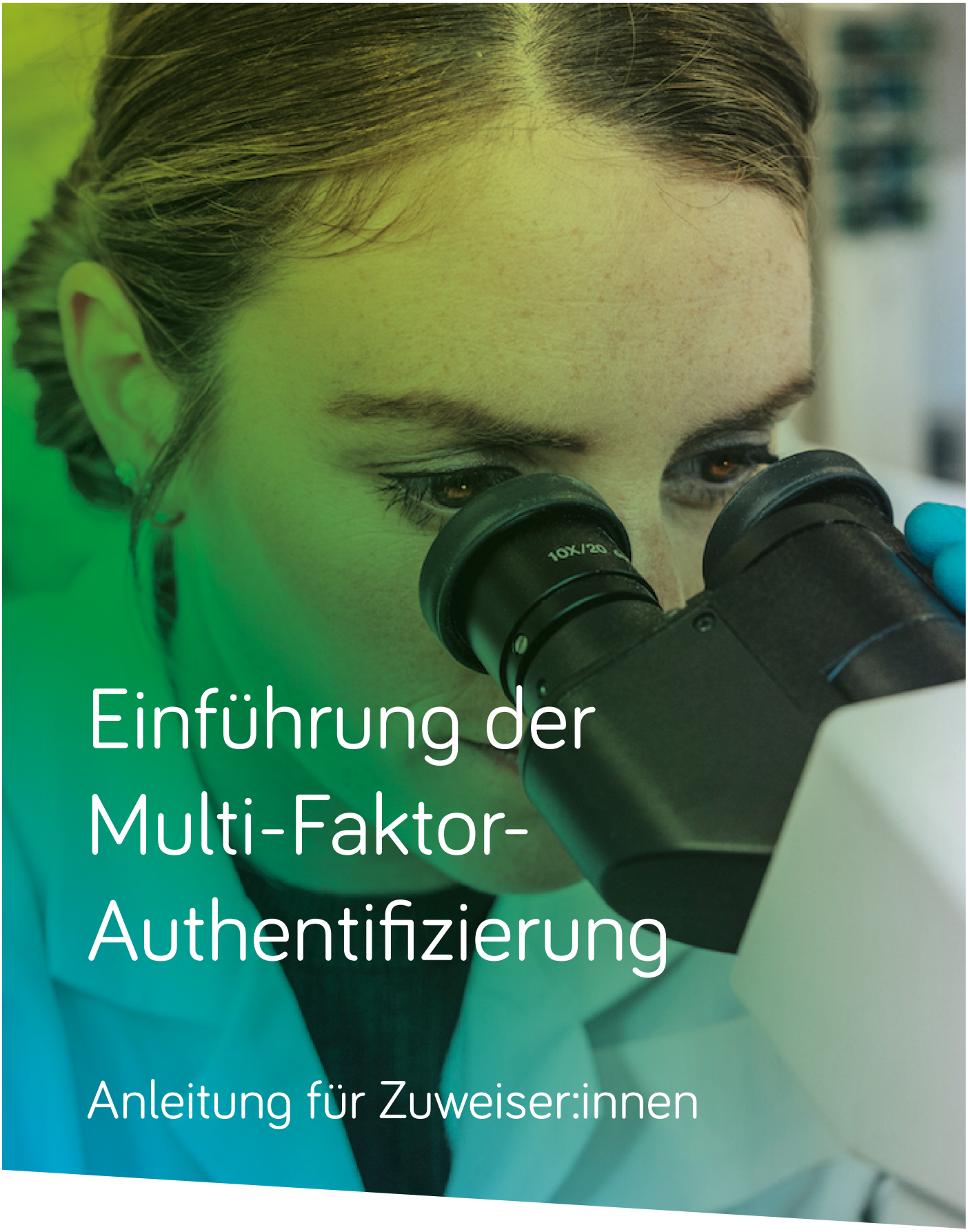


Einführung der Multi-Faktor-Authentifizierung

Anleitung für Zuweiser:innen

labors.at

Dem Menschen den richtigen Wert geben.

labors.at
Dem Menschen den richtigen Wert geben.

Inhaltsverzeichnis

labors.at
Dem Menschen den richtigen Wert geben.

Darum führt labors.at die Multi-Faktor-Authentifizierung ein

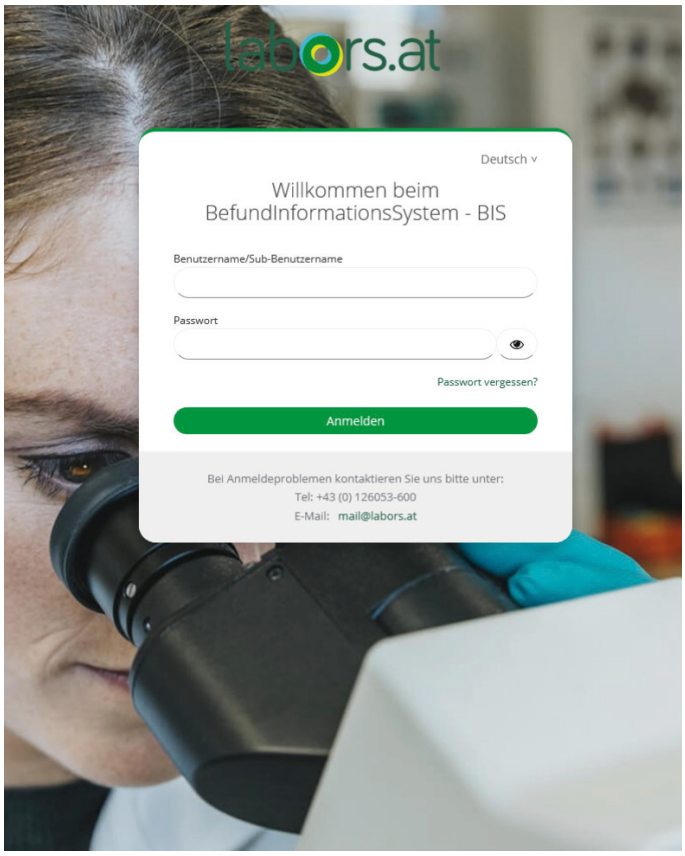
Durch die Nutzung mehrerer Sicherheitsfaktoren – wie z. B. einem Passwort in Kombination mit einem Bestätigungscode auf dem Smartphone – wird das Risiko von Datenlecks und unbefugtem Zugriff deutlich reduziert. Dies ist entscheidend in einer Zeit, in der cyberkriminelle Angriffe auf medizinische Einrichtungen zunehmen. Mit dieser zusätzlichen Sicherheitsstufe gewährleisten wir einen noch besseren Schutz Ihrer Patient:innendaten. Dank neuer technischer Möglichkeiten ist die Einführung der Multifaktor-Authentifizierung jetzt nicht nur einfacher, sondern auch nutzerfreundlicher geworden. Gleichzeitig schaffen wir damit die Grundlage für ein zukünftiges Portal, das Ihnen den Zugang zu einer Vielzahl weiterer Funktionalitäten ermöglichen wird.

