

Handreichung

Die Austauschplattform für Referendare:

Einrichtung und Zugriff

Erläuterungen für Referendarinnen und Referendare

Stand: März – 2023

Status: Freigegeben

Verantwortlich: ITD2C

Inhaltsverzeichnis

1	Einleitung.....	3
2	Zugang.....	3
2.1	Technische Voraussetzungen	3
2.2	Anmeldung	3
2.3	Kontoeinstellungen	6
2.3.1	Passwort ändern	7
2.3.2	Ausblendungsmöglichkeit der Mailadresse	7
2.3.3	Möglichkeiten bei Verlust des Zugangs zur 2FA-App	8
3	Anhang.....	9
3.1	Backup-Codes für die Zwei-Faktor-Authentifizierung	9
3.2	Neuen TOTP-Schlüssel generieren.....	10

1 Einleitung

Die Referendarplattform des IT-Dienstleisters der Justiz NRW (ITD) soll den Auszubildenden sowie den Referendarinnen und Referendaren die Möglichkeit eröffnen, Akteninhalte und erarbeitete Entwürfe auszutauschen, ohne auf externe Datenträger zurückgreifen zu müssen. Hierdurch wird der Austausch erleichtert und der notwendigen Datensicherheit Rechnung getragen.

Im Nachfolgenden werden Ihnen der Zugang und die Anmeldung erläutert.

2 Zugang

2.1 Technische Voraussetzungen

Die Plattform basiert auf Nextcloud. Der Aufruf ist mit allen aktuellen Browsern (z.B. Edge, Firefox, Chrome oder Safari) möglich.

Empfohlen wird grundsätzlich die Nutzung über Ihren Laptop oder den PC.

2.2 Anmeldung

Sie erhalten von Ihrer Referendarabteilung einen Benutzernamen und ein Passwort, mit denen Sie sich über den nachfolgenden Link

<https://itd.justiz.nrw.de/referendare>

an der Plattform anmelden können.

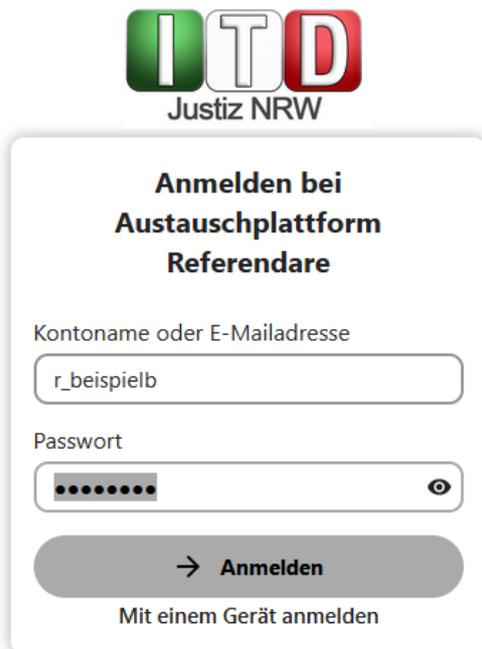
Die Anmeldung erfolgt im Wege der **Zwei-Faktor-Authentifizierung**, um die Sicherheit der Daten gewährleisten zu können. Bitte laden Sie sich auf Ihr Smartphone hierfür eine sogenannte **TOTP-App** (Time-based One-time Password). Die App generiert in kurzen Zeitintervallen eine Ziffer, die Sie im Anschluss an Ihre Anmeldung mit Benutzerkennung und Passwort in das angezeigte Feld eingeben, um anschließend Zugang zu der Plattform zu erhalten.

Wir empfehlen Ihnen den Einsatz einer der vielen kostenlosen TOTP-Apps (z.B. TOTP Authenticator, FreeTOP Authenticator u.a.), die Sie über ihren Google Playstore/ F-Droid (Android) bzw. den App-Store (Apple) beziehen und auf Ihrem Smartphone installieren können.

