Zentrum für Bewegung & Lebenskunst

Datenschutzordnung

1. Ziel, Geltungsbereich, Grundsätze

Diese Ordnung konkretisiert die Verarbeitung personenbezogener Daten im Verein und regelt Aufgaben, Verfahren und Maßnahmen zur Umsetzung der DSGVO/BDSG in Mitgliederverwaltung, Übungsbetrieb, Abrechnung/SEPA, Kommunikation (E-Mail/Newsletter) sowie Web-/Social-Media-Auftritten (sofern vom Verein verantwortet).

Die Verarbeitung folgt den Grundsätzen Rechtmäßigkeit, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität/Vertraulichkeit und der Rechenschaftspflicht (Art. 5 DSGVO).

2. Verantwortliche Stelle & Kontakt

Vorstand: Der Vorstand ist für die Einhaltung der DSGVO verantwortlich und setzt geeignete technische und organisatorische Maßnahmen (TOMs) um (Art. 24 DSGVO).

Datenschutzbeauftragte*r (DSB): Der Verein benennt eine*n DSB, sobald die gesetzlichen Voraussetzungen vorliegen –

a) nach Art. 37 DSGVO (z. B. umfangreiche Verarbeitung besonderer Kategorien), und/oder
b) nach § 38 BDSG, wenn in der Regel ≥ 20 Personen ständig automatisiert personenbezogene Daten verarbeiten (nichtöffentliche Stelle).

Vertraulichkeit: Personen, die im Verein Daten verarbeiten (z. B. Vorstands-/Team-Mitglieder, Übungsleitende), sind auf Vertraulichkeit und Zweckbindung verpflichtet (Art. 32 Abs. 4 DSGVO).

3. Zwecke & Rechtsgrundlagen

Der Verein verarbeitet personenbezogene Daten nur, soweit dies erforderlich ist:

1. Mitgliedschaft & Kursverwaltung (Begründung/Durchführung, Beitragswesen/SEPA, Kurslisten, Anwesenheiten): Art. 6 Abs. 1 b DSGVO (Vertrag).
2. Rechtliche Pflichten (Steuern, Aufbewahrung, Versicherungs-/Unfallmeldungen): Art. 6 Abs. 1 c DSGVO.
3. Berechtigte Interessen (interne Organisation, IT-Sicherheit, minimal erforderliche Kommunikation): Art. 6 Abs. 1 f DSGVO; Widerspruchsrecht nach Art. 21 DSGVO.
4. Einwilligung (z. B. Foto/Video, Newsletter, optionale Gesundheitsangaben): Art. 6 Abs. 1 a DSGVO; bei Gesundheitsdaten zusätzlich Art. 9 Abs. 2 a DSGVO (ausdrückliche Einwilligung).
5. Besondere Kategorien (Gesundheitsdaten): Verarbeitung grundsätzlich untersagt, nur bei Ausnahmen nach Art. 9 Abs. 2 DSGVO, im Vereinskontext regelmäßig Einwilligung (z. B. Selbstauskunft „trainingstauglich“).

4. Kategorien personenbezogener Daten

1. Stamm- und Kommunikationsdaten (Name, Anschrift, E-Mail, Telefon), Geburtsdatum
2. Bankdaten (SEPA-Mandat), Mitgliedsstatus, Teilnahme-/Kursdaten, Qualifikations-/Ehrenamtsdaten
3. Foto/Video (nur mit Einwilligung)
4. Gesundheitsangaben (freiwillig, nur bei ausdrücklicher Einwilligung und notwendigem Zweck, z. B. Kurs-Tauglichkeit, Allergie-Hinweis)

5. Empfänger*innen, Auftragsverarbeitung & Drittlandübermittlung

Verbände/Versicherungen/Behörden: nur soweit erforderlich (z. B. Sportversicherung, Meldungen an Fachverbände).

Auftragsverarbeiter (z. B. Vereinssoftware/Cloud/Newsletter): nur mit AV-Vertrag nach Art. 28 DSGVO; Weisungsbindung, TOMs-Nachweis.

Drittländer: Übermittlungen in Staaten außerhalb des EWR nur nach Kapitel V DSGVO (Angemessenheitsbeschluss / Standardvertragsklauseln / geeignete Garantien).

6. Veröffentlichungen, Foto-/Videoaufnahmen

Namensnennungen/Ergebnisse/Berichte auf Website/Social Media nur, wenn erforderlich und verhältnismäßig; Widerspruch nach Art. 21 DSGVO möglich.

Fotos/Videos werden nur mit Einwilligung veröffentlicht (bei Minderjährigen: Sorgeberechtigte), Widerruf jederzeit möglich; Rechtsgrundlagen: Art. 6 Abs. 1 a und ggf. Art. 9 Abs. 2 a DSGVO.

7. Informationspflichten & Transparenz

Der Verein informiert betroffene Personen zum Zeitpunkt der Datenerhebung mindestens über Verantwortliche*n, Zwecke/Rechtsgrundlagen, Empfänger-Kategorien, Speicherdauer, Rechte, Beschwerderecht und ggf. Drittlandübermittlungen (Art. 13 DSGVO). Für Daten, die nicht bei der betroffenen Person erhoben werden, gelten Art. 14 DSGVO. Diese Informationen stellt der Verein in einer separaten Datenschutzerklärung bereit.

