

SPORTAL



Inhalt

SPORTAL

**Hilfe für die Selbstregistrierung
der Ärzte/Ärztinnen und deren
Ordinationsmitarbeiter*innen**

Abteilung 1 Organisation und Informationstechnik

Stand: 08.02.2021

2021



Das Land
Steiermark

| Dokumentinformationen: | |
|-------------------------------|-----------------------|
| Version: | 1.0 |
| Stand: | 08.02.2021 |
| Speicherort: | |
| Erstellt von: | Caroline Müller |
| Freigegeben von: | Herbert Hüttenbrenner |
| Freigegeben am: | 08.02.2021 |
| Publikationsort: | Öffentlich per Email |
| GZ: | |

INHALTSVERZEICHNIS

| | | |
|----------|-------------------------------------|----------|
| 1 | ZWECK DIESES DOKUMENTS | 2 |
| 2 | SELBSTREGISTRIERUNG..... | 3 |
| 3 | ERSTANMELDUNG..... | 7 |
| 4 | PASSWORTRICHTLINIE..... | 9 |

1 ZWECK DIESES DOKUMENTS

Für die Freischaltung der Anwendung HIPPO für die Ärzte/Ärztinnen und deren Ordinationsmitarbeiter*innen, müssen sich ALLE Personen einer Arztpraxis, welche Zugriff auf die Anwendung HIPPO benötigen am Portal des Landes Steiermark registrieren, damit ihnen der Zugriff freigeschalten werden kann. Hierfür sind folgende Schritte auszuführen:

1. Selbstregistrierung JEDER Person, welche für eine Arztpraxis Zugriff auf die Anwendung HIPPO benötigt – siehe Selbstregistrierung
2. Anruf beim Land Steiermark zur Bestätigung der selbstregistrierten Benutzer durch eine Person der Arztpraxis. Die Kontaktdaten und –zeiten entnehmen Sie bitte dem Schreiben an Sie. Bei diesem Anruf benötigen wir folgende Informationen von Ihnen:
 1. Österreichische Ärztekammernummer
 2. Namen der Personen, welche sich selbst registriert haben

Erst durch diesen Anruf wird der Zugriff auf das Portal des Landes Steiermark freigeschalten – dies ist aus Datenschutzgründen zwingend erforderlich, da andernfalls unberechtigte Personen Zugriff auf die Anwendung HIPPO erhalten könnten.

3. Nach Freischaltung erhält jede Person eine Mail mit ihren persönlichen Zugangsdaten, mit welchen sie sich umgehend anmelden sollte, da das initiale Kennwort bereits nach 3 Tagen ungültig wird und bei Erstanmeldung geändert werden muss – das selbst gewählte Kennwort ist dann länger gültig. Siehe Erstanmeldung

2 SELBSTREGISTRIERUNG

3. Aufruf des **STERZ-Portals**: <https://sterz.stmk.gv.at>
4. Für die Selbstregistrierung wählen Sie bitte die Schaltfläche **E-Formular: STERZ-Selbstregistrierung** aus.

E-Formular STERZ-Selbstregistrierung

ANMELDUNG

Benutzername

Passwort

Anmelden

ALTERNATIVE ANMELDEMETHODEN



Handy



Karte (lokal)

> Neuladen der Seite bei Problemen mit Handy oder Karte

**Um sich mit Karte anzumelden, benötigen Sie eine lokale Bürgerkartenumgebung.
Um diese herunterzuladen, klicken Sie bitte hier.**

5. Im nächsten Schritt müssen Sie die **Domain des Portalteilnehmers** eingeben.

Domain

Die für Sie korrekte Domain enthält ihre Österreichische Ärztekamernummer und setzt sich wie folgt zusammen:

ärztekamernummer.oeak.gda.stmk.gv.at → dh im Falle der Ärztekamernummer 11111-11 müssen Sie hier bitte 11111-11.oeak.gda.stmk.gv.at angeben!

STERZ - externe Benutzermeldung



Bitte beachten Sie

[Hinweise zum Verfahren / Formular](#) * Feld muss ausgefüllt sein [Hinweise zum Verfahren / Formular](#) [Fehlerhinweis](#) » Mobil

Domain des Portalteilnehmers

Domain *

Zwischenspeichern Daten laden Weiter Abbrechen

STERZ - externe Benutzermeldung - 29.06.2009
[Bedienungshinweise](#)

Im nächsten Schritt wird Ihnen die Arztpraxis angezeigt, welche zu der angegebenen Domain hinterlegt ist. Ist dies die korrekte, bestätigen Sie dies bitte mit Weiter, andernfalls gehen sie „Zurück“ und kontrollieren die angegebene Ärztekammernummer.