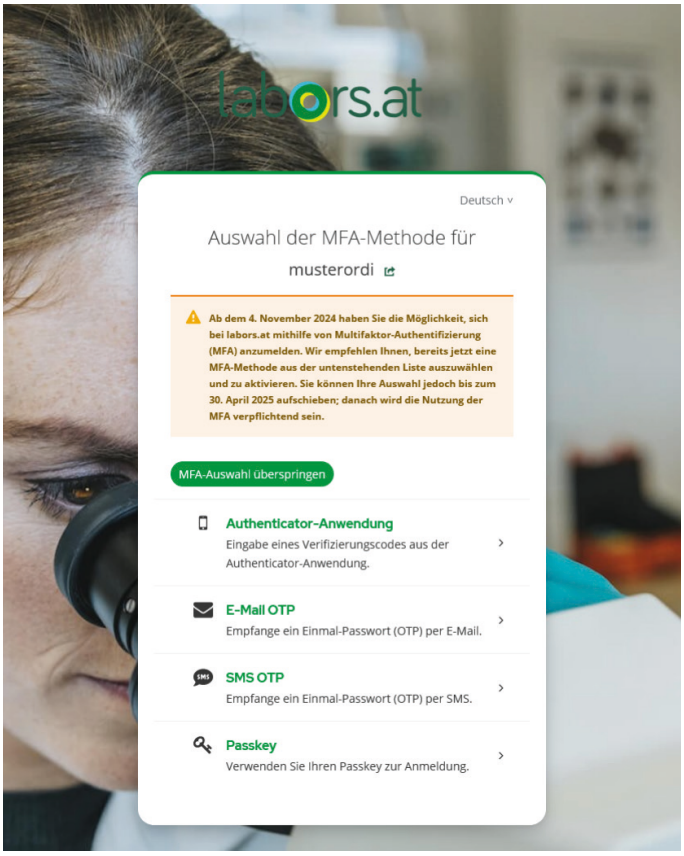
Sie können über den Link:
http://www.labors.at/befundabfrage/?user_type=referrerSubuser
oder über den QR-Code in die Benutzeroberfläche einsteigen

Start und Auswahl MFA-Methode

Wenn Sie dem Link oder QR-Code gefolgt sind, gelangen Sie auf diesem Bildschirm.

Hier geben Sie wie gewohnt Benutzernamen und Passwort ein und klicken auf „Anmelden“.





Bitte wählen Sie die MFA-Methode, mit der Sie die Authentifizierung durchführen möchten.

Es stehen die folgenden Methoden zur Auswahl:

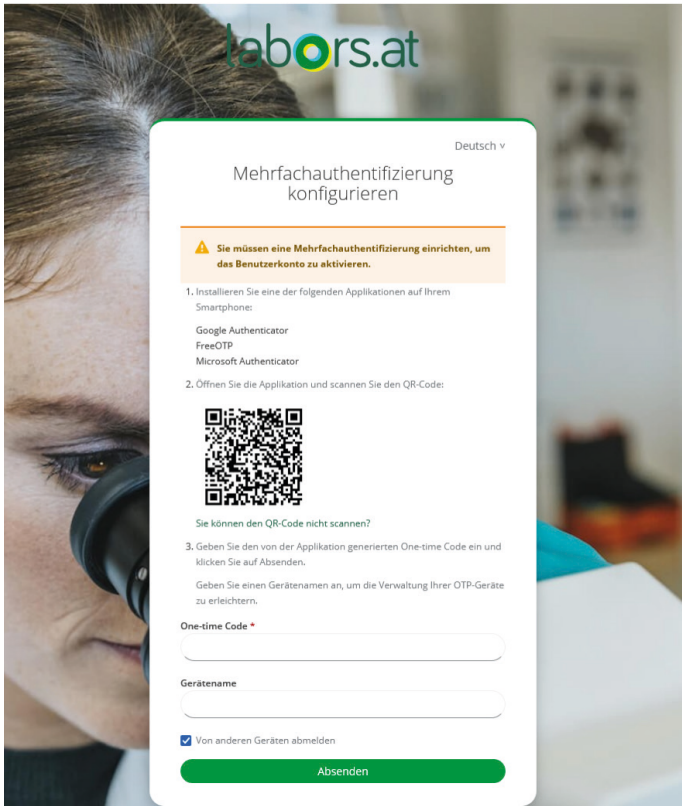
- Authenticator-Anwendung S.5
- E-Mail Einmalpasswort (OTP) S.6
- SMS Einmalpasswort (OTP) S.7
- Passkey S.8-11

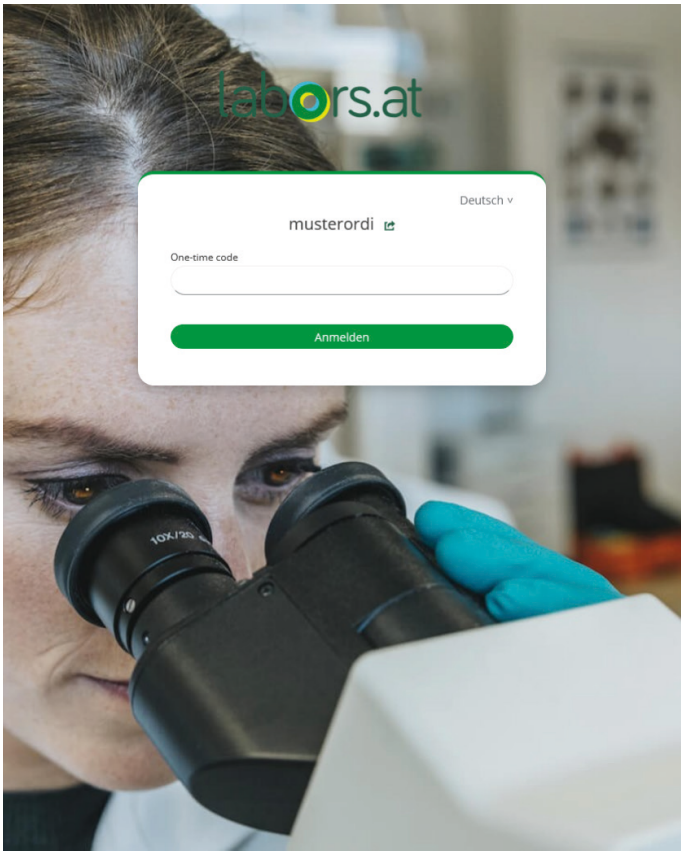
Authenticator-Anwendung

Wenn Sie die Authenticator-Anwendung wählen, kommen Sie zu diesem Bildschirm.