Nachdem Sie eine 2FA unter Ihrem Smartphone eingerichtet haben, erfolgt die Anmeldung zum Nextcloud-System in **zwei** Schritten:

1. Schritt:

Rufen Sie über den oben angegebenen Link die Anmeldeseite auf und geben Ihren Benutzernamen und das Passwort ein:



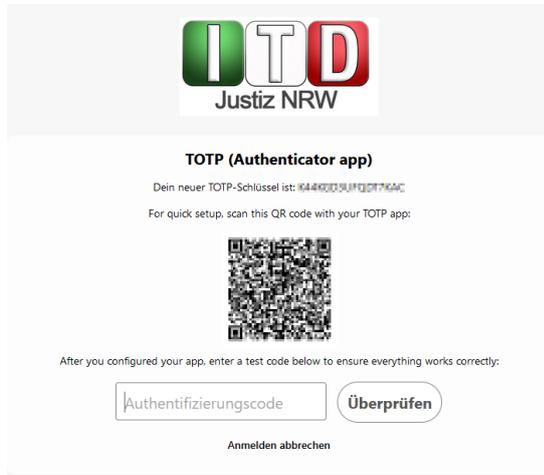
Betätigen Sie anschließend die Schaltfläche „Anmelden“.

2. Schritt

Es erscheint das nachfolgende Fenster. Betätigen Sie die Schaltfläche „TOTP (Authenticator app) Mit einer TOTP-App authentifizieren“.



Es öffnet sich unmittelbar das folgende Fenster, in dem Ihnen ein QR Code angezeigt wird:



Nun öffnen Sie die installierte Authenticator-App auf Ihrem Mobiltelefon. Die App wird den Zugriff auf Ihre Kamera verlangen. Nachdem Sie den Zugriff erlaubt haben, kann der QR-Code gescannt werden. Geben Sie nun den angezeigten Ziffern-Code in das entsprechende Feld auf dem Bildschirm ein und betätigen Sie die Schaltfläche „Überprüfen“. Sie erhalten anschließend Zugang zu der Plattform.

2.2.1 Folgeanmeldungen

Nachdem Sie die **Zwei-Faktor-Authentifizierung** eingerichtet haben, erfolgt künftig die Anmeldung zum Nextcloud-System in **zwei** Schritten:

1. Schritt:

Rufen Sie über den oben angegebenen Link die Anmeldeseite auf und geben Ihren Benutzernamen und das Passwort ein:



**Anmelden bei
Austauschplattform
Referendare**

Kontoname oder E-Mailadresse

Passwort

→ Anmelden

Mit einem Gerät anmelden

Betätigen Sie anschließend die Schaltfläche „Anmelden“.



TOTP (Authenticator app)

Erhalte den Authentifizierungscode von der
Zweifaktoraauthifizierung-App auf deinem
Gerät.

Übermitteln

[Backup-Code benutzen](#)

[Anmeldung abbrechen](#)

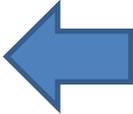
Geben Sie nun in das Feld „Authentifizierungscode“ die aktuelle Nummernfolge an, die Ihnen in Ihrer verwendeten App angezeigt wird. Sie erhalten anschließend Zugang zu der Plattform.

2.3 Kontoeinstellungen

Über Ihr Namenssymbol in der oberen rechten Ecke gelangen Sie in die allgemeinen Einstellungen.