STERZ - externe Benutzermeldung



Bitte beachten Sie

[Hinweise zum Verfahren / Formular](#) * Feld muss ausgefüllt sein [Hinweise zum Verfahren / Formular](#) [Fehlerhinweis](#) » Mobil

Organisation des Portalteilnehmers

Organisation *

Zwischenspeichern Zurück Weiter Abbrechen

STERZ - externe Benutzermeldung - 29.06.2009
[Bedienungshinweise](#)

Sollten Ihnen mehrere Arztpraxen angezeigt werden, wählen Sie bitte die Arztpraxis aus, für welche Sie sich registrieren möchten.

STERZ - externe Benutzermeldung



Bitte beachten Sie [Hinweise zum Verfahren / Formular](#) * Feld muss ausgefüllt sein [Hinweise zum Verfahren / Formular](#) [Fehlerhinweis](#) » Mobil

Organisation des Portalteilnehmers

Organisation *
 Organisation des Landes Steiermark
 Land Steiermark Verein
 Test Organisation 2

Weiter Abbrechen

STERZ - externe Benutzermeldung - 29.06.2009
[Bedienungshinweise](#)

- Auf der nächsten Seite geben Sie bitte Ihre **Personendaten** an. Bitte bestätigen Sie Ihre Eingaben mit Weiter.

Dienstadresse und -kontakt

Beim Block **Dienstadresse und -kontakt** ist bereits die Adresse der, anhand der angegebenen Domain, ausgewählten Arztpraxis hinterlegt – hier sind nur ggf. fehlende Daten zu ergänzen.

Mobil

Beim Block **Dienstadresse und -kontakt** ist zwingend eine Mobiltelefonnummer zu hinterlegen, da Sie diese für den Zugriff auf die Anwendung HIPPO zum Erhalt eines Handy-TANs/SMS-TANs benötigen. Um zu verhindern, dass durch Verlust/Erraten von einer Username/Passwort Kombination der Zugriff auf die Daten in HIPPO durch nicht befugte Dritte erfolgt, wird der Zugriff zusätzlich zu Username/Passwort noch mit einem SMS-TAN abgesichert. Wie die Eingabe davon erfolgt, erhalten Sie als gesonderte Anleitung zusammen mit der Information zu HIPPO.

STERZ - externe Benutzermeldung

E-Government



Bitte beachten Sie [Hinweise zum Verfahren / Formular](#) * Feld muss ausgefüllt sein [Hinweise zum Verfahren / Formular](#) [Fehlerhinweis](#) [» Mobil](#)

Portalsbenutzer/in

| | | | |
|-----------------------------|----------------------|--------------|--|
| Familienname * | <input type="text"/> | Akadem. Grad | <input type="text"/> |
| Vorname * | <input type="text"/> | Geschlecht * | Bitte auswählen ... <input type="button" value="v"/> |
| Geburtsdatum (TT.MM.JJJJ) * | <input type="text"/> | | |

Dienstadresse und -kontakt

| | | | |
|--|---|-------|----------------------|
| Land * | <input type="text" value="Österreich"/> <input type="button" value="v"/> | | |
| PLZ Ort * | <input type="text" value="8010 Graz"/> <input type="button" value="i"/> | | |
| Strasse Hausnummer * | <input type="text" value="Burggasse 2"/> <input type="button" value="i"/> | | |
| Vorwahl, Hauptnummer und Nebenstelle mit "/" trennen | | | |
| Festnetz | <input type="text"/> | Mobil | <input type="text"/> |
| E-Mail * | <input type="text"/> | | |

STERZ - externe Benutzermeldung - 29.06.2009
[Bedienungshinweise](#)

Ihre Daten werden im Hintergrund mit dem **Zentralen Melderegister** (ZMR) überprüft. Wenn Ihre Angaben zu keinem eindeutigen Ergebnis führen, erscheint eine Fehlermeldung im Formular. Wenn Sie der Meinung sind, dass Ihre Daten korrekt sind, so können Sie die Eingabe trotzdem übernehmen. Aktivieren Sie bitte in dem Fall unter **Eingabebestätigung** "Eingaben trotz Warnungen übernehmen". Ihre Angaben werden anschließend in der zuständigen Stelle überprüft.