Authenticator-Anwendungen gibt es für Mobiltelefone und PC/Mac.

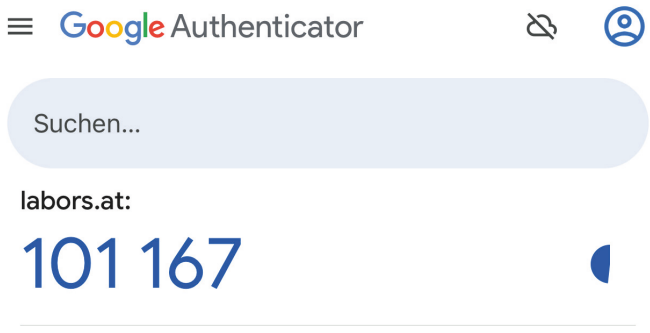
Sie haben die Auswahl zwischen verschiedenen Anbietern.





In der Authenticator-Anwendung wird ein temporär gültiger Code erzeugt, den Sie als zweiten Faktor bei der Anmeldung bei labors.at eingeben können.

Hier sehen Sie den Google Authentificator als Beispiel

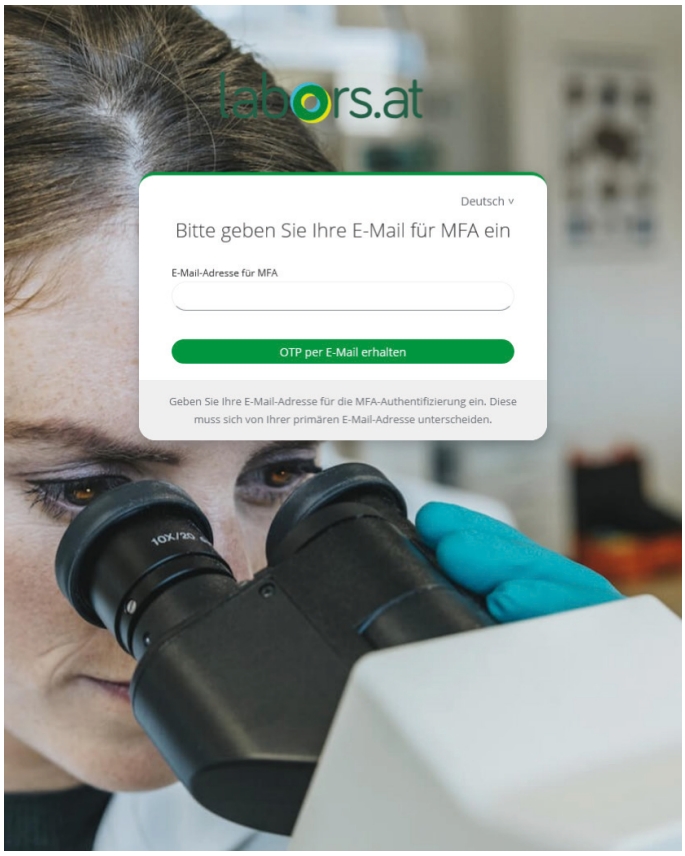


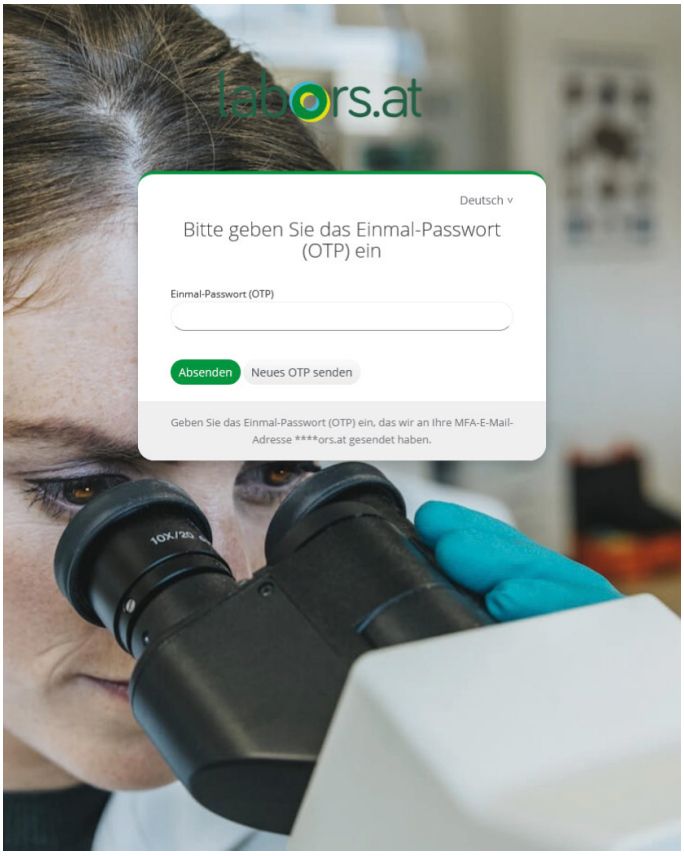
Dies ist ein ausgedachter Code.

E-Mail OTP

Bei der Nutzung von E-Mail OTP wird ein Einmal-Passwort generiert, welches per E-Mail zugestellt wird. Diese Passwort wird als zweiter Faktor bei der Anmeldung bei labors.at verwendet. Nach der Anmeldung verliert das Passwort seine Gültigkeit und kann für den nächsten Anmeldevorgang nicht mehr verwendet werden. Fordern Sie im Bedarfsfall ganz einfach ein weiteres Einmal-Passwort (OTP) an.

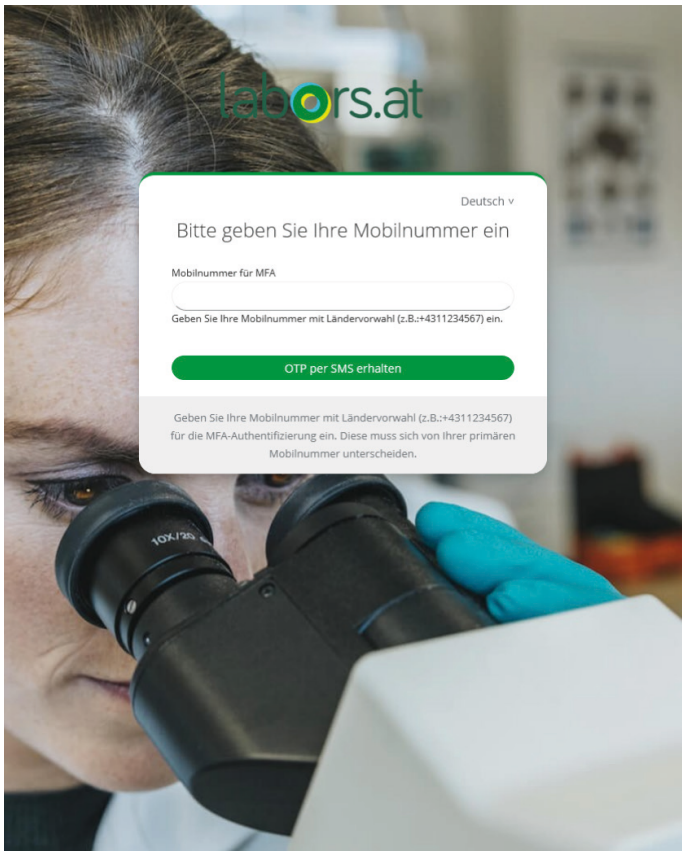
Die E-Mail-Adresse die Sie angeben, darf nicht dieselbe E-Mail-Adresse sein, mit der Sie Ihr Passwort zurücksetzen können.

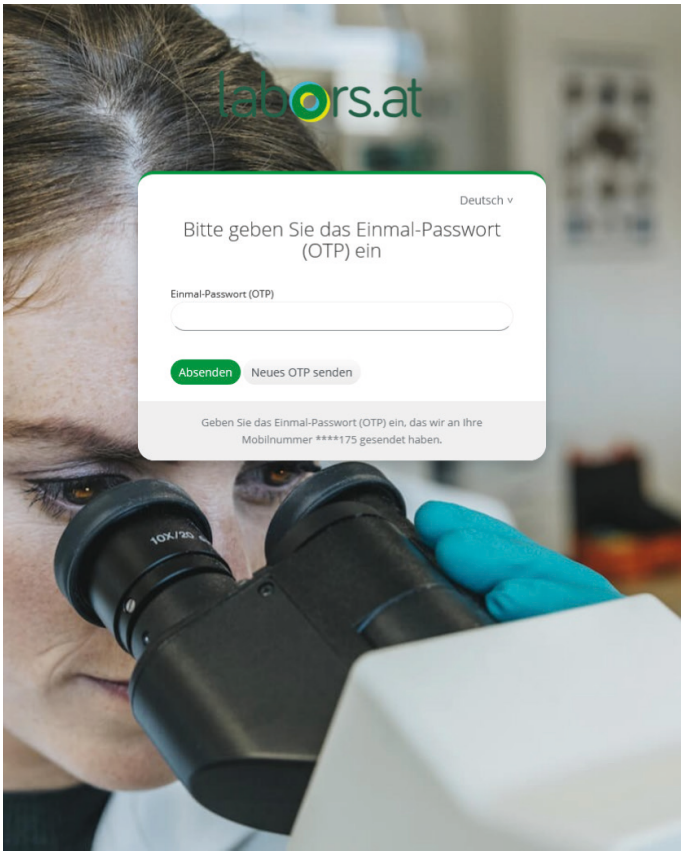




SMS OTP

Bei der Nutzung von SMS OTP wird ein Einmal-Passwort generiert, welches per SMS auf Ihr Mobiltelefon zugestellt wird. Dieses Passwort wird als zweiter Faktor bei der Anmeldung verwendet. Nach der Anmeldung verliert das Passwort seine Gültigkeit und kann für den nächsten Anmeldevorgang nicht mehr verwendet werden. Fordern Sie im Bedarfsfall ganz einfach ein weiteres Einmal-Passwort an.



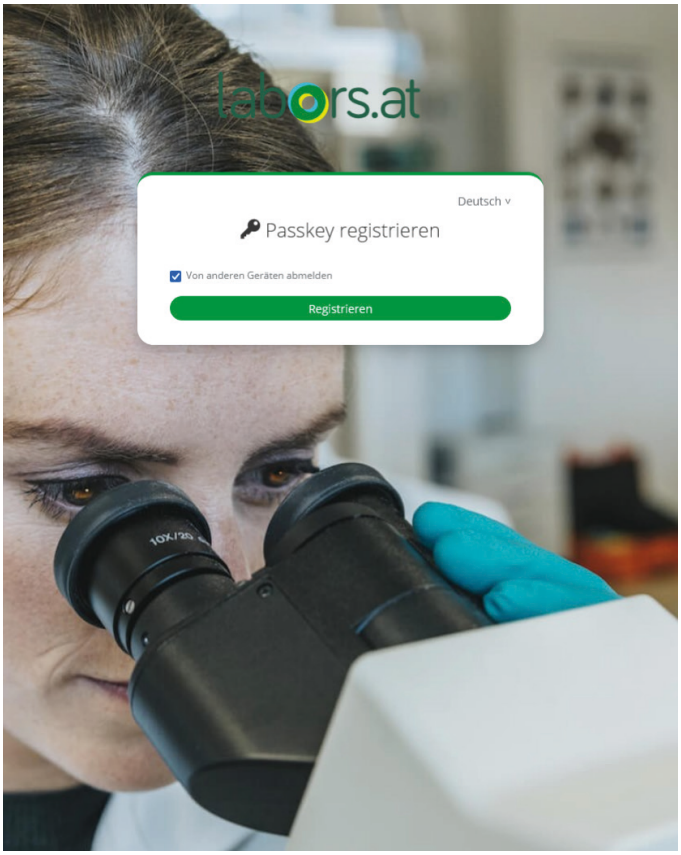


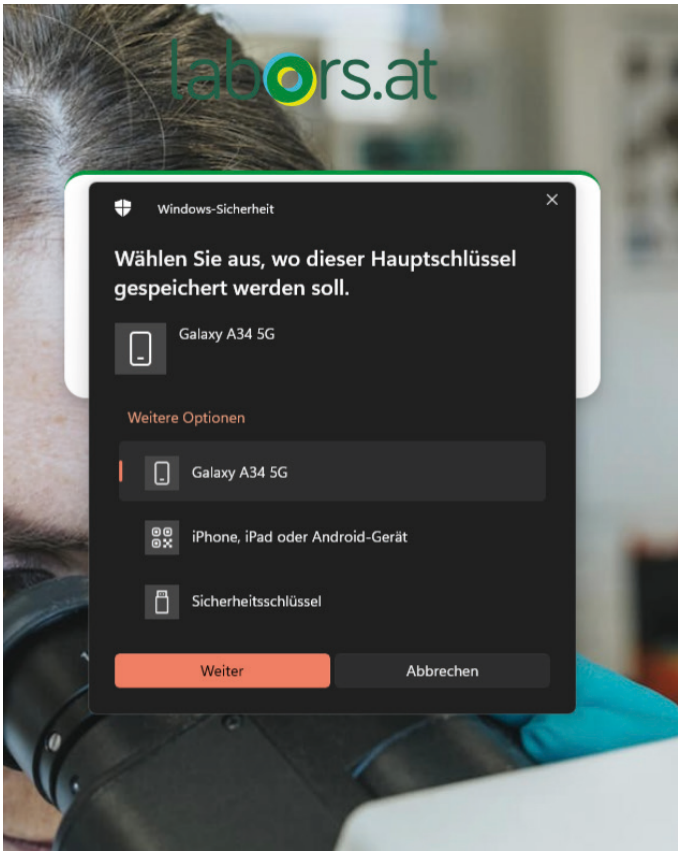
Passkey

Wenn Sie sich bei labors.at über die MFA-Methode Passkey anmelden, kommuniziert die Website mit dem Passkey auf Ihrem lokalen Gerät (z.B. Mobiltelefon oder PC/Mac). Die Website sendet dazu eine Anfrage. Danach sendet Ihr Gerät eine digitale Signatur an die Website zurück. Sind alle Prüfungen erfolgreich abgeschlossen, sind Sie bei labors.at authentifiziert.

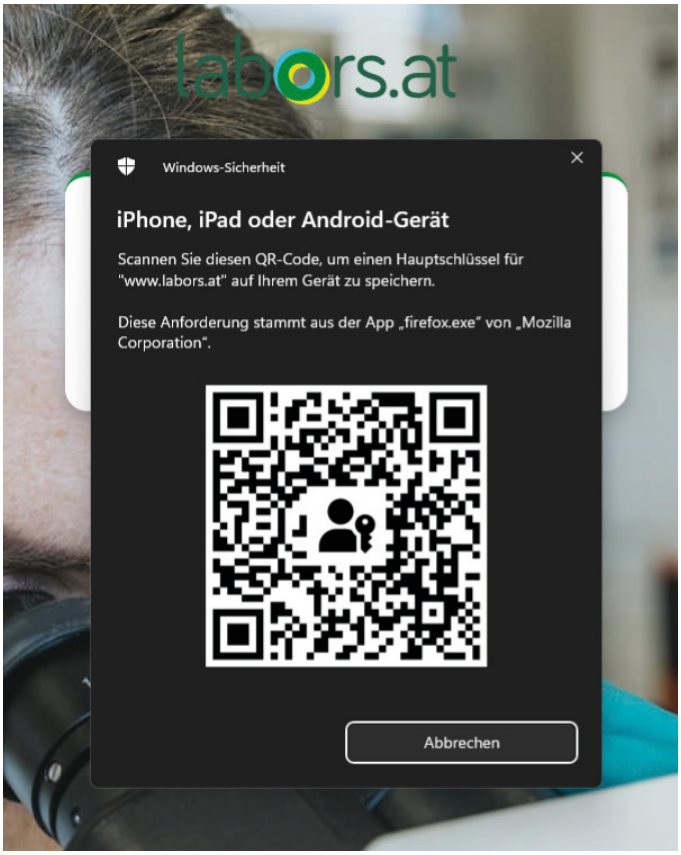
Folgen Sie dazu den Schritten der Screenshots. Je nach Gerät, kann es zu Abweichungen kommen.

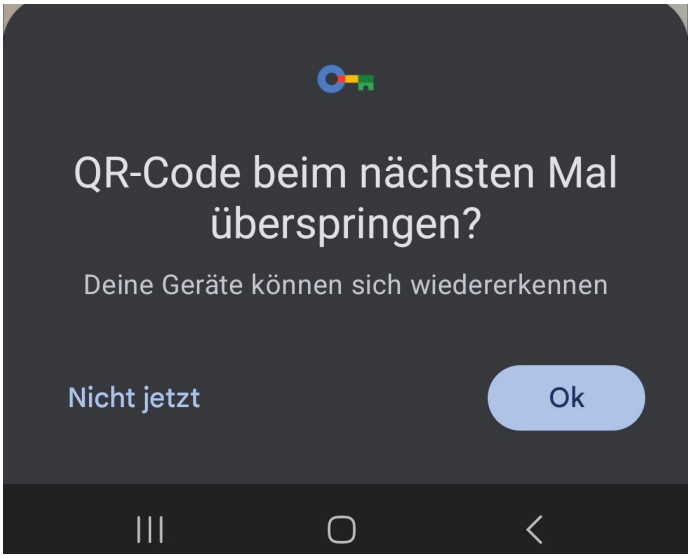
Wählen Sie als nächstes den Punkt „ iPhone, iPad oder Android-Gerät“ aus, damit der entsprechende QR-Code generiert werden kann und klicken Sie auf „Weiter“.





Bitte Scannen Sie den von Ihrem Gerät erzeugten QR-Code.