8. Rechte der betroffenen Personen

Der Verein gewährleistet Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch sowie den Widerruf von Einwilligungen; außerdem das Beschwerderecht bei der LDI NRW (Art. 15–21 DSGVO). Beim Widerspruch gegen Direktwerbung werden Daten hierfür nicht mehr verarbeitet (Art. 21 Abs. 2–3 DSGVO)

9. Speicher- und Löschkonzept

Grundsatz: Löschen, sobald der Zweck entfällt und keine Pflichten entgegenstehen (Art. 5 Abs. 1 e DSGVO).

Steuer-/Buchführungsunterlagen (AO):

- 10 Jahre: Bücher/Abschlüsse etc. (§ 147 Abs. 3 i. V. m. Abs. 1 Nr. 1 AO)
- 8 Jahre: Buchungsbelege (§ 147 Abs. 3 S. 1 AO, seit 01.01.2025 verkürzt)
- 6 Jahre: sonstige aufbewahrungspflichtige Unterlagen (§ 147 Abs. 3 S. 1 AO)
- Fristbeginn: jeweils Jahresende (§ 147 Abs. 4 AO; Fristverlängerung, solange steuerlich relevant)

Löschfristen-Matrix (Auszug, intern zu konkretisieren im Verarbeitungsverzeichnis):

- Mitgliedsdaten: nach Austritt Löschung; Basisdaten ggf. gesperrt bis Ablauf von Ansprüchen/Fristen.
- Kurs-/Anwesenheitslisten: max. 2 Jahre (organisatorische Nachweise), sofern keine längeren Pflichten greifen.
- SEPA-Mandate/Beitragsläufe: 10/8 Jahre gemäß AO (s. oben).

10. Technische und organisatorische Maßnahmen (TOMs)

Der Verein hält ein dem Risiko angemessenes Schutzniveau aufrecht (Art. 32 DSGVO) und setzt Datenschutz durch Technikgestaltung & Voreinstellungen um (Art. 25 DSGVO). Maßnahmen umfassen u. a.:

- Zugriffsbeschränkungen & Berechtigungskonzepte, starke Passwörter/MFA, Verschlüsselung in Übertragung und – wo angemessen – im Ruhezustand;
- Backups & Wiederherstellungsfähigkeit, Protokollierung, regelmäßige Wirksamkeitsprüfungen;
- Schulungen & Vertraulichkeit für alle, die mit personenbezogenen Daten arbeiten;
- Clean-Desk/Device-Policy und sichere Entsorgung/Anonymisierung bei Löschung.

11. Verzeichnis von Verarbeitungstätigkeiten (VVT)

Der Verein führt und pflegt ein VVT (Art. 30 DSGVO) inklusive Zweck, Kategorien Betroffener/Daten, Empfänger, Drittlandübermittlungen, Löschfristen und TOMs; Vorlagen/Leitfäden der Datenschutzkonferenz (DSK) können genutzt werden.

12. Datenschutz-Folgenabschätzung (DSFA)

Bei Verarbeitungen mit voraussichtlich hohem Risiko (z. B. umfangreiche Verarbeitung besonderer Kategorien, neue Technologien) wird vorab eine DSFA durchgeführt (Art. 35 DSGVO; DSK-Kurzpapier Nr. 5 / EDSA-Leitlinien).

13. Umgang mit Datenschutzvorfällen (Datenpannen)

Datenschutzvorfälle sind unverzüglich an den Vorstand zu melden. Der Verein prüft die Meldepflicht an die Aufsichtsbehörde binnen 72 Stunden (Art. 33 DSGVO) und ggf. die Benachrichtigung betroffener Personen (Art. 34 DSGVO); die Vorfälle werden dokumentiert. Es gelten die Leitlinien des EDSA.

14. Auftragsverarbeitung & gemeinsame Verantwortlichkeit

Bei Dienstleistern mit Zugang zu personenbezogenen Daten schließt der Verein AV-Verträge (Art. 28 DSGVO).

Soweit Zwecke/Mittel gemeinsam festgelegt werden (selten; z. B. Kampagnen mit Partner*innen), wird eine Vereinbarung gemeinsamer Verantwortlichkeit geschlossen (Art. 26 DSGVO / § 63 BDSG-Hinweis).

15. Kinder & Jugendliche

Bei Minderjährigen sind Einwilligungen der Sorgeberechtigten einzuholen, sofern Einwilligung Rechtsgrundlage ist (z. B. Foto/Video; optionale Gesundheitsangaben). Datensparsamkeit und besondere Schutzbedarfe werden beachtet (Art. 5, Art. 6, Art. 9 DSGVO).

16. Dokumentation & Rechenschaft

Der Verein dokumentiert Einwilligungen, Verträge, TOMs, VVT, DSFA (falls erforderlich) und Vorfall-Dokumentationen, um die Einhaltung der DSGVO nachzuweisen (Art. 5 Abs. 2, Art. 24 DSGVO).

17. Inkrafttreten

Diese Ordnung wurde vom Vorstand 28.02.2026 beschlossen und am 28.02.2026 veröffentlicht. Sie tritt am Tag nach der Veröffentlichung auf der Vereins-Homepage in Kraft (§ 22 Abs. 2 Satzung).