Bitte beachten Sie **Hinweise zum Verfahren / Formular** * Feld muss ausgefüllt sein **Hinweise zum Verfahren / Formular** **Fehlerhinweis** » Mobil

Folgende Angaben fehlen oder sind fehlerhaft:
 • Sie können im Stammzahlenregister nicht eindeutig gefunden werden. Prüfen Sie Familienname, Vorname und Geburtsdatum und korrigieren Sie sie, wenn die Schreibweise nicht mit der der Geburtsurkunde übereinstimmt (wichtig bei Doppelnamen). Sie können die Daten dennoch übernehmen, indem Sie das Feld "Eingaben trotz Warnungen übernehmen" anhaken.

Portalsbenutzer/in

Familienname * x Akadem. Grad

Vorname * Geschlecht *

Geburtsdatum (TT.MM.JJJJ) *

Dienstadresse und -kontakt

Land * i

PLZ Ort * i

Strasse Hausnummer * i

Vorwahl, Hauptnummer und Nebenstelle mit "/" trennen

Festnetz Mobil

E-Mail *

Eingabebestätigung

Eingaben trotz Warnungen übernehmen

Zwischenspeichern Zurück Weiter Abbrechen

STERZ - externe Benutzermeldung - 29.06.2009
Bedienungshinweise

1. Abschließend gelangen Sie auf der letzten Seite auf die **Verpflichtungserklärung** zu Datensicherheitsmaßnahmen für Web-Anwendungen. Bitte lesen Sie die **Verpflichtungserklärung** sorgfältig durch und bestätigen Sie diese.

STERZ - externe Benutzermeldung

E-Government

EINSTIEG ORGANISATION BENUTZER/IN ZUSTIMMUNG KONTROLLE ABSCHLUSS

Bitte beachten Sie **Hinweise zum Verfahren / Formular** * Feld muss ausgefüllt sein **Hinweise zum Verfahren / Formular** **Fehlerhinweis** » Mobil

Verpflichtungserklärung

Verpflichtungserklärung: Datensicherheitsmaßnahmen für Web-Anwendungen

Generelle Bestimmungen
 Zielsetzung: Sicheres elektronisches Kommunikation zwischen der Steirischen Landesverwaltung und ihren Kommunikationspartnern sind Sicherheitsmaßnahmen auf mehreren Ebenen zu treffen. Die Einhaltung dieser Bestimmungen ist Voraussetzung für einen reibungslosen Ablauf elektronischer Kommunikation und daher verpflichtend für alle Teilnehmer.
 In Abhängigkeit von der Sicherheitsklassifizierung der jeweiligen Anwendung können neben den hier beschriebenen Allgemeinen Bestimmungen noch weitere Vorschriften wie etwa die Nutzung von SSL-Clientzertifikaten hinzukommen. Diese zusätzlichen Anforderungen werden im Bedarfsfall in einem separaten Dokument festgehalten.
 Die unter dem Punkt **Allgemeine Sorgfaltspflicht** beschriebenen Maßnahmen gelten für alle Benutzer, unabhängig von ihrer Funktion.

Allgemeine Sorgfaltspflicht
Benutzerkonten und Passwörter
 Die Anlage von Benutzerkonten (Benutzermeldung) in den einzelnen personalführenden Stellen erfolgt durch die jeweils **nominierten Benutzerverwalter**. Beim Einrichten der Benutzerkonten wird ein **vereinbartes Standard-Passwort** vergeben, welches beim **ersten Anmeldevorgang vom berechtigten Benutzer zu verändern** ist. Es ist darauf zu achten, dass diese Passwort-Änderung noch am selben Tag, jedenfalls aber so bald wie möglich erfolgt.
 Benutzerkonten sind **personenbezogen**, daher darf nur der Eigentümer das jeweilige Konto benutzen. Die Benutzer dürfen das Passwort **unter keinen Umständen** anderen Personen **bekannt geben**. Eine schriftliche Fixierung ist nur zulässig bei versiegelter Aufbewahrung in einem Schließfach, wobei die Erfüllung des Siegels zu dokumentieren ist.

Weitere gelten die folgenden Bestimmungen für Passwörter:

