachweisen, Zertifikaten, Protokollen oder Berichten per E-Mail an info@erp-buddy.de;
- **Fragebögen:** Einsendung von Datenschutz-Fragebögen oder Sicherheitsfragebögen, die der Auftragsverarbeiter innerhalb angemessener Frist (in der Regel 14 Werktage) beantwortet;
- **Vor-Ort-Prüfungen:** Ankündigung mindestens 4 Wochen im Voraus; Kosten trägt der Verantwortliche, sofern keine wesentlichen Verstöße festgestellt werden.

Audits durch akkreditierte Prüfer mit gleichwertigen Erkenntnissen (z. B. ISO 27001) können Vor-Ort-Prüfungen ersetzen.

## § 11 Haftung

Die Haftung der Parteien richtet sich nach den gesetzlichen Regelungen sowie den Bestimmungen der DSGVO. Insbesondere gilt:

- Jede Partei haftet gegenüber betroffenen Personen für den Schaden, den sie durch eine DSGVO-widrige Verarbeitung verursacht hat (Art. 82 DSGVO).
- Handelt der Auftragsverarbeiter entgegen den Weisungen des Verantwortlichen oder unter Verstoß gegen diesen AVV, gilt er insoweit als Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO.
- Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen im Übrigen nach Maßgabe des zwischen den Parteien geschlossenen Nutzungsvertrags.

## § 12 Schlussbestimmungen

### 12.1 Schriftform

Änderungen und Ergänzungen dieses AVV bedürfen der Textform (E-Mail genügt). Die Nutzung der fillQR-Plattform nach Inkrafttreten einer neuen AVV-Version gilt als Zustimmung, sofern der Verantwortliche der neuen Version nicht innerhalb von 30 Tagen nach Benachrichtigung widerspricht.

### 12.2 Anwendbares Recht und Gerichtsstand

Es gilt deutsches Recht. Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz des Auftragsverarbeiters.

### 12.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieses AVV ganz oder teilweise unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die unwirksame oder undurchführbare Bestimmung ist durch eine wirksame zu ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt.

### 12.4 Verhältnis zum Nutzungsvertrag

Dieser AVV ist Bestandteil des Nutzungsvertrags und ergänzt diesen in datenschutzrechtlicher Hinsicht. Im Falle von Widersprüchen zwischen diesem AVV und dem Nutzungsvertrag in Bezug auf die Verarbeitung personenbezogener Daten hat dieser AVV Vorrang.

### 12.5 Elektronische Zustimmung

Diese Vereinbarung kommt durch die elektronische Zustimmung im Onboarding-Prozess zustande und ist auch ohne handschriftliche Unterschrift rechtlich bindend. Die Zustimmung wird in unserem System (Datenbank-Tabelle `tbl_consent`) mit folgenden Audit-Daten dokumentiert: Datum der Zustimmung, AVV-Version, IP-Adresse des Zustimmenden. Der Verein kann auf Anfrage jederzeit eine Kopie des Audit-Eintrags sowie der zum Zustimmungs-Zeitpunkt gültigen AVV-Version anfordern (per E-Mail an info@erp-buddy.de).

Bei wesentlichen späteren Änderungen dieser AVV (z. B. neue Subprozessoren) wird eine neue Version zur erneuten Zustimmung vorgelegt. Die Zustimmungs-Spur (Datum, AVV-Version, IP-Adresse) wird ebenfalls im Audit-Log dokumentiert.

---

## Anlage 1: Technische und organisatorische Maßnahmen (TOM)

*Stand: 12. Juni 2026 | Gilt für: fillQR Produktionsinfrastruktur auf Hetzner Falkenstein*

Nachfolgend sind ausschließlich technische und organisatorische Maßnahmen aufgeführt, die zum Zeitpunkt der Erstellung dieses Dokuments aktiv umgesetzt sind und in Betrieb sind. Geplante oder in Entwicklung befindliche Maßnahmen werden erst nach vollständiger Umsetzung in dieses Dokument aufgenommen.

### A. Vertraulichkeit

#### A.1 Zugangskontrolle (Unbefugter Zugang zur Infrastruktur wird verhindert)

| Maßnahme | Umsetzung |
|---|---|
| Hetzner Cloud-Firewall | Netzwerk-Firewall vor dem Server: eingehend nur Web-Ports (HTTP, HTTPS) und ein administrativer SSH-Port erlaubt. SSH ist zusätzlich auf autorisierte Admin-Quellen beschränkt. Alle anderen Ports und Protokolle werden geblockt. |
| UFW (Uncomplicated Firewall) | Host-basierte Firewall auf dem Server: nur die freigegebenen Web- und Admin-Ports erlaubt, deny default für alle anderen eingehenden Verbindungen. |
| SSH-Hardening | SSH läuft auf einem nicht-standardmäßigen Port. Key-Only-Authentifizierung (kein Passwort-Login). PermitRootLogin deaktiviert. X11-Forwarding deaktiviert. |
| Tailscale (VPN-Overlay) | Internes administratives VPN-Overlay für autorisierte Admin-Zugriffe und Monitoring. Mobiler Zugriff verifiziert. Kein offener Admin-Port im öffentlichen Internet. |
| fail2ban | Automatische IP-Sperrung nach mehreren Fehlversuchen beim SSH-Login. sshd-Jail aktiv überwacht. Autorisierte Admin-Quellen sind in `ignoreip` eingetragen. |
| PostgreSQL — kein externer Zugriff | Die Datenbank ist ausschließlich auf 127.0.0.1 (localhost) gebunden und nicht aus dem Internet erreichbar. Externer Zugriff nur über verschlüsselten SSH-Tunnel. |

### A.2 Zugriffskontrolle (Nur berechtigte Personen können auf Daten zugreifen)

| Maßnahme | Umsetzung |
|---|---|
| Row-Level-Security (RLS) auf Datenbankebene | PostgreSQL RLS-Policies sind auf 10 Mandanten-Tabellen aktiv (tbl_tenants, tbl_members, tbl_guardians, tbl_sepa_mandates u. a.). Separater Datenbank-Nutzer `fillqr_app_rls` mit aktiver RLS für alle tenant-scoped Queries. Tenant-ID wird als PostgreSQL-Session-Variable gesetzt ( `set_config` ). Cross-Tenant-Datenlecks sind auf DB-Ebene technisch verhindert. |
| Caddy IP-Whitelist für Admin-Bereiche | pgAdmin und Betreiber-Panel (admin.fillqr.de) sind durch IP-Whitelist auf autorisierte Admin-Quellen beschränkt. Kein externer Zugriff aus dem öffentlichen Internet. |
| Session-basierte Authentifizierung | Admin-Zugang zu Vereinsdaten erfolgt ausschließlich über authentifizierte Sessions (iron-session, 7 Tage). E-Mail + bcrypt-Hash (Faktor 10). Kein offener API-Zugang ohne Authentifizierung. |
| Rate-Limiting (Brute-Force-Schutz) | App-seitiges Rate-Limiting: Login 5 Versuche/15 min/E-Mail, Betreiber 5/15 min/IP, Vergessen-Passwort 3/h/E-Mail. Caddy-seitiges Rate-Limiting: global 300 req/min/IP, Login 5/15 min, Formular-Submit 10/min. Defense-in-Depth: beide Schichten aktiv. |
| Tenant-isolierter E-Mail-Versand | Jeder Verein sendet E-Mails über eine eigene Subdomain ( `<slug>.fillqr.de` ) mit eigenem DKIM-Schlüssel. Kompromittierung der Mail-Reputation eines Vereins hat keine Auswirkungen auf andere Vereine. |

### A.3 Pseudonymisierung und Datensparsamkeit

| Maßnahme | Umsetzung |
|---|---|
| Logs-Scrubbing | Zentraler Logger mit automatischem Scrubbing: E-Mail-Adressen, IBANs, Kartennummern und sensible Schlüsselwörter (password, token, secret, authorization) werden in Logs durch Platzhalter ersetzt. Kein Klardaten-Logging. |
| IBAN-Anzeige maskiert | Im CSV-Export werden IBAN-Nummern maskiert ausgegeben. Vollständige IBAN nur in der Datenbankzeile des SEPA-Mandats gespeichert (erforderlich für den Beitragseinzug durch den Verein). |
| Foto-EXIF-Daten entfernt | Hochgeladene Profilfotos werden serverseitig mit Sharp re-encodet. GPS-Koordinaten und alle EXIF-Metadaten werden dabei entfernt. Ausgabe: JPEG max. 1200×1200 px via mozjpeg. |
| Rate-Limit-Daten-Cleanup | IP-basierte Rate-Limit-Einträge (tbl_login_attempts) werden automatisch nach 7 Tagen via Cleanup-Cron gelöscht. |

## B. Integrität

### B.1 Weitergabekontrolle (Daten werden nur verschlüsselt übertragen)

| Maßnahme | Umsetzung |
|---|---|
| TLS-Verschlüsselung (HTTPS) | Alle Verbindungen zur fillQR-Anwendung und Landingpage erfolgen ausschließlich über HTTPS (TLS). Let's-Encrypt-Zertifikat mit automatischer Erneuerung via Caddy + Cloudflare DNS-Challenge. HTTP-Anfragen werden automatisch auf HTTPS umgeleitet. |
| Security-Header | Caddy setzt folgende Security-Header auf alle Responses: HSTS (Strict-Transport-Security), X-Content-Type-Options: nosniff, X-Frame-Options: DENY, Referrer-Policy: strict-origin-when-cross-origin, Permissions-Policy, Content-Security-Policy (CSP). |
| Bot-Schutz auf Formularen | Cloudflare Turnstile (Privacy-First-CAPTCHA) auf allen öffentlichen Formularen (Kontaktformular, Self-Signup, Mitgliedsantrag, Login). Keine Cookies, kein User-Tracking durch Turnstile. |

### B.2 Eingabekontrolle (Datenintegrität bei Eingabe)

| Maßnahme | Umsetzung |
|---|---|
| Serverseitige Validierung (Zod) | Alle eingehenden API-Anfragen werden serverseitig mit Zod-Schemas validiert. Fehlerhafte oder unvollständige Daten werden abgelehnt. |
| IBAN-Prüfziffervalidierung | SEPA-IBANs werden serverseitig auf das DE-Format und korrekte Modulo-97-Prüfziffer validiert. |
| Foto-Upload-Hardening | Hochgeladene Dateien werden per Magic-Byte-Prüfung (file-type@22) verifiziert. SVG wird strikt abgelehnt (XML-Script-Risiko). Bilder werden via Sharp re-encodet — auch nach bestandener Magic-Byte-Prüfung. |
| Audit-Log DSGVO-Löschungen | Jede Datenlöschung nach Art. 17 DSGVO wird in tbl_data_deletion_log protokolliert (Aktion, Datensatz-ID, Benutzer, Zeitstempel, Begründung). |

