VORSTANDSBESCHLUSS

zur Einführung des Safeguarding-/Schutzkonzepts
und Beschwerdeverfahrens
des Vereins The LGBT life e.V.

Datum: 07.01.2026
Ort: Berlin

§1 Grundlage

Die/der Vorstand des Vereins The LGBT life e.V. besteht gemäß Satzung aus einer Person und ist gemäß § 26 BGB alleinvertretungsberechtigt.
Zur Wahrung der Sicherheit, Antidiskriminierung und Vertraulichkeit in allen Vereinsformaten wird folgende Entscheidung getroffen:

§2 Beschluss

Hiermit beschließt der Vorstand:

1. Das Safeguarding-/Schutzkonzept & Beschwerdeverfahren (Stand: 07.01.2026) wird eingeführt.
2. Das Schutzkonzept tritt mit sofortiger Wirkung in Kraft.
3. Es gilt für alle im Auftrag oder unter Verantwortung des Vereins handelnden Personen sowie für alle Angebote (analog und digital).
4. Der Vorstand kann das Schutzkonzept jederzeit ändern, anpassen oder außer Kraft setzen.

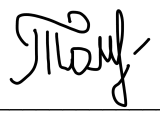
§3 Umsetzung

1. Der/die Vorstandsvorsitzende macht das Schutzkonzept allen beteiligten Personen zugänglich.
2. Zuständigkeiten, Onboarding, Schulungen sowie die Beschwerde- und Incident-Wege (inkl. anonymer Meldung) werden verbindlich umgesetzt.
3. Ergänzende interne Regelungen (z. B. Kontaktwege, Checklisten, Formulare) können zur Konkretisierung erlassen werden.

§4 Archivierung

Dieser Vorstandsbeschluss wird im Vereinsarchiv abgelegt und kann auf Anfrage Dritten (z. B. Fördermittelgeber*innen, Wirtschaftsprüfer*innen, Kooperationspartner*innen) vorgelegt werden.

The LGBT life e.V.
Ein-Personen-Vorstand gemäß § 26 BGB



_____

Fatal Flash
Vorstandsvorsitzende

SCHUTZKONZEPT

Safeguarding / Schutzkonzept & Beschwerdeverfahren
für Angebote, Veranstaltungen und interne Zusammenarbeit im Verein
The LGBT life e.V.

VORSTANDSBESCHLUSS vom 07.01.2026
Stand: 2026

§1 Zweck und Leitprinzipien

Dieses Schutzkonzept dient der Prävention und dem konsequenten Umgang mit Grenzverletzungen, Diskriminierung, Belästigung, Gewalt, Bedrohungslagen sowie Datenschutz- und Vertraulichkeitsvorfällen. Leitprinzipien sind Menschenwürde, Antidiskriminierung, Trauma-Sensibilität, Selbstbestimmung, Vertraulichkeit, Schadensminimierung, Transparenz im Verfahren und Null-Toleranz gegenüber Gewalt.

§2 Geltungsbereich und Begriffsbestimmungen

1. Dieses Schutzkonzept gilt für alle Vereinsräume, Veranstaltungen, Beratungen, Workshops, Reisen/Exkursionen, Kooperationen sowie für digitale Angebote und Kommunikationskanäle (E-Mail, Messenger, Social Media), soweit Vereinsbezug besteht.
2. Es gilt für alle Personen, die im Auftrag oder unter Verantwortung des Vereins handeln (Vorstand, Mitarbeitende, Ehrenamtliche/Freiwillige, Honorarkräfte, Praktikant*innen, Dienstleister*innen, Kooperationspartner*innen im Einsatzkontext).
3. Begriffe: Grenzverletzung (unangemessenes Verhalten), Übergriff/Gewalt (körperlich, psychisch, sexualisiert), Diskriminierung/Belästigung, Stalking (Nachstellen/Belästigen), Leak (unbefugte Offenlegung sensibler Informationen), Incident (sicherheitsrelevantes Ereignis).

§3 Rollen, Zuständigkeiten und Erreichbarkeit

1. Safeguarding Focal Point (Schutzbeauftragte*r): nimmt Meldungen entgegen, koordiniert Erstmaßnahmen, dokumentiert und steuert die Fallbearbeitung.
2. Beschwerde-Ansprechpersonen: mindestens zwei benannte Personen (inkl. Stellvertretung). Bei Interessenkonflikten wird eine alternative Person zugewiesen.
3. Datenschutz-Ansprechperson (DSGVO): wird bei Datenpannen/Leaks zwingend eingebunden.
4. Kontaktwege (intern verbindlich zu befüllen): Safeguarding: [E-Mail/Telefon]; Beschwerdestelle: [E-Mail/Telefon]; anonymer Kanal: [Link/Briefkasten/Postadresse]; Notfall: 110/112.

§4 Regeln für Personal und Ehrenamtliche (Verhaltenskodex)

Die folgenden Regeln sind verbindlich und gelten in allen Vereinsformaten:

- Respekt und Antidiskriminierung: keine diskriminierenden Aussagen/Handlungen; konsequente Achtung von Namen/Pronomen; kein Deadnaming.
- Grenzen und Machtgefälle: keine Ausnutzung von Abhängigkeiten (z. B. Zugang zu Ressourcen, Wohnraum, Behördenbegleitung).
- Nähe und Intimität: keine romantischen/sexuellen Annäherungen in Betreuungs- oder Abhängigkeitskontexten; im Zweifel strikte Distanz.
- Körperkontakt nur mit eindeutiger Zustimmung und situativer Angemessenheit; bei Unsicherheit kein Körperkontakt.
- Vertraulichkeit/Outing-Schutz: keine Weitergabe von Identitäten, Aufenthaltsstatus, Fluchtgründen, Standorten, Fotos/Videos ohne ausdrückliche Einwilligung und Rechtsgrundlage.
- Kommunikation: professionelle Kanäle bevorzugen; keine privaten Chatgruppen für sensible Daten; respektvolle Sprache ohne Einschüchterung oder sexualisierte Kommentare.
- Geld und Geschenke: keine Annahme/Weitergabe von Geld oder wertvollen Geschenken in Schutz-/Betreuungskontexten; Ausnahmen nur nach Freigabe durch den Vorstand.
- Substanzen und Sicherheit: kein Alkohol-/Drogenkonsum bei Einsätzen; keine Waffen.
- Meldepflicht: beobachtete oder vermutete schwerwiegende Vorfälle sind unverzüglich zu melden.

§5 Prävention, Onboarding und Schulung

1. Vor Einsatz erhalten alle verpflichteten Personen ein Onboarding zu Grenzen/Macht, Trauma-Sensibilität, Antidiskriminierung, Datenschutz und Meldewegen.
2. Je nach Einsatzfeld kann der Verein zusätzliche Nachweise und Schutzmaßnahmen verlangen (z. B. Referenzen, Selbstauskunft, bei Tätigkeiten mit Minderjährigen ggf. erweitertes Führungszeugnis, sofern rechtlich geboten).
3. Mindestens jährlich erfolgt ein Review der Standards und ein kurzes Refresh-Update für relevante Rollen.

§6 Incident- und Notfallverfahren (Drohungen, Stalking, Leaks)

Grundsatz: Sicherheit hat Vorrang. Betroffene entscheiden, welche Unterstützung sie wünschen, soweit keine akute Gefahr vorliegt.

1. Akute Gefahr: sofort 110/112; sichere Umgebung herstellen; Betroffene nicht allein lassen (wenn gewünscht); Täter*in/Bedrohung auf Distanz; Veranstaltungsleitung informieren.
2. Meldung: Incident unverzüglich an Safeguarding/Beschwerdestelle melden; anonyme Meldung möglich (siehe §7).
3. Dokumentation: Datum/Uhrzeit, Ort, Beschreibung, Beteiligte, Beweise (Screenshots/Logs), Sofortmaßnahmen; keine Spekulationen.
4. Sofortmaßnahmen je nach Lage: Trennung der Parteien, Hausverbot/Contact-Ban, Freistellung vom Einsatz, Zugangssperren, Passwortwechsel, Sicherung betroffener Systeme/Daten.