- Ein **Passwort** muss aus **mindestens 8 Zeichen** bestehen und muss nach **spätestens 180 Tagen** umgesetzt werden. Sollte der Verdacht bestehen, dass das Passwort auch Personen außerhalb des berechtigten Personenkreises bekannt ist, so ist das Passwort auch vor Ablauf dieser Frist sofort zu ändern.
- Die Verwendung von **Trivial-Passwörtern** ist unbedingt zu **unterlassen**. (Trivial-Passwörter sind solche Passwörter mit spezieller Bedeutung, welche leicht auch von Außenstehenden erraten oder bestimmt werden können. Also z.B. Namen (eigene, aus der Familie, von Prominenten), Geburtsdaten, Firmen- und Abteilungsbezeichnungen, Kfz-Kennzeichen usw.. Ebenfalls in diese Gruppe fallen Standardausdrücke wie etwa TEST, SYSTEM, Tastatur- und Zeichenmuster, wie ABCDEF, QWERTZ, 123456,...)
- Innerhalb eines Passwortes sollte mindestens 1 Zeichen verwendet werden, das kein Buchstabe ist (**Zahl oder Sonderzeichen**).
- Ganz allgemein ist darauf zu achten, dass die **Eingabe** des Passwortes **unbeobachtet** erfolgt.
- Passwörter dürfen **nicht** auf programmierbaren Funktionskarten **gespeichert** werden.
- Soweit es das jeweilige Betriebssystem zulässt, ist die Einhaltung dieser Richtlinien durch entsprechende Einstellungen des Betriebssystems sicherzustellen.

Eine fünfmalige Fehleingabe des Passwortes führt zur Sperrung der Zugangsberechtigung, welche nur durch den Rechteinhaber der Organisationseinheit wieder aufgehoben werden kann.

Virenschutz
 Viren, ebenso wie Trojaner, Würmer u.a.m., sind Programme, die verdeckte Funktionen enthalten und damit durch Löschen, Überschreiben oder sonstige Veränderungen **unkontrollierbare Schäden an Daten und Programmen** anrichten können. Um diese Schäden und die damit verbundenen oft erheblichen Kosten und Aufwänden zu vermeiden, sind insbesondere die **folgenden vorbeugenden Maßnahmen** zu treffen:

- Einsatz eines marktgängigen **Anti-Viren Programms**
- **Regelmäßiges Update** der Virendatenbank.
- **Überprüfung** aller ein- und ausgehenden **Datenträger**.

Zugriffsschutz und Raumsicherheit
 Zusätzlich zu den schon genannten Maßnahmen ist es notwendig, den Zutritt zu den Räumen und Geräten zu regeln, in denen sich Kommunikationsendpunkte (also in der Regel PCs) befinden.

Folgende Maßnahmen werden dringend empfohlen:

- **Verbindungen sind zu trennen**, sobald sie nicht mehr benötigt werden.
- Bei **kurzer Abwesenheit** ist immer ein **Bildschirmschoner** mit **Passwortschutz** zu verwenden (**Wartezeit 5 Minuten**).
- Bei **längerer Abwesenheit** ist der PC / die Workstation **niederzufahren**.
- **Räume sind beim Verlassen abzusperren**, wo immer das möglich ist.
- **Bildschirme** sind so **aufzustellen**, dass **keine unbefugte Einsicht** möglich ist.
- **Datenträger / Ausdrucke** sind vor **Einsichtnahme zu schützen**.

Ich habe die obenstehenden Maßnahmen gelesen und verstanden. Ich verpflichte mich, diese Vorschriften zu beachten und die oben angeführten Maßnahmen einzuhalten. Mir ist bewusst, dass ein Missachtung dieser Bestimmungen zum Entzug der Zugangsberechtigung als STERZ-Benutzer führt. *

Zwischenspeichern Zurück Weiter Abbrechen

STERZ - externe Benutzermeldung - 29.06.2009
Bedienungshinweise

2. Ihnen wird in Kürze ein Einmal-Passwort per E-Mail zugesendet. Bitte führen Sie anschließend die **Erstanmeldung** durch, um Ihre Registrierung abzuschließen.

3 ERSTANMELDUNG

Vor der ersten Anmeldung erhalten Sie (nach Freischaltung Ihres Kontos) eine automatisch generierte E-Mail mit ihre Zugangsdaten. Diese beinhaltet folgende Informationen:

1. Link zum STERZ-Portal

Sg. Hr. Mustermann

Das Kennwort ihres Benutzerkontos wurde im Berechtigungssystem des Landes Steiermark (STERZ) rückgesetzt. Sie werden ersucht sich umgehend am eGovernment-Portal des Landes (<https://sterztest.stmk.gv.at>) anzumelden und das Kennwort zu ändern. Wenn das Kennwort innerhalb von drei Tagen nicht geändert wird, wird das Benutzerkonto gesperrt.

Ihre Anmeldedaten sind:

Benutzername: mustermann@muster.stmk.gv.at
einmaliges Kennwort: 2jAT8pMSAX

Hinweis: Hilfe zum Anmelden finden Sie unter <http://sterz.stmk.gv.at/E-Learning/demo/sterz-anmeldung-erste.htm>

Ihre Kennworrücksetzung erfolgte durch:

A1 Organisation und Informationstechnik
Telefon: +43 316 877

2. Benutzername, Einmaliges Passwort

Sg. Hr. Mustermann

Das Kennwort ihres Benutzerkontos wurde im Berechtigungssystem des Landes Steiermark (STERZ) rückgesetzt. Sie werden ersucht sich umgehend am eGovernment-Portal des Landes (<https://sterztest.stmk.gv.at>) anzumelden und das Kennwort zu ändern. Wenn das Kennwort innerhalb von drei Tagen nicht geändert wird, wird das Benutzerkonto gesperrt.