## C. Verfügbarkeit und Belastbarkeit

### C.1 Backup und Disaster Recovery

| Maßnahme | Umsetzung |
|---|---|
| Hetzner Auto-Backup (Server-Image) | Automatische Image-Snapshots des Servers durch Hetzner. Backup-History verfügbar. |
| Manueller Hetzner-Snapshot (Pre-Launch-Anker) | Manueller Snapshot des Produktionsstands als Recovery-Anker. Dient als schnelle Wiederherstellungsgrundlage bei kritischen Fehlern. |
| PostgreSQL-Datenbankdumps | Tägliche pg_dump-Sicherungen mit Rotation, lokal auf dem Produktionsserver. Getrennter Sicherungsweg unabhängig von Server-Snapshots. |
| Offsite-Backup auf Hetzner StorageBox | Verschlüsselte Offsite-Replikation (restic mit clientseitiger Verschlüsselung, AES-256) auf eine Hetzner StorageBox (Rechenzentrum Falkenstein, DE). Drei Backup-Pläne: System-Konfiguration, Datenbankdumps, Mitglieder-Foto-Uploads. Retention bis zu 60 Snapshots im Repository. Restic-Repo-Passwort ist kein Bestandteil des Backups (3-fach-Ablage: Server-Notfallverzeichnis, lokales Admin-Gerät, Passwort-Manager) — ein Angreifer mit Zugriff auf die StorageBox sieht ausschließlich Ciphertext. |
| Wochentlicher Restore-Verify | Automatisierter wochentlicher Lauf ( `dr-verify.sh` ) prüft Snapshot-Alter, Speicherplatz, und führt einen Stichproben-Restore-Test durch. Telegram-Alert bei Abweichung. |
| Hetzner Delete-Protection | Delete-Protection für den Produktionsserver ist aktiviert (delete=true + rebuild=true). Versehentliches Löschen über die Hetzner-API oder das Hetzner-Dashboard ist damit verhindert. |

### C.2 Betriebsüberwachung und Fehlerbehandlung

| Maßnahme | Umsetzung |
|---|---|
| System-Health-Check + Telegram-Alerts | Automatischer Health-Check täglich um 05:05 Uhr UTC. Schwellwert-basierte Benachrichtigungen (GELB/ROT/KRITISCH) per Telegram-Bot. Überwacht Festplattenauslastung, Arbeitsspeicher, Container-Status. |
| Security-Smoketest (täglich) | Automatischer Sicherheits-Smoketest via GitHub Actions täglich um 07:00 Uhr UTC gegen demo.fillqr.de. Prüft: HTTP-Security-Header, Caddy-Rate-Limits, Foto-Upload-Ablehnung. Bei Fehler Telegram-Alert. |
| Docker Restart-Policy | Alle Container laufen mit restart: unless-stopped. Automatischer Neustart bei Abstürzen ohne manuelle Intervention. |
| Unattended Upgrades | Automatische Sicherheitsupdates des Betriebssystems (Ubuntu 24.04 LTS) via unattended-upgrades. Kein automatischer Reboot — bewusst manuell kontrolliert. |
| Swap-Speicher | 4 GB Swap-Partition als Sicherheitsnetz bei Speicher-Spitzen (sysctl vm.swappiness=10 + vfs_cache_pressure=50). Verhindert OOM-Kills bei kurzzeitig erhöhter Last. |
| E-Mail-Queue mit Retry-Mechanismus | Transaktionale E-Mails werden in einer persistenten Queue (tbl_email_pending) gehalten. Bei Fehlschlag automatischer Retry mit exponentiellem Backoff (bis zu 5 Versuche, Gesamtfenster ~2,5 Stunden). Nach endgültigem Fehlschlag Telegram-Alert. |

**Hinweis zu Telegram-Alerts:** Alle in diesem Abschnitt genannten Telegram-Alerts enthalten ausschließlich System-Health-Informationen (Container-Status, Schwellwert-Überschreitungen, Tenant-IDs, Mail-IDs, Fehler-Meldungen). Personenbezogene Daten der Mitglieder (Namen, E-Mail-Adressen, IP-Adressen) werden bewusst NICHT an Telegram übertragen. Telegram ist daher kein Subprozessor im Sinne von Art. 28 DSGVO und nicht in der Subprozessoren-Liste enthalten.

