kasaio.

Stand 2026 · Ausgabe 1

LEAD-MAGNET · FÜR VORSTÄNDE

DSGVO-Checkliste für deutsche Non-Profit-Organisationen.

Was dein Vorstand jetzt geprüft haben sollte — in 30 Minuten.

- 5 Sektionen
- 30 Prüfpunkte
- ca. 30 Min.
- Druckbar & abhakbar

Für Sportvereine · Kitas · soziale Träger · Förder- und Kulturvereine

kasaio.de

Erst wissen, wo du stehst.

Bevor du irgendwas reparierst, brauchst du den Überblick. Diese sechs Punkte sind das Fundament — ohne sie ist alles andere wackelig.

- [ ] **Verantwortlicher benannt?**

  Wer ist intern für Datenschutz zuständig? Name und Erreichbarkeit dokumentieren. Bei Vereinen ist das in der Regel der Vorstand (§ 26 BGB).

- [ ] **Datenschutzbeauftragte:r geprüft?**

  Pflicht nach Art. 37 DSGVO bzw. § 38 BDSG, wenn mindestens 20 Personen ständig mit automatisierter Verarbeitung beschäftigt sind — oder bei besonderen Datenkategorien (Art. 9). Auch Ehrenamtliche zählen mit.

- [ ] **Datenarten erfasst?**

  Welche personenbezogenen Daten verarbeitet ihr? Mitglieder, Eltern, Kinder, Spender, Übungsleiter, Klienten — alle Kategorien auflisten.

- [ ] **Software-Dienstleister benannt?**

  E-Mail-Anbieter, Webseite, Vereins-Software, Buchhaltung, Cloud-Speicher, Messenger — alle Dienste in einer Liste.

- [ ] **Verzeichnis von Verarbeitungstätigkeiten (VVT)?**

  Pflicht nach Art. 30 DSGVO. Ohne Ausnahme bei besonderen Datenkategorien. Muss schriftlich oder elektronisch vorliegen.

- [ ] **Auftragsverarbeitungsverträge (AVV)?**

  Mit jedem Dienstleister, der in eurem Auftrag personenbezogene Daten verarbeitet, ist ein AVV nach Art. 28 DSGVO Pflicht.

Was du vorzeigen können musst.

Wenn die Aufsichtsbehörde anklopft, muss alles parat liegen. Diese Dokumente sind nicht verhandelbar.

- [ ] **Datenschutzerklärung auf der Website?**
  Pflichtangaben nach Art. 13 DSGVO: Verantwortlicher, ggf. Datenschutzbeauftragte:r, Zwecke und Rechtsgrundlagen, Speicherdauer, Betroffenenrechte, Beschwerderecht. Verständlich formuliert — keine Copy-Paste-Textbausteine.

- [ ] **Datenschutzhinweise im Mitgliedsantrag?**
  Schon beim Beitritt informieren, wozu welche Daten verarbeitet werden. Rechtsgrundlage ist meist Art. 6 Abs. 1 lit. b (Vertragserfüllung).

- [ ] **Einwilligungen für Foto- und Videoveröffentlichungen?**
  Schriftlich, freiwillig, zweckgebunden, jederzeit widerrufbar (Art. 7 DSGVO). Bei Vereinsfesten reicht ein Hinweis am Eingang nicht aus, wenn Fotos auf Social Media landen.

- [ ] **Einwilligung bei Kindern?**
  Bei Kindern unter 16 Jahren ist die Einwilligung der Sorgeberechtigten erforderlich, soweit Art. 8 DSGVO greift. Bei sensiblen Verarbeitungen schriftlich beide Sorgeberechtigte einbinden.

- [ ] **Notfall-Plan bei Datenpannen?**
  Meldepflicht an die Aufsichtsbehörde innerhalb von 72 Stunden (Art. 33 DSGVO). Bei hohem Risiko zusätzlich Information der Betroffenen (Art. 34). Wer entscheidet wann?

- [ ] **Technisch-organisatorische Maßnahmen (TOM)?**
  Dokumentiert nach Art. 32 DSGVO: Zugangskontrolle, Passwort-Standards, Backups, Verschlüsselung, Schulung der Ehrenamtlichen.

Wo liegen eure Daten wirklich?

Seit dem Schrems-II-Urteil (2020) ist der Datentransfer in die USA keine Kleinigkeit mehr. Hier prüft ihr ehrlich.

- [ ] **Speicherorte dokumentiert?**
  Wo liegen Mitgliederdaten, Buchhaltung, E-Mail-Archive physisch? Welcher Anbieter, welcher Server-Standort, welches Rechenzentrum?

- [ ] **Datenübertragung in Drittländer geprüft?**
  USA, UK, Schweiz — alles außerhalb EU/EWR ist „Drittland" (Art. 44 ff. DSGVO). US-Anbieter sind wegen des CLOUD Act besonders kritisch: US-Behörden haben Zugriff, auch wenn Daten in der EU liegen.

- [ ] **Rechtsgrundlage für Drittland-Transfer?**
  Angemessenheitsbeschluss (EU-US Data Privacy Framework seit Juli 2023), Standardvertragsklauseln (SCC) plus zusätzliche Maßnahmen (Art. 46), oder Ausnahmen nach Art. 49.

