FAQs
Zwei-Faktor-Authentifizierung (2FA) für Q-global und Q-interactive

Im Folgenden finden Sie Fragen und Antworten rund um die Zwei-Faktor-Authentifizierung für Q-global und Q-interactive.
Wenn Sie noch weitere Fragen haben, hilft Ihnen unser Beratungsservice unter 069-756 146-17/-25/-32 oder per E-Mail an beratungsservice.de@pearson.com gerne weiter.

Was ist die Zwei-Faktor-Authentifizierung?
Die Zwei-Faktor-Authentifizierung (2FA) erfordert neben der Eingabe von Benutzername und Passwort eine zusätzliche Sicherheitsstufe beim Login in Q-global und Q-interactive durch die Eingabe eines Codes, der bei jedem Login neu generiert werden muss. Durch die Kombination aus Benutzername, Passwort und Code ist es Unbefugten nur schwer möglich, auf Ihre Daten zuzugreifen, auch wenn sie Ihr Passwort kennen sollten. Die 2FA kommt bereits bei anderen Diensten, beispielsweise beim Online-Banking oder in sozialen Medien zum Einsatz. Sie erfüllt außerdem die Richtlinien und Anforderungen der Datenschutzverordnung DSGVO, die ab 25. Mai 2018 in Kraft tritt.

Wie funktioniert die Zwei-Faktor-Authentifizierung?
Sobald Sie sich – nach Aktivierung der 2FA – das erste Mal in Q-global oder Q-interactive „Central" mit Ihrem Benutzernamen und Passwort anmelden, werden Sie aufgefordert, folgende Authentifizierungsmethoden für zukünftige Logins zu aktivieren:
- **E-Mail**
- **SMS**
- **Google Authenticator (**Android, iOS**)**

Sie müssen mindestens eine der drei Methoden einmalig aktivieren. **Wir empfehlen für eine größere Flexibilität, bei der erstmaligen Aktivierung mindestens zwei der drei Methoden als Option auszuwählen.** Bei zukünftigen Logins können Sie zwischen den von Ihnen aktivierten Methoden als zusätzliche Authentifizierung wählen. Daraufhin wird Ihnen ein Code per E-Mail oder SMS zugesandt bzw. in der Google Authenticator App generiert (die App muss dazu geöffnet sein).

Für Q-interactive „Central" und Q-global ist die Authentifizierung mit dem Code nach der Generierung des Codes für 12 Stunden gültig, sofern Sie das selbe Gerät verwenden. Wenn Sie sich mit einem anderen Gerät in Ihr Benutzerkonto einloggen, müssen Sie sich erneut mit der Zwei-Faktor-Authentifizierung anmelden.

Nur bei Q-interactive: Für die iPad-Anwendung Q-interactive „Assess" ist die Zwei-Faktor-Authentifizierung nur dann notwendig, wenn Sie mit dem Internet verbunden sind. Dies bedeutet, dass die Offline-Nutzung von „Assess" nur den Benutzernamen und das Passwort

erfordert. Bei der Anmeldung auf dem iPad haben Sie außerdem die Möglichkeit, die Option "Dieses Gerät merken" auszuwählen. Damit ist die Authentifizierung für das Gerät 30 Tage lang gültig. Ihren Benutzernamen und Ihr Passwort müssen Sie bei jedem Login dennoch eingeben.

Kann ich die Authentifizierungsoptionen im Nachhinein ändern?
Ja, im Verwaltungsbereich ist eine nachträgliche Änderung der Authentifizierungsoptionen möglich.

Wie lange ist der Code gültig?
Der einmalige, per SMS oder E-Mail versandte Code ist 15 Minuten lang gültig. Wenn Sie den Code nicht innerhalb dieses Zeitlimits verwenden, müssen Sie einen neuen Code generieren. Die Google Authenticator App generiert fortlaufend alle 30 Sekunden automatisch einen neuen Code. Codes über die App sind daher für 30 Sekunden gültig.

Ich habe mir den Code mehrmals gesendet. Welchen soll ich nutzen?
Gültig ist immer der neueste Code.

Was ist der Google Authenticator und wie funktioniert er?
Der Google Authenticator ist eine kostenlose App, die auf das Smartphone (Android, iOS, Windows Phone, Blackberry) oder – bei Q-interactive auch auf das Testpersonen-iPad – heruntergeladen und installiert wird. Die Anwendung generiert Codes, die Sie bei jedem Login in Ihr persönliches Q-global oder Q-interactive Benutzerkonto zur Zwei-Faktor-Authentifizierung verwenden können. Der Google Authenticator ist einfach zu verwenden und funktioniert ohne Internet und Netzwerkverbindung. Für den Google Authenticator benötigen Sie zwei Komponenten: Ihr Smartphone und Q-global bzw. Q-interactive „Central“. Sie öffnen zuerst die App auf dem Smartphone und lesen dann den Barcode in Q-global bzw. Q-interactive „Central“ mit der Smartphone-Kamera ab. Die App zeigt Ihnen daraufhin einen sechsstelligen Code an, den Sie in Q-global bzw. Q-interactive „Central“ zur Authentifizierung eingeben. Da die Anwendung alle 30 Sekunden einen neuen Code generiert, ist dies eine sehr sichere Methode der Zwei-Faktor-Authentifizierung.

Was passiert, wenn ich mein Smartphone verliere oder nicht zur Hand habe und daher keine Codes per SMS empfangen oder über den Google Authenticator verwenden kann?
Wenn Sie sich nur für die Authentifizierungsmethode des Google Authenticators entschieden haben, wenden Sie sich bitte an unseren Kundenservice telefonisch unter 069 756 146 -0 oder per Mail an info.de@pearson.com. Der Kundenservice setzt Ihre Einstellungen zurück und Sie können weitere Authentifizierungsmethoden im Verwaltungsbereich von Q-interactive „Central“ aktivieren.

Wenn Sie Ihr Smartphone nicht zur Hand haben und Sie nur den Google Authenticator oder SMS als Authentifizierungsoption aktiviert haben, ist zu diesem Zeitpunkt kein Login möglich. Alternativ ist es aber möglich, den Google Authenticator bei Q-interactive auf das Testpersonen-iPad zu installieren.

Ihr Kontakt zu uns: Pearson Beratungsservice | Tel.: 069/756 146-17/-25/-32 | beratungsservice.de@pearson.com

Wenn Sie jedoch auch die Authentifizierungsmethode E-Mail eingerichtet haben, können Sie sich mit dieser Methode anmelden. Im Anschluss können Sie Ihre Einstellungen im Verwaltungsbereich von Q-global bzw. Q-interactive „Central“ ändern.

Ich teile mir ein Benutzerkonto mit Kollegen, jedoch kann nur eine E-Mail-Adresse bzw. eine Handynummer hinterlegt werden. Was soll ich tun?
Jeder Benutzer benötigt für Q-global und Q-interactive eine eigene Lizenz mit persönlichen Login-Daten. Es ist aus datenschutzrechtlichen Gründen nicht erlaubt, die eigