

Richtlinie Videoüberwachung

Stand: 26.02.2026 / DSC

Diese Richtlinie regelt den Umgang mit der Videoüberwachung und den daraus entstehenden Aufnahmen im Tennisclub Teufenthal. Sie dient der rechtskonformen, datenschutzfreundlichen Nutzung gemäss Schweizer Datenschutzgesetz (DSG), dem Persönlichkeitsschutz (insb. Art. 28 ZGB) sowie den Empfehlungen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).

1. Zweck und Grundsätze

Die Videoüberwachung wird ausschliesslich eingesetzt für:

- Diebstahlschutz
- Schutz vor Einbruch
- Abklärung von Sicherheitsvorfällen (z.B. Sachbeschädigung, Gewalt, Unfall)

Eine Nutzung zur Verhaltens- oder Leistungskontrolle von Mitgliedern, Gästen oder Mitarbeitenden ist ausgeschlossen. Es gilt: so wenig wie möglich filmen, so kurz wie möglich speichern, so klar wie möglich informieren.

2. Überwachte Bereiche und Betrieb

Kamerapositionen:

- Haupteingang
- Clubraum
- Bar
- Wintergarten

Betrieb: 24/7 Aufzeichnung.

Der Aufnahmebereich ist auf vereinseigene Bereiche beschränkt. Besonders schützenswerte Bereiche (z.B. Toiletten, Garderoben) werden nicht überwacht.

3. Information und Kennzeichnung

Vor Betreten der überwachten Bereiche werden gut sichtbare Hinweisschilder angebracht. Eine kurze Datenschutzinfo wird zusätzlich via Aushang und QR-Code bereitgestellt.

4. Rollen, Zugriff und Protokollierung

Zugriff auf Livebild und Aufnahmen haben grundsätzlich nur:

- Präsident
- Vizepräsident

Zugriffe erfolgen nur bei Bedarf (konkreter Vorfall/Verdacht) und nicht aus Neugier.

Passwörter werden nicht geteilt. Wenn möglich werden persönliche Benutzerkonten genutzt und Mehrfaktor-Authentisierung (MFA) aktiviert.

5. Speicherung, Aufbewahrung und Löschung

Speicherort: Schweizer Cloud

Reguläre Speicherdauer: maximal 21 Tage (automatische Überschreibung/Löschung).

Vorfalldateien: Relevante Sequenzen dürfen separat gesichert werden, soweit dies für Abklärung/Anzeige/Versicherung erforderlich ist. Nach Abschluss werden die Sequenzen gelöscht.

6. Weitergabe an Dritte und Verbot der Veröffentlichung

Aufnahmen werden grundsätzlich nicht an Dritte weitergegeben und niemals veröffentlicht (insbesondere nicht via Messenger/Soziale Medien).

Eine Weitergabe ist nur zulässig, wenn sie erforderlich ist, z.B.:

- an Polizei/Strafverfolgungsbehörden bei Verdacht auf Straftat
- an Versicherungen im Schadenfall
- an Rechtsvertretung/Behörden im konkreten Verfahren

Es wird jeweils nur der notwendige Ausschnitt und nur über einen sicheren Übertragungsweg übermittelt.

7. Datensicherheit (technische und organisatorische Massnahmen)

Mindestens folgende Massnahmen sind umzusetzen:

- Starke Passwörter, MFA wenn verfügbar, regelmässiger Passwortwechsel bei Bedarf (z.B. Rollenwechsel)
- Aktuelle Firmware/Software (Patches), gesicherte Admin-Geräte
- Zugriffsrechte nach dem Need-to-know-Prinzip (nur Präsident/Vizepräsident)
- Verschlüsselte Übertragung und Speicherung, soweit vom System unterstützt
- Sicherer Export (verschlüsselte Datei, geschützter Speicherort), klare Löschroutine

Für die Cloud-Nutzung besteht ein Vertrag zur Auftragsbearbeitung (inkl. Weisungsbindung, Datensicherheit, Unterauftragsbearbeiter, Support bei Auskunft/Löschung, Meldeprozesse bei Sicherheitsvorfällen).

8. Betroffenenrechte und Anlaufstelle

Betroffene Personen können Auskunft verlangen, ob und welche Aufnahmen sie betreffen. Bei Herausgabe werden Rechte Dritter geschützt (z.B. Verpixelung/Standbilder, wo sinnvoll). Anfragen sind an den oben genannten Kontakt zu richten.

9. Prüfung und Revision

Der Vorstand überprüft mindestens jährlich, ob Kamerastandorte, Betrieb (24/7), Speicherdauer und Zugriffsregeln weiterhin erforderlich und verhältnismässig sind. Änderungen werden dokumentiert.

Anhang A – Datenschutzinfo für Aushang

Aushang im Clubhaus

1. Verantwortlicher: Tennisclub Teufenthal, Schmittengasse, 5723 Teufenthal. Kontakt: daniel@tcteufenthal.ch.
2. Zweck: Diebstahlschutz, Einbruchschutz, Sicherheitsabklärung; keine Verhaltens- oder Leistungskontrolle.
3. Orte: Haupteingang, Clubraum, Bar, Wintergarten; keine Sanitärbereiche.
4. Betrieb: 24/7 Aufzeichnung; Einsichtnahme nur bei konkretem Ereignis/Verdacht.
5. Zugriff: Ausschliesslich Präsident und Vizepräsident; Exports werden protokolliert.
6. Speicherdauer: max. 21 Tage (automatische Überschreibung)
7. Empfänger: grundsätzlich keine; bei Vorfällen ggf. Polizei/Behörden/Versicherung; keine Veröffentlichung.
8. Cloud: Speicherung bei Schweizer Provider; vertraglich geregelt (Datensicherheit, Unteraufträge, Support).
9. Datensicherheit: Zugriffsschutz (Passwort/MFA), Updates, Berechtigungen.
10. Rechte: Auskunft und weitere Betroffenenrechte nach DSGVO; Anfragen z.H. obigen Kontakt.