Ihre Anmeldedaten sind:

Benutzername: mustermann@muster.stmk.gv.at
einmaliges Kennwort: 2jAT8pMSAX

Hinweis: Hilfe zum Anmelden finden Sie unter <http://sterz.stmk.gv.at/E-Learning/demo/sterz-anmeldung-erste.htm>

Ihre Kennworrücksetzung erfolgte durch:

A1 Organisation und Informationstechnik
Telefon: +43 316 877

 **Achtung:** Das hier zugewiesene Passwort ist nur für 3 Tage gültig! Bitte führen Sie die Erstanmeldung unbedingt sofort durch und ändern Sie Ihr Passwort.

Bitte öffnen Sie den Link und geben Ihren Benutzernamen und Ihr einmaliges Passwort ein.

ANMELDUNG

Benutzername

Passwort

Sie werden umgehend zur Passwortänderung aufgefordert.

PASSWORT ÄNDERN

Passwortänderung muss durchgeführt werden. Es sind keine anderen Aktionen erlaubt.

Altes/Einmaliges Passwort

Neues Passwort

Passwort bestätigen

Senden

Passwortregelung

Bitte beachten Sie bei der Wahl Ihres Passworts auch die [Passwortrichtlinie](#).

4 PASSWORTRICHTLINIE

An Passwörter werden vom Stammportal folgende Mindestanforderungen gestellt:

- Ein Passwort muss aus mindestens 8 Zeichen bestehen und muss nach spätestens 180 Tagen erneuert werden.
- Innerhalb eines Passwortes müssen sowohl Groß- und Kleinbuchstaben, als auch Ziffern und Sonderzeichen verwendet werden.
- Die Wiederverwendung der letzten neun in der Vergangenheit bereits verwendeten Passwörter ist nicht möglich.
- Die mehrfache Fehleingabe eines Passwortes führt zu einer Sperre des zugehörigen Kontos. Die Sperre kann nur durch die zuständigen [Benutzerverwalter](#) aufgehoben werden.

Die folgenden allgemeinen Anforderungen sollten von BenutzerInnen eingehalten werden:

- Eine Benutzerin/ein Benutzer darf ihr/sein persönliches Passwort unter keinen Umständen anderen Personen bekannt geben.
- Eine schriftliche Fixierung ist nur zulässig in begründeten Ausnahmefällen und bei Aufbewahrung an einem sicheren Ort (etwa einem Safe), welcher für Unbefugte nicht zugänglich ist bzw. mit dem zugehörigen Benutzerkonto nicht in Verbindung gebracht werden kann. Die Bildschirmkante, die Tastaturunterseite und ähnliche „Hinterlegungsorte“ sind folglich nicht zulässig.
- Die Verwendung von Trivial-Passwörtern oder Wörtern, die sich in einem Wörterbuch finden, ist unbedingt zu unterlassen.
 - Trivial-Passwörter sind Begriffe mit spezieller Bedeutung, welche leicht auch von Außenstehenden erraten oder bestimmt werden können. Also z.B. Namen (eigene, aus der Familie, von Prominenten), Geburtsdaten, Firmen- und Abteilungsbezeichnungen, Kfz-Kennzeichen usw.. Ebenfalls in diese Gruppe fallen Standardausdrücke wie etwa TEST, SYSTEM, Tastatur- und Zeichenmuster, wie ABCDEF, QWERTZ, 123456, ...
 - Wörterbuch-Wörter sind solche, die in einer verbreiteten Sprache eine Bedeutung haben, und daher in einem Wörterbuch zu finden sind. Das trifft auch auf Ausdrücke spezieller Themengebiete zu, wie etwa Computer, Medizin, Fantasy, u.a.m.!
- Ganz allgemein ist darauf zu achten, dass die Eingabe des Passwortes unbeobachtet erfolgt.
- Sollte der Verdacht bestehen, dass das Passwort nicht mehr geheim ist, so ist es schon vor Ablauf der Erneuerungsfrist sofort zu ändern und eine entsprechende Meldung an den für Sie zuständigen [Benutzerverwalter](#) zu machen, damit festgestellt werden kann, ob weitere Schritte unternommen werden müssen.