### D. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

| Maßnahme | Umsetzung |
|---|---|
| Täglicher automatischer Security-Smoketest | Regelmäßige automatische Prüfung aller sicherheitsrelevanten HTTP-Eigenschaften (Security-Header, Rate-Limits, Datei-Upload-Ablehnung) in der Produktionsumgebung. |
| Quartals-Review-Checkliste | Manuelle Sicherheitsprüfung nach Dokumentation in docs/security.md: TLS-Konfiguration, Certifikatsablauf, fail2ban-Logs, Backup-Restore-Test, Rate-Limit-Validierung, RLS-Isolation-Test. |
| DSGVO-Lösch-Flow dokumentiert und getestet | Mitglieder-Löschung (Art. 17) und Tenant-Löschung sind als technische Flows implementiert und in docs/dsgvo.md dokumentiert. Hard-Delete mit Kaskade, Foto-Disk-Löschung mit Path-Traversal-Schutz, Audit-Log. |
| Incident-Dokumentation | Sicherheitsrelevante Vorfälle werden dokumentiert und ausgewertet. Lessons Learned fließen in die Systemkonfiguration ein. |

---

## Anhang: Subprozessoren

*Stand: 12. Juni 2026 | Subprozessoren-Liste Version 1.0*

Wir setzen die unten genannten Subprozessoren zur Bereitstellung von fillQR ein. Änderungen an dieser Liste (neuer Subprozessor, Wegfall eines bestehenden) werden bestehenden Kunden mindestens 30 Tage vorab per E-Mail angekündigt (gemäß § 7 oben). Bei Widerspruch besteht ein Sonderkündigungsrecht.

Zur Bereitstellung der fillQR-Plattform setzen wir folgende Auftragsverarbeiter ein. Mit allen Anbietern bestehen Verträge gemäß Art. 28 DSGVO.

### Hetzner Online GmbH (Hosting)

- **Sitz:** Industriestr. 25, 91710 Gunzenhausen, Deutschland
- **Zweck:** Hosting der fillQR-Anwendung (Web-Server, PostgreSQL-Datenbank) sowie der Landingpage
- **Daten:** Alle Tenant-Daten (Mitgliederdaten, SEPA-Mandate, E-Mails in Warteschlange, Server-Logs)
- **Standort:** Rechenzentrum Falkenstein, Deutschland — keine Drittlandsübermittlung
- **AVV:** Abgeschlossen am 18.05.2026 (Version 1.2 vom 16.02.2026) gemäß Art. 28 DSGVO
- **Schutzmaßnahmen:** TOM-Anlage 2 zum AVV (V1.2 vom 16.02.2026), TÜV-Audit-bestätigt
- **Mehr Info:** Hetzner Datenschutz

### Cloudflare, Inc. (DNS-Nameserver + Bot-Schutz auf Formularen)

> **Wichtige Klarstellung:** Cloudflare ist **kein** Web-Traffic-Proxy für fillQR. Der eigentliche Datenverkehr (Antrags-Eingaben, Mitgliedsdaten, Mails, alle Inhalte) läuft **direkt** zwischen deinem Browser und unserem Server bei Hetzner in Falkenstein, Deutschland. Cloudflare hat zwei klar abgegrenzte Aufgaben — und nur eine davon berührt überhaupt einen US-Server:

- **Sitz:** 101 Townsend Street, San Francisco, CA 94107, USA
- **Aufgabe 1 — DNS-Nameserver (Grey-Cloud-Modus):**

- Wenn dein Browser die IP-Adresse zu `<dein-verein>.fillqr.de` nachschlagen möchte, antwortet ein Cloudflare-Nameserver mit der IP unseres Hetzner-Servers in Falkenstein, DE. Diese DNS-Antworten kommen über Cloudflares anycast-Netzwerk vom geographisch nächsten Cloudflare-Standort (meist Frankfurt). - **Es werden keine personenbezogenen Daten übermittelt.** Eine DNS-Lookup-Anfrage ist anonym (nur die Domain, keine Identität, kein Inhalt). - **Der eigentliche Web-Traffic geht NICHT durch Cloudflare.** Nach der DNS-Auflösung verbindet sich dein Browser direkt mit dem Hetzner-Server.

