medsolv.MRM

HANDOUT BENUTZERANLAGE

VERSION: 8/2026

Intention

Im Folgenden eine Anleitung zur Benutzeranlage.

Hinweis: In diesem Handout wurde auf die Verwendung einer geschlechtsneutralen Sprache, der besseren Lesbarkeit wegen, verzichtet.

Inhalt

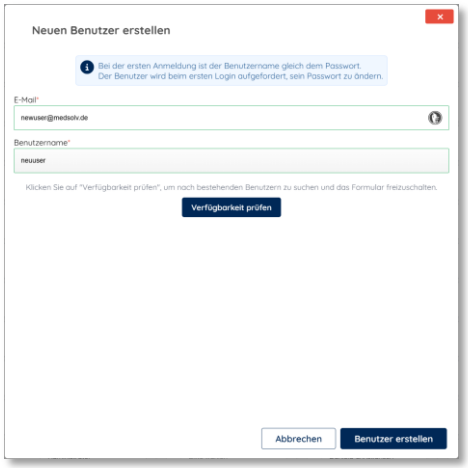
Benutzer erstellen

`Hauptmenü -> Administration -> Benutzer`

Benutzer erstellen ist ´den Rollen ADMINISTRATION und SUPER USER vorbehalten.

Zum Erstellen eines neuen Benutzers sind folgende Eingaben vorzunehmen

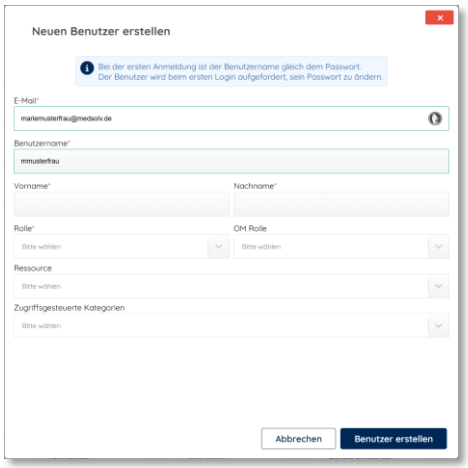
- E-Mail
- Benutzername



Weiter mit ***Verfügbarkeit prüfen***

a) Benutzer neu

- Vorname*
- Nachname*
- Rolle*
- OM Rolle
  notwendig für Kunden mit OrderManagement, ohne Auswirkung für andere.

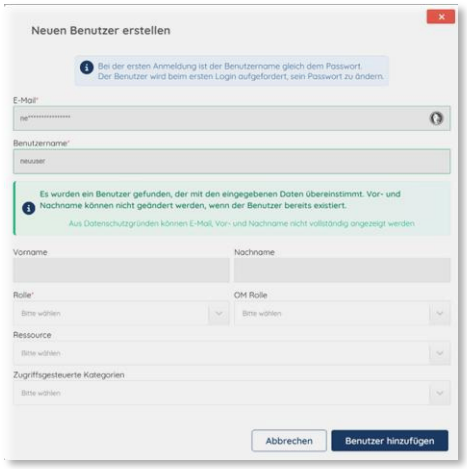


  - Ressource
    Zuordnung eines Mitarbeiters / einer Mitarbeiterin, sofern diese im MRM als Ressource angelegt ist.
  - Zugriffsgesteuerte Kategorien

Bei der ersten Anmeldung ist der Benutzername gleich dem Passwort.
Der Benutzer wird beim ersten Login aufgefordert, sein Passwort zu ändern.

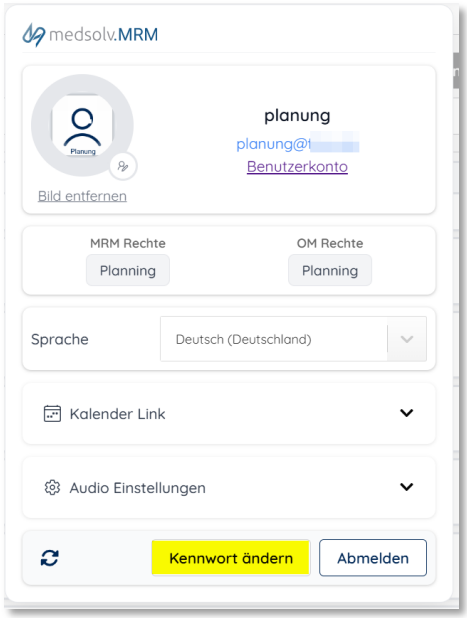
b) Benutzer ist bereits vorhanden

Wenn der Benutzer bereits vorhanden, aber nicht dem Mandanten zugeordnet ist, kann der Benutzer nach Zuordnung der Rollen hinzugefügt werden.



Kennwort ändern

Der Benutzer kann jederzeit sin Kennwort im Benutzerprofil ändern.



E-Mail als Pflichtfeld

E-Mail als Pflichtfeld

Um die rechtlichen Anforderungen an eine lückenlose Personenbindung von Zugängen zu erfüllen, ist die Angabe einer individuellen E-Mail-Adresse als Pflichtfeld vorgeschrieben. Nur so lässt sich der Betrieb gemeinsamer Benutzerkonten vermeiden – ein Verstoß gegen DSGVO, § 75c SGB V und

TI-Vorgaben im deutschen Gesundheitswesen. Jede Person erhält somit ein eigenes Konto mit persönlicher Authentifizierung.

Hier LLM-Antwort[1] für Deutschland

Rechtlicher Hintergrund: Verbot von Shared Accounts im deutschen Gesundheitswesen

Das Verbot von geteilten Benutzerkonten (Shared Accounts) im deutschen Gesundheitswesen lässt sich nicht auf ein einzelnes Gesetz zurückführen, sondern ergibt sich aus einem Zusammenspiel mehrerer Rechtsgrundlagen:

1. Datenschutz-Grundverordnung (DSGVO) und BDSG

*Die zentrale rechtliche Basis bildet **Art. 32 DSGVO**, der Krankenhäuser und andere Leistungserbringer verpflichtet, technische und organisatorische Maßnahmen (TOMs) zu treffen, um die Sicherheit personenbezogener Daten zu gewährleisten. Da Gesundheitsdaten gemäß Art. 9 DSGVO zur Kategorie der besonders sensiblen Daten gehören, gelten hier verschärfte Anforderungen.*

Shared Accounts widersprechen dabei mehreren DSGVO-Prinzipien:

- ***Nachvollziehbarkeit (Art. 5 Abs. 2 DSGVO):** Es muss jederzeit nachvollziehbar sein, wer auf welche Daten zugegriffen hat. Bei geteilten Konten ist eine klare Zuordnung von Aktivitäten zu einzelnen Personen nicht möglich.*
- ***Rechtmäßigkeit und Verantwortlichkeit:** Die Verarbeitung sensibler Gesundheitsdaten setzt eine eindeutige Identifizierbarkeit der handelnden Person voraus.*
- ***Datensparsamkeit und Datenminimierung:** Jede Person soll nur auf die Daten zugreifen können, die sie für ihre konkrete Aufgabe benötigt – was bei Shared Accounts nicht kontrollierbar ist.*

*Ein Verstoß kann zu **empfindlichen Bußgeldern** führen, die je nach Schwere bis zu 20 Mio. Euro oder 4 % des weltweiten Jahresumsatzes betragen können.*

2. § 75c SGB V – IT-Sicherheitsverpflichtung

*Seit Einführung von **§ 75c SGB V** existiert eine gesetzliche IT-Sicherheitsverpflichtung für alle Leistungserbringer im Gesundheitswesen – nicht nur für KRITIS-Krankenhäuser. Diese Norm verpflichtet zur Einhaltung von IT-Sicherheitsstandards nach dem Stand der Technik, was implizit auch individuelle Authentifizierungsmechanismen erfordert. Zuvor galt diese Pflicht nur für Einrichtungen, die unter das BSI-Gesetz (KRITIS-Verordnung) fielen – nun wurde die Lücke für kleinere Häuser geschlossen.*

3. BSI-Gesetz und KRITIS-Verordnung

*Krankenhäuser, die als **KRITIS-Betreiber** eingestuft sind, unterliegen den strengen Vorgaben des BSI-Gesetzes. Dieses fordert angemessene organisatorische Maßnahmen zur IT-Sicherheit, wozu auch die **individuelle Benutzeridentifikation** gehört. Shared Accounts stellen hier einen direkten Verstoß dar.*

4. Telematikinfrastruktur (TI) und gematik-Vorgaben

*Für Systeme innerhalb der **Telematikinfrastruktur** – wie die elektronische Patientenakte (ePA), das E-Rezept oder die elektronische Gesundheitskarte (eGK) – gelten spezifische Vorgaben der gematik. Diese schreiben **persönliche Benutzerkonten ohne Weitergabe** vor, um die Vertraulichkeit, Integrität und Verfügbarkeit von Patientendaten zu sichern. Rechtlich verankert sind diese Vorgaben u. a. im **Digitalen-Versorgung-Gesetz (DVG)**.*

5. Berufsrechtliche Pflichten

*Auch berufsrechtlich (z. B. Musterberufsordnung für Ärzte) besteht eine Pflicht zur **Dokumentations- und Sorgfaltspflicht**. Eine ordnungsgemäße Dokumentation setzt voraus, dass klar ist, welche Person welche medizinische Entscheidung getroffen oder dokumentiert hat – bei Shared Accounts ist das nicht gegeben.*

[1] Lumo 2.0 Max – 19.08.2026

Zusammenfassung

Rechtliches Verbot von Shared Accountsinfo

Das Verbot von Shared Accounts im deutschen Gesundheitswesen ergibt sich nicht aus einem Einzelgesetz, sondern aus dem Zusammenspiel von DSGVO (Art. 5, 9, 32), § 75c SGB V, BSI-Gesetz/KRITIS-VO, gematik-Vorgaben zur Telematikinfrastruktur und berufsrechtlichen Pflichten. Kernprinzip ist die durchgehende Personenbindung von Zugangsdaten.

*In der Praxis bedeutet dies: Jede Mitarbeitende benötigt ein **individuelles Benutzerkonto** mit persönlichen Zugangsdaten, damit Zugriffe auf Patientendaten lückenlos nachvollziehbar sind. Bei Verstößen drohen nicht nur Bußgelder, sondern auch haftungsrechtliche Konsequenzen bei Datenschutzverletzungen.*