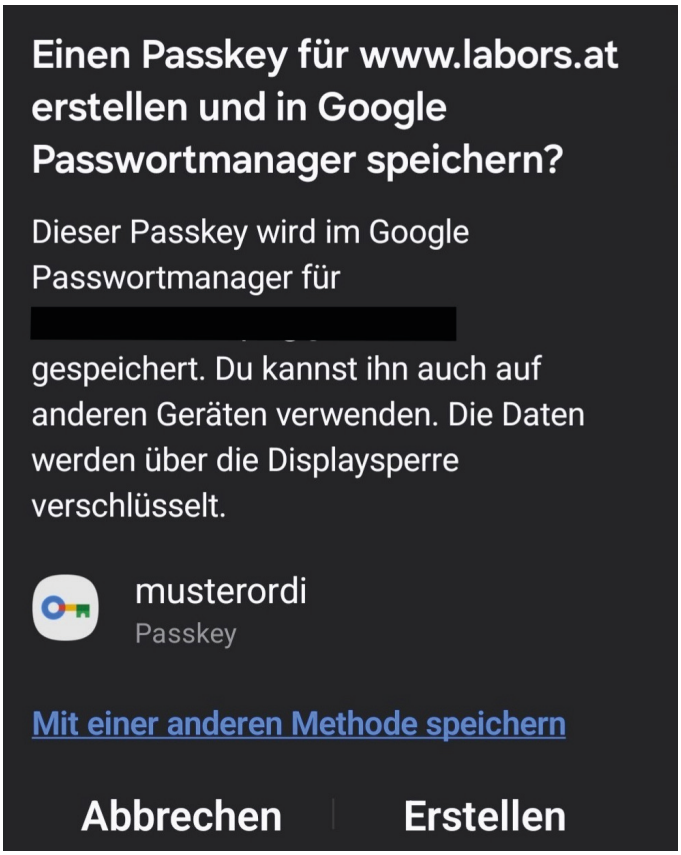


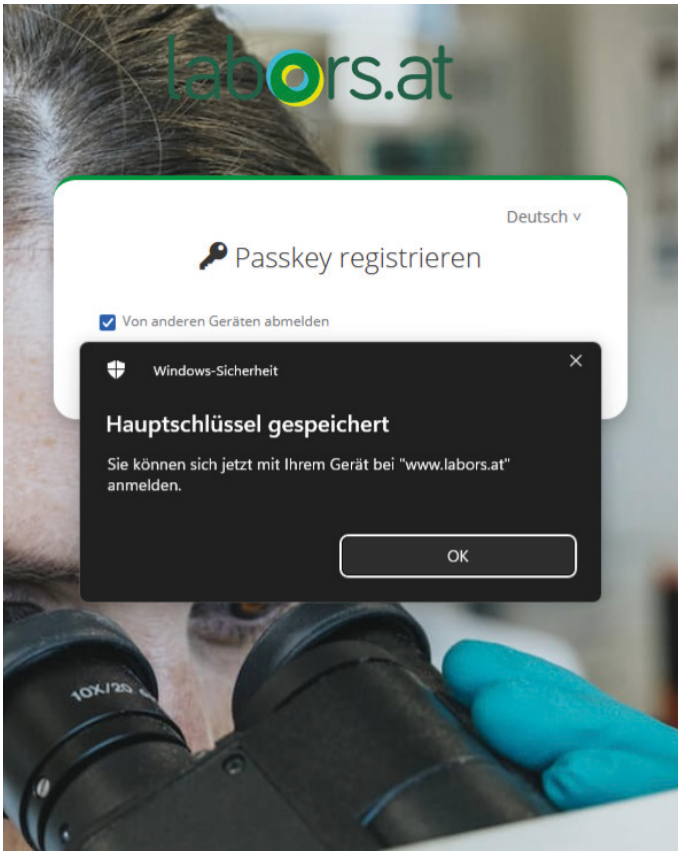
Nach dem Scannen erscheint am Smartphone (in diesem Fall Android) dieses Fenster.

Bestätigen Sie dies bitte mit „OK".

Am Smartphone erscheint dann das nächste Fenster, hier klicken Sie rechts unten auf „Erstellen“.

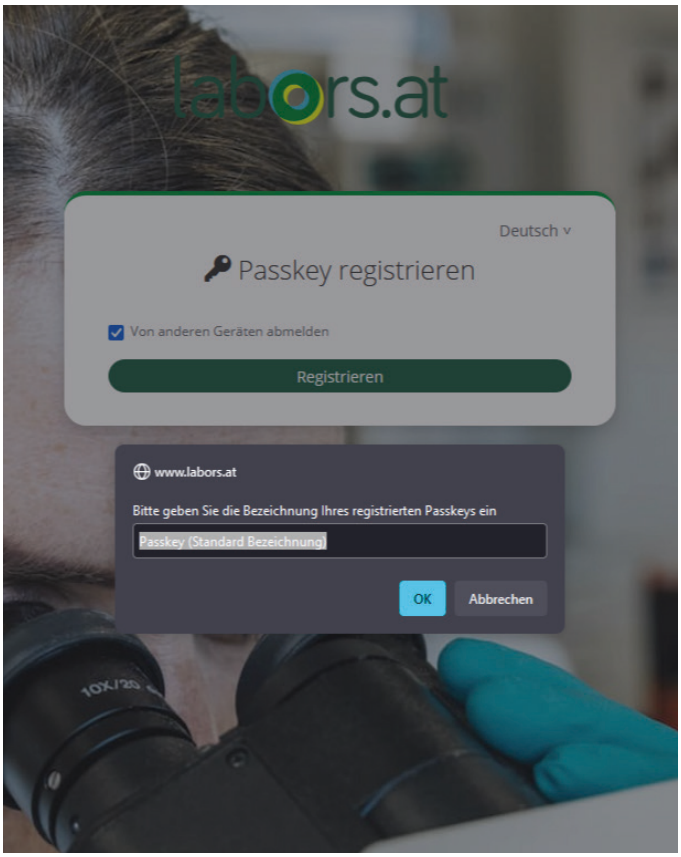
Anschließend muss das gewählte Gerät entsperrt werden (z.B. Fingerabdruck/Gesichtserkennung etc.).





Daraufhin erscheint dieses Fenster am Computer-/ Mac-Bildschirm, klicken Sie hier auf „OK“.