Arndt Beispiel

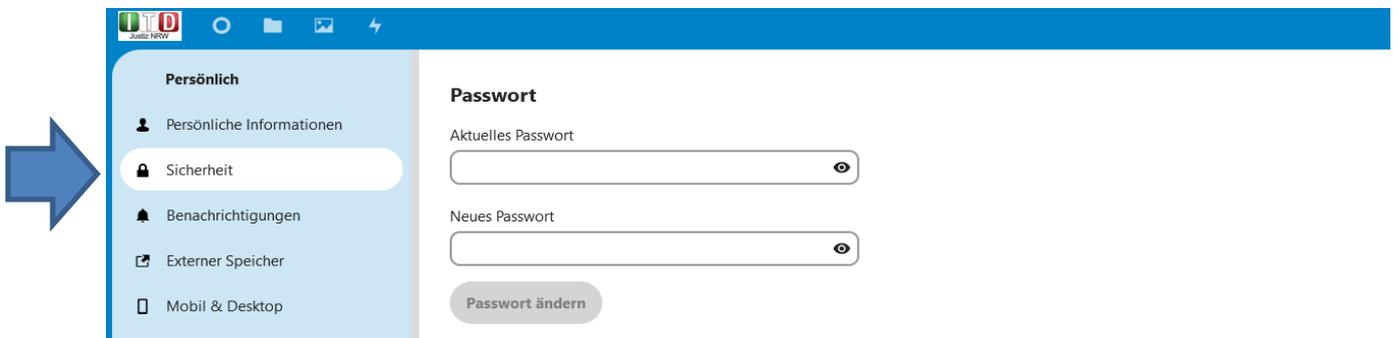
Profil ansehen

- Status setzen
-  Erscheinungsbild und Barrierefreiheit
-  Einstellungen 
-  Über
-  Hilfe
-  Abmelden

Hier können Sie Ihre persönlichen Daten bearbeiten.

2.3.1 Passwort ändern

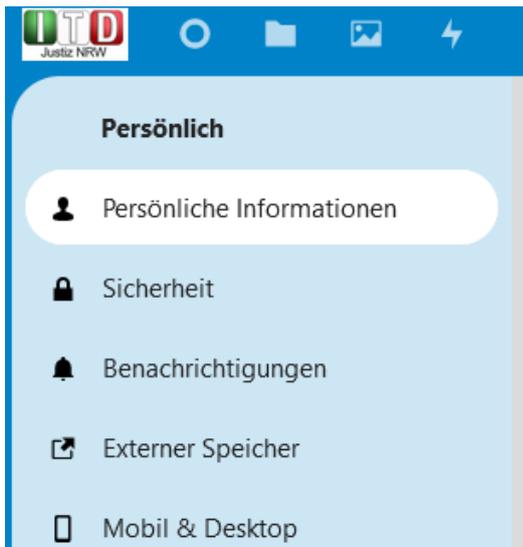
Über die Schaltfläche „Sicherheit“ können Sie Ihr Passwort ändern:



 **Ändern Sie bitte aus Gründen der Datensicherheit unbedingt nach der Erst-anmeldung Ihr Passwort!**

2.3.2 Ausblendungsmöglichkeit der Mailadresse

Sie haben die Möglichkeit, ihre persönlichen Einstellungen dahingehend anzupassen, dass ihre persönliche Mailadresse von anderen Benutzern ihrer Gruppe nicht eingesehen werden kann. Klicken Sie dazu auf „Persönliche Informationen“.



Scrollen Sie nun bis auf „Sichtbarkeit deines Profils“ herunter.

Sichtbarkeit deines Profils

Die restriktivere Einstellung von Sichtbarkeit oder Bereich wird in deinem Profil berücksichtigt. Wenn beispielsweise die Sichtbarkeit auf "Für jeden sichtbar" und der Bereich auf "Privat" festgelegt ist, wird "Privat" respektiert.

Adresse	<input type="text" value="Nur für angemeldete Benutzer sichtbar"/>	Twitter	<input type="text" value="Für jeden sichtbar"/>
E-Mail	<input type="text" value="Nur für angemeldete Benutzer sichtbar"/>		<input type="text" value="Für jeden sichtbar"/>
Funktion	<input type="text" value="Für jeden sichtbar"/>	Überschrift	<input type="text" value="Für jeden sichtbar"/>
Organisation	<input type="text" value="Für jeden sichtbar"/>	Vollständiger Name	<input type="text" value="Für jeden sichtbar"/>
Profilbild	<input type="text" value="Für jeden sichtbar"/>	Webseite	<input type="text" value="Für jeden sichtbar"/>
Telefon	<input type="text" value="Nur für angemeldete Benutzer sichtbar"/>		

Im Menüpunkt E-Mail können Sie die Einstellungen anpassen.