- **Aufgabe 2 — Cloudflare Turnstile (Bot-Schutz auf öffentlichen Formularen):**

- Beim Absenden eines öffentlichen Formulars (Mitgliedsantrag, Self-Signup, Passwort-Vergessen) prüft Turnstile im Hintergrund ob du ein Mensch oder ein Bot bist und stellt einen anonymen Token aus. - Dieser Token wird zwischen Browser und Cloudflare ausgetauscht — und nur dieser eine Token landet kurz auf US-Infrastruktur. Inhalt deines Formulars sieht Cloudflare nicht. - Keine Cookies, kein User-Tracking, keine Fingerprint-Speicherung (Cloudflare-Selbstauskunft).

- **Drittlandsübermittlung (USA):** Nur durch Aufgabe 2 (Turnstile-Token) relevant — DNS-Lookups sind technisch anonym. Absicherung durch:

- EU-US Data Privacy Framework (DPF) — Cloudflare ist aktiver Teilnehmer, Status „Active" (Stand 06/2026, verifizierbar unter dataprivacyframework.gov) - Standard Contractual Clauses (SCCs) als Backup im Cloudflare Customer DPA

- **DPA:** Cloudflare Customer DPA
- **Zertifizierungen:** SOC 2 Type II + ISO 27001/27701
- **Mehr Info:** Cloudflare Datenschutz

### Scaleway SAS (Transactional E-Mail)

- **Sitz:** 8 rue de la Ville l'Évêque, 75008 Paris, Frankreich
- **Zweck:** Versand transaktionaler E-Mails (Self-Signup-Verifikation, Passwort-Reset, Welcome-Mails, Mitglieder-Bestätigungen)
- **Daten:** Empfänger-E-Mail-Adresse, Subject, Mail-Inhalt
- **Standort:** Region fr-par (Frankreich) — keine Drittlandsübermittlung
- **DPA:** Data Processing Agreement Version 01.06.2024 (Validated im Scaleway-Account)
- **Mehr Info:** Scaleway Privacy Policy

### Variomedia AG (Mail-Empfang für fillqr.de)

- **Sitz:** Hagenauer Strasse 47, 65203 Wiesbaden, Deutschland
- **Zweck:** Mail-Empfang für Adressen unter `fillqr.de` und Tenant-Subdomains. Beispiel: wenn ein Mitglied auf eine `noreply@<dein-verein>.fillqr.de`-Mail antwortet, landet die Antwort im Postfach bei Variomedia.
- **Daten:** Empfänger-E-Mail-Adresse, Absender-E-Mail-Adresse, Subject, Mail-Inhalt der Antworten
- **Standort:** Deutschland — keine Drittlandsübermittlung
- **AVV:** Bestandteil der Variomedia-Vertragsbedingungen (DSGVO-konform, Auftragsverarbeitung nach Art. 28 DSGVO)
- **Mehr Info:** Variomedia Datenschutz

### Google LLC — Google Workspace (Mail-Empfang für info@erp-buddy.de)

- **Sitz:** 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
- **Zweck:** Mail-Postfach für die Impressum-Kontakt-Adresse `info@erp-buddy.de`. Wenn du als Vereinsmitarbeiter oder Antragsteller den Anbieter (ERP Buddy) per E-Mail kontaktierst, landet deine Mail in diesem Postfach.
- **Daten:** Absender-E-Mail-Adresse, Subject, Mail-Inhalt
- **Drittlandsübermittlung (USA):** Abgesichert durch:

- EU-US Data Privacy Framework (DPF) — Google ist aktiver Teilnehmer, Status „Active" (Stand 06/2026, verifizierbar unter dataprivacyframework.gov) - Standard Contractual Clauses (SCCs) als Backup im Google Workspace Data Processing Amendment

- **DPA:** Google Workspace Cloud Data Processing Addendum (CDPA)
- **Mehr Info:** Google Cloud Privacy Notice