- [ ] **Transfer-Impact-Assessment (TIA)?**
  Bei Nutzung von SCC seit Schrems II Pflicht — ihr müsst prüfen und dokumentieren, ob im Zielland ein der EU vergleichbares Schutzniveau besteht.

- [ ] **US-Tools im Einsatz inventarisiert?**
  Google Workspace, Microsoft 365, Mailchimp, Zoom, WhatsApp, Meta-Pixel — alles kritisch prüfen. Pro Tool: Rechtsgrundlage, AVV, TIA-Ergebnis.

TIPP

EU-Alternativen lassen sich für die meisten Anwendungsfälle finden — Hosting in Deutschland, kein US-Cloud-Anbieter, kein CLOUD Act. Wer das Risiko minimieren will, wechselt auf DSGVO-konforme EU-Lösungen.

Besonders schützenswerte Kategorien.

Manche Daten genießen erhöhten Schutz nach Art. 9 DSGVO — und der ist streng. Hier reichen die normalen Standards nicht.

- [ ] **Gesundheitsdaten?**

  Allergien, Medikamentengabe in der Kita, Behinderungen, Verletzungen im Sportverein. Verarbeitung nur mit ausdrücklicher Einwilligung (Art. 9 Abs. 2 lit. a) oder spezifischer Rechtsgrundlage. Höhere TOM-Anforderungen.

- [ ] **Religion oder Weltanschauung?**

  Bei kirchlichen Trägern, konfessionellen Kitas, weltanschaulichen Vereinen relevant. Art. 9 — ausdrückliche Einwilligung oder Sondertatbestand (z. B. Art. 9 Abs. 2 lit. d für religiöse Vereinigungen).

- [ ] **Strafrechtliche Daten?**

  Erweitertes Führungszeugnis bei Übungsleitern, Trainern, Erziehern: Art. 10 DSGVO. Nur unter behördlicher Aufsicht oder gesetzlicher Grundlage zulässig. Möglichst kurz aufbewahren, nicht in der Personalakte.

- [ ] **Daten von Kindern?**

  Kinder genießen erhöhten Schutz nach Erwägungsgrund 38 DSGVO. Einwilligung der Sorgeberechtigten klären, kindgerechte Informationen, Datenminimierung besonders ernst nehmen.

- [ ] **Biometrische Daten?**

  Fingerabdruck-Scanner für Anwesenheit in der Kita? Gesichtserkennung? Art. 9 — nur mit ausdrücklicher Einwilligung und sehr engen Rahmenbedingungen.

FAUSTREGEL

Für jede sensible Kategorie braucht ihr: gesonderte Einwilligung, dokumentierte Rechtsgrundlage, höhere Sicherheitsstandards und kurze Speicherfristen.

Die Rechte eurer Mitglieder.

Mitglieder, Eltern und Spender haben Rechte — und ihr müsst sie erfüllen können. Innerhalb eines Monats (Art. 12 Abs. 3 DSGVO).

- [ ] **Auskunftsrecht (Art. 15)**
  Welche Daten habt ihr von mir? Antwort in Kopie, kostenfrei, innerhalb eines Monats. Wer bearbeitet Anfragen? Wo werden sie dokumentiert?

- [ ] **Berichtigungsrecht (Art. 16)**
  Falsche Adresse, neuer Name, neue Bankverbindung: unverzüglich korrigieren.

- [ ] **Löschrecht / Recht auf Vergessen (Art. 17)**
  Wie wird gelöscht? Auch in Backups? Aufbewahrungspflichten (AO § 147, Vereinsregister, Spendenquittungen) gehen vor — dann Daten sperren statt löschen.

- [ ] **Einschränkungsrecht (Art. 18)**
  In bestimmten Fällen muss die Verarbeitung „eingefroren" werden, ohne dass gelöscht wird.

- [ ] **Datenübertragbarkeit (Art. 20)**
  Bei Verarbeitung auf Grundlage von Einwilligung oder Vertrag: Daten in einem gängigen, maschinenlesbaren Format herausgeben.

- [ ] **Widerspruchsrecht (Art. 21)**
  Insbesondere gegen Direktwerbung. Sofort umsetzen — keine weiteren Newsletter, keine Spendenaufrufe.

- [ ] **Beschwerderecht bei der Aufsichtsbehörde (Art. 77)**
  In eurer Datenschutzerklärung muss stehen, wo sich Betroffene beschweren können — die zuständige Landesdatenschutzbehörde.

Was jetzt zu tun ist.

Viele offene Kästchen? Kein Grund zur Panik — aber ein guter Anlass, in den nächsten Wochen ein paar Punkte abzuarbeiten. Empfohlene Reihenfolge:

1. **VVT anlegen oder aktualisieren.**
   Ohne Verzeichnis der Verarbeitungstätigkeiten ist alles andere wackelig.

2. **AVV mit allen Dienstleistern prüfen.**
   Fehlende Verträge sind die häufigste Beanstandung bei Audits.

3. **Datenschutzerklärung überprüfen.**
   Stimmt sie noch mit dem überein, was ihr tatsächlich tut?

4. **Drittland-Transfers prüfen.**
   Welche US-Tools sind im Einsatz, und gibt es bessere EU-Alternativen?

5. **Notfall-Plan für Datenpannen festlegen.**
   Die 72-Stunden-Frist nach Art. 33 DSGVO ernst nehmen.