2.3.3 Möglichkeiten bei Verlust des Zugangs zur 2FA-App

Sollten Sie den Zugang zu Ihrer Zwei-Faktor-Authentifizierungs-App verlieren, z.B. durch Verlust Ihres Smartphone, haben Sie die Möglichkeit, sich mit Einmal-Codes anzumelden. Voraussetzung ist jedoch, dass von Ihnen **zuvor** Backup-Codes (Tan-Liste) erzeugt wurden.



Eine ausführliche Beschreibung zur Erstellung dieser Backup-Codes finden Sie im Anhang. Sollten Sie diese Code-Liste nicht erstellt haben, so wenden Sie sich im Falle des Zugangsverlustes bitte an Ihr Support-Team über das Funktionspostfach nextcloud@itd.nrw.de

3 Anhang

3.1 Backup-Codes für die Zwei-Faktor-Authentifizierung

Bei den Backup-Codes handelt es sich um eine erzeugte TAN-Liste, mit dessen Einmal-Codes Sie im Bedarfsfall die Zwei-Faktor-Authentifizierung durchführen können.

Über die Einstellungen und den Bereich „Sicherheit“ (siehe oben 2.3) gelangen Sie zu der Schaltfläche, die die Codes erstellt:

Zwei-Faktor-Authentifizierung ⓘ

Verwende neben deinem Passwort einen zweiten Faktor, um die Sicherheit für dein Konto zu erhöhen.

Wenn du Anwendungen von Drittanbietern verwendest, um dich mit Nextcloud zu verbinden, stelle bitte sicher, dass du für jede Anwendung ein Anwendungspasswort erstellst und einrichtest, bevor du die Zwei-Faktor-Authentifizierung aktivierst.

TOTP (Authenticator app)

TOTP aktivieren

Backup-Code

Backup-Codes erzeugen



Nach Betätigung werden Ihnen die Codes angezeigt.

Backup-Code

Dies sind Ihre Backup-Codes. Bitte speichern und/oder drucken Sie diese, da diese Codes später nicht mehr gelesen werden können

dZkGGSS7aSGvmsbA

qda5fCtMwffFARM6

JcFGedgt6XDi2bAt

HPf9cFkC3jAY603F

Yg3QPSjwc iT8P42b

wgASz2WNRW3PTEL

3JzGJw5nrMHFawTk

iWBKA2RHCHRSLXMS

CrgErn54RSFaDTyZ

GpdFg7mfxy3pjmDi



Backup-Codes speichern

Backup-Codes drucken

Backup-Codes erneuern

Wenn Sie die Backup-Codes erneuern, werden die alten Codes automatisch ungültig.

Sie sollten diese Codes an einem sicheren Ort aufbewahren. Legen Sie sie nicht zusammen mit Ihrem zweiten Faktor wie Ihrem Mobiltelefon ab, sondern stellen Sie sicher, dass Sie bei Verlust des einen, den anderen noch haben.

3.2 Neuen TOTP-Schlüssel generieren

Sofern Sie sich mit einem Backup-/Einweg-Code authentifiziert haben, können Sie sich einen neuen TOTP-Schlüssel generieren, den Sie dann in Zukunft für die Anmeldung nutzen können.

Klicken Sie hier auf die Schaltfläche TOTP aktivieren.

Zwei-Faktor-Authentifizierung ⁱ

Verwende neben deinem Passwort einen zweiten Faktor, um die Sicherheit für dein Konto zu erhöhen.

Wenn du Anwendungen von Drittanbietern verwendest, um dich mit Nextcloud zu verbinden, stelle bitte sicher, dass du für jede Anwendung ein Anwendungspasswort erstellst und einrichtest, bevor du die Zwei-Faktor-Authentifizierung aktivierst.

TOTP (Authenticator app)

TOTP aktivieren



Sie werden ggfls. nach Ihrem Passwort zur Bestätigung gefragt. Die TOTP-Schaltfläche wird dann aktiviert und Sie können die Schlüsselgenerierung erneut durchlaufen.