

Rollenkonzept und Registrierung

- [Rollenkonzept](#)
- [Registrierung](#)

Rollenkonzept

Das Rollenkonzept der digitalen Personalakte basiert auf dem strengen Minimalprinzip ("Need-to-Know"). Jeder Benutzer sieht nur exakt die Informationen und Personalakten, für die er aufgrund seiner Funktion autorisiert ist. Das System stellt im Hintergrund technisch sicher, dass Zugriffe auf fremde Ortswehren oder nicht zuständige Abteilungen völlig unmöglich sind – selbst dann, wenn jemand versucht, die Adresse (URL) im Browser manuell zu manipulieren.

Das System unterscheidet grob zwischen folgenden Hierarchie- und Funktionsebenen:

1. Ortswehrführer & Stellvertreter Die Ortswehrführung hat vollen Zugriff auf die Mitglieder der *aktiven Einsatzabteilung* sowie der *Alters- und Ehrenabteilung* ihrer zugewiesenen Ortswehr. In der Regel ist einer Führungskraft genau eine Wehr zugewiesen; das System ist jedoch flexibel genug, um bei Bedarf auch die Betreuung mehrerer Ortswehren gleichzeitig zu ermöglichen.

2. Fachwarte auf Ortsebene (Jugendwart & Kidswart) Der Zugriff für Fachwarte ist aus Gründen des Datenschutzes strikt auf ihre jeweiligen Schutzbefohlenen limitiert.

- Ein **Jugendwart** sieht ausschließlich die Jugendfeuerwehr seiner zugewiesenen Wehr(en).
- Ein **Kidswart** sieht dementsprechend ausschließlich die Kidsfeuerwehr.

Die Akten der aktiven Einsatzabteilung oder der Ehrenabteilung bleiben für diese Rollen unsichtbar.

3. Die Amtsebene (Amtsbrandmeister & Amtsfachwarte)

- **Amtsbrandmeister:** Haben einen uneingeschränkten, ressortübergreifenden Zugriff auf *alle* Ortswehren und *alle* Abteilungen innerhalb des gesamten Amtes.
- **Amtsjugendwarte & Amtskidswarte:** Sehen alle Mitglieder ihrer jeweiligen Zielgruppe (Jugend- bzw. Kidsfeuerwehr) – dies jedoch amtsweit über *alle* Ortswehren hinweg.

4. Systemadministrator (IT) Diese Rolle kümmert sich um die technische Verwaltung der Plattform. Administratoren legen Benutzerkonten an, verwalten Systemkonfigurationen (z. B. Katalogwerte) und vergeben die Berechtigungen an die Führungskräfte.

Besonderheit: Der Abteilungswechsel (Überführung) Ein zentrales Merkmal dieses Rechtekonzepts zeigt sich beim Wechsel eines Mitglieds in eine andere Altersgruppe. Fachwarte sowie die Amtsführung haben die Möglichkeit, Mitglieder direkt in die nächsthöhere Abteilung zu überführen (z. B. beim Übertritt aus der Kidswehr in die Jugendwehr).

Wichtiger Datenschutz-Aspekt: Sobald ein Kidswart ein Kind in die Jugendfeuerwehr überführt, verliert er augenblicklich den Zugriff auf diese Akte. Das Mitglied verschwindet aus seinem Sichtfeld und taucht vollautomatisch im System des zuständigen Jugendwarts auf. (Weitere Details zu diesem Prozess finden Sie im Kapitel "Akten- und Dashboardmanagement").

Registrierung

Für die Nutzung der digitalen Personalakte ist keine klassische Registrierung durch den Benutzer erforderlich. Stattdessen erfolgt eine gezielte Freischaltung Ihres bereits bestehenden Benutzerkontos.

Der Ablauf der Freischaltung:

1. **Beantragung:** Bitte beantragen Sie den Zugang zunächst bei der Amtswehrführung (Amtsbrandmeister). Geben Sie dabei an, welche Rollen und Berechtigungen Sie für Ihre Funktion benötigen (siehe hierzu Kapitel 1.4 *Das Rechtekonzept*).
2. **Einrichtung:** Nach der inhaltlichen Freigabe durch die Amtswehrführung erfolgt die technische Freischaltung ausschließlich durch die IT-Abteilung.

Anmeldung über bestehende Zugangsdaten (Single Sign-On) Sie müssen sich keine neuen Passwörter merken! Ein separater Zugang ist nicht erforderlich. Die Anmeldung erfolgt ganz bequem über die Ihnen bereits bekannten Zugangsdaten Ihrer E-Mail-Verwaltung – exakt so, wie Sie es bereits vom Login der Unterspreewald-Cloud gewohnt sind.

“ **⚠ WICHTIGE SICHERHEITSINFORMATION: Zwingende Zwei-Faktor-Authentifizierung (2FA)** Da in der Personalverwaltung hochsensible, personenbezogene Daten verarbeitet werden, greifen hier verschärfte Sicherheitsrichtlinien zum Datenschutz.

Sobald Ihr Konto durch die IT für die Personalakte freigeschaltet wurde, wird für Ihren gesamten Account serverseitig ein strikter **2FA-Zwang** hinterlegt. Das bedeutet: Bei Ihrer nächsten Anmeldung *müssen* Sie zwingend eine Zwei-Faktor-Methode (z. B. eine Authenticator-App auf dem Smartphone) einrichten.

Erfolgt dies nicht, ist aus Sicherheitsgründen **keine Anmeldung mehr möglich**. Wie Sie die 2FA genau einrichten, erfahren Sie Schritt für Schritt im Handbuch *"E-Mail Verwaltung der Feuerwehrmailadressen"*.