Spezifische Prozeduren:

- Drohungen/Gewaltandrohung: Risiko einschätzen (Konkretisierung, Zugang, Wiederholung); bei konkreter Gefahr Polizei; Schutzplanung (Wege, Kontaktlisten, Event-Security).
- Stalking (online/offline): Beweise sichern; Kontaktabbruchs-Strategie; Privatsphäre- und Sicherheitseinstellungen; interne Kontaktverbote/Hausverbot; Begleitmaßnahmen für sichere Teilnahme.

- Leaks/Datenschutzpannen: Zugriff stoppen; Systeme isolieren; Passwörter/Keys rotieren; Umfang ermitteln; Datenschutz-Ansprechperson einbinden; DSGVO-Prüfung inkl. ggf. Meldung binnen 72 Stunden und Information der Betroffenen bei hohem Risiko.
- Diskriminierung/Belästigung/Übergriffe: betroffenenorientierte Stabilisierung; Schutz vor Retraumatisierung; keine Repressalien; risikobasierte Maßnahmen bis zur Klärung (z. B. Freistellung, Ausschluss aus Formaten).

§7 Beschwerdeverfahren (inkl. anonymer Kanal)

1. Ziele: niedrigschwellige Meldung, Schutz vor Repressalien, klare Bearbeitung, transparente Rückmeldungen im rechtlich möglichen Rahmen.
2. Kanäle (nicht anonym): [E-Mail/Telefon Beschwerdestelle]; persönliches Gespräch nach Termin; Begleitperson ist zulässig.
3. Anonymer Kanal: [Link zu anonymem Online-Formular ohne Login / Briefkasten 'Beschwerdestelle - vertraulich' / Postadresse]. Bei anonymer Meldung wird ein Rückkanal empfohlen (z. B. anonyme E-Mail), um Rückfragen zu ermöglichen.
4. Bearbeitung (Richtwerte): Eingangsbestätigung binnen 7 Tagen (sofern Rückkanal vorhanden); Erstbewertung binnen 7 Tagen; Abschluss i. d. R. binnen 14-30 Tagen mit Zwischenständen bei komplexen Fällen.
5. Interessenkonflikte: betrifft die Beschwerde eine Ansprechperson oder den Vorstand unmittelbar, wird eine alternative interne oder externe Vertrauensperson benannt.

§8 Dokumentation, Vertraulichkeit und Datenschutz

1. Alle Meldungen werden vertraulich behandelt; Zugriff nur für zuständige Rollen nach dem Need-to-know-Prinzip.
2. Dokumentation erfolgt minimalinvasiv, zweckgebunden und sicher gespeichert; Aufbewahrungs- und Löschfristen werden intern festgelegt (DSGVO-konform).
3. Repressalienverbot: Benachteiligung von Betroffenen oder Hinweisgeber*innen ist untersagt und selbst ein meldepflichtiger Vorfall.

§9 Konsequenzen und Sanktionen

Maßnahmen erfolgen verhältnismäßig und risikobasiert. Mögliche Konsequenzen sind insbesondere:

- Gespräch, Auflagen, verpflichtende Schulung, Supervision
- Entzug von Aufgaben/Zugängen, Rollenwechsel, Freistellung vom Einsatz
- Abmahnung, Beendigung der Zusammenarbeit, Hausverbot/Ausschluss
- Anzeige oder zivilrechtliche Schritte, wenn erforderlich

§10 Kommunikation, Sichtbarkeit und Event-Safety

1. Bei Veranstaltungen werden Meldewege, Notfallkontakte sowie Foto-/Video- und Outing-Regeln sichtbar gemacht (Aushang/Slide/Moderationshinweis).
2. Bei erhöhtem Risiko wird ein kurzes Safety-Briefing zu Beginn durchgeführt und es werden Rückzugs- und Supportstrukturen benannt.
3. Medien- und Fotoaufnahmen erfolgen nur nach Einwilligung; Schutz vulnerabler Personen hat Vorrang.

1.
   § **11 Monitoring, Review und Inkrafttreten**

   1. Der Vorstand überprüft das Schutzkonzept mindestens jährlich und nach schwerwiegenden Vorfällen (anonymisierte Lessons Learned).

2. Dieses Schutzkonzept tritt mit Vorstandsbeschluss vom 07.01.2026 in Kraft. Änderungen werden in geeigneter Form bekanntgegeben; die jeweils gültige Version ist intern abrufbar.