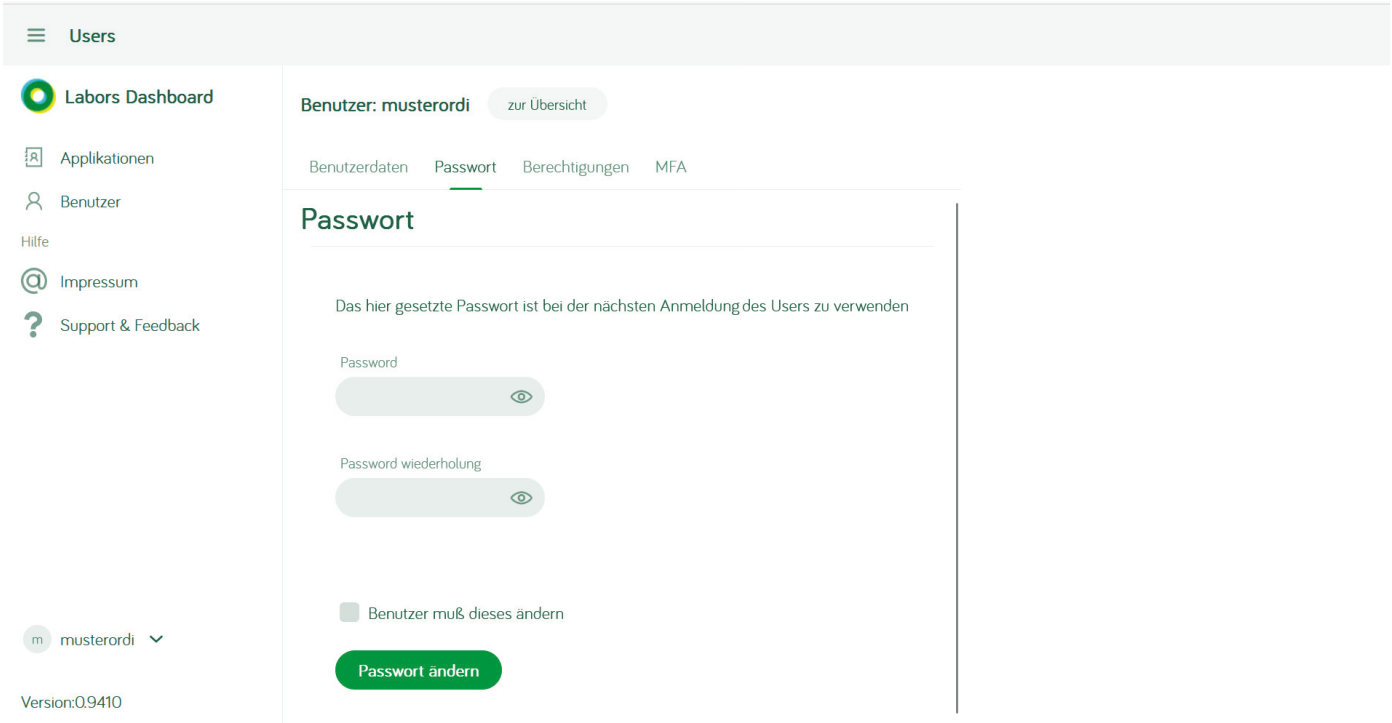
Hier können Sie Ihren Passkey umbenennen, wenn gewünscht, andernfalls drücken Sie direkt auf „OK“.



Dashboard/Selfservice

Wenn Sie die Multi-Faktor-Authentifizierung durchgeführt haben, gelangen Sie ins Befundinformationssystem. Dort gehen Sie über „Optionen“ und „Konto“ ins Dashboard.

Wenn Sie dies durchgeführt haben, landen Sie in diesem Fenster.

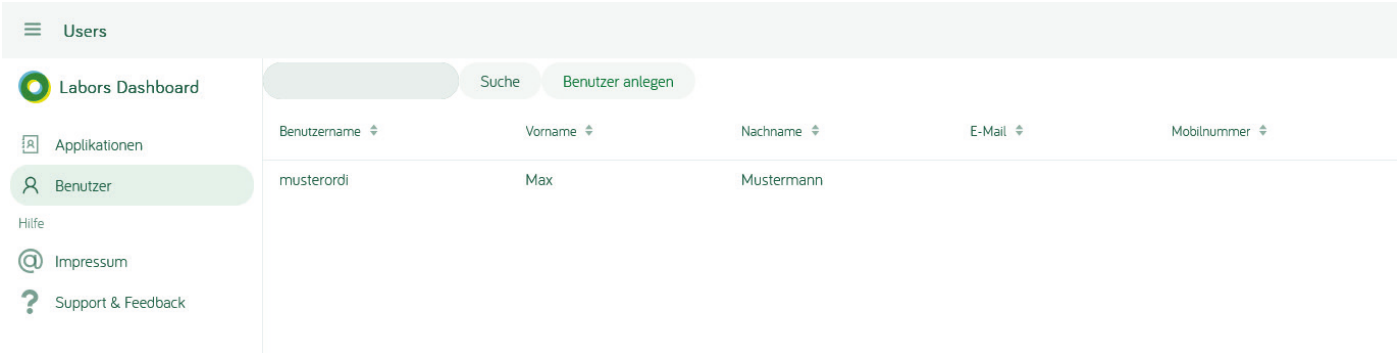


Um Anpassungen in Ihrem Konto durchzuführen, klicken Sie auf das entsprechende Feld und ändern Sie Ihre Daten wie gewünscht.

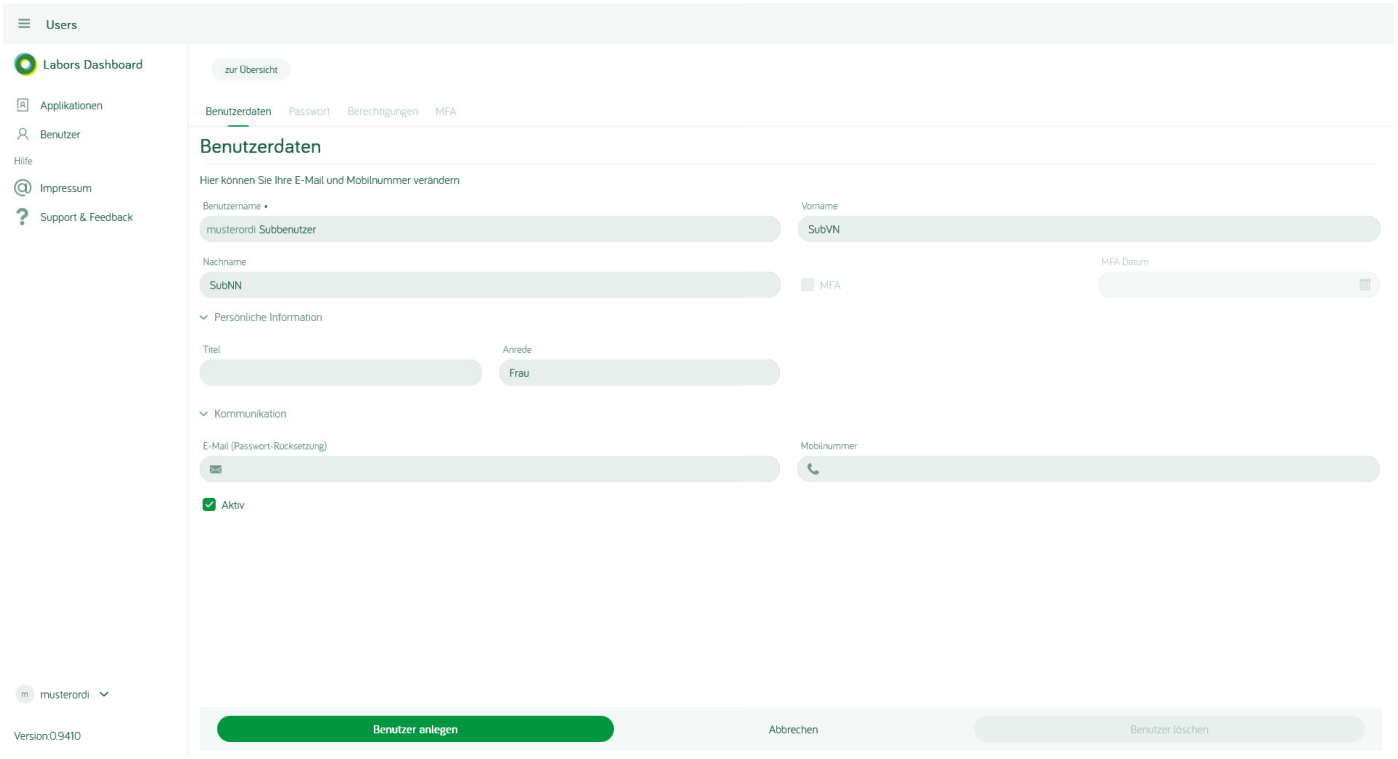
Anlegen von Subusern

Falls nicht jeder Benutzer des BIS Zugriff auf denselben zweiten Faktor hat, gibt es die Möglichkeit Subuser anzulegen, denen verschiedene eigene zweite Faktoren zugewiesen werden können.

Das Anlegen funktioniert über den Button „Benutzer anlegen“.

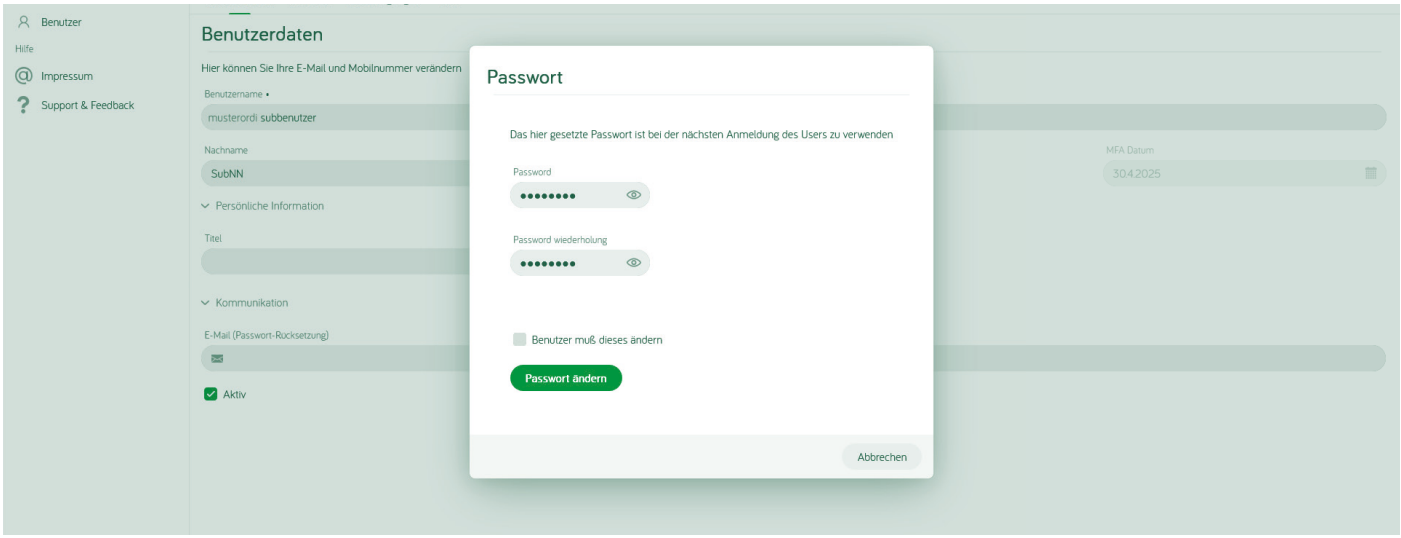


Das einzige Pflichtfeld für den Subuser, ist das Namensfeld.

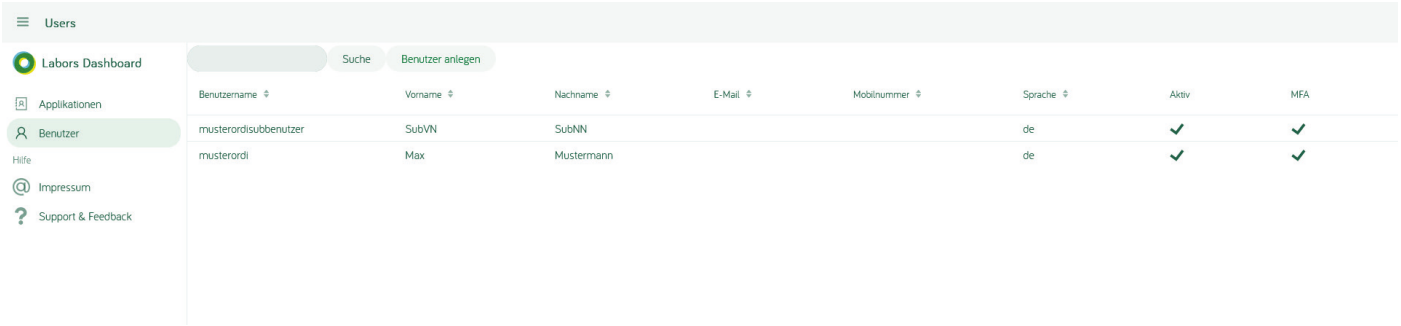


Mit dem grünen Butten „Benutzer anlegen“ kommen Sie dann zur Passwortvergabe.

Für den Subuser kann, wenn gewünscht dann ein eigenes Passwort vergeben werden. Dies ist aber nicht notwendig. Es kann weiterhin ein Einstieg mit dem bisher verwendeten Benutzernamen und Passwort stattfinden. Falls Sie doch ein eigenes Passwort vergeben möchten, beachten Sie die Mindestanforderung von acht Zeichen.



Im Anschluss finden Sie im Dashboard unter „Benutzer“ den angelegten Subuser und alle anderen User.



Anmeldung mit Subuser

Wenn Sie sich mit dem Subuser anmelden wollen, wählen Sie den entsprechenden User und somit auch automatisch den zugehörigen zweiten Faktor aus und können sich auf diesem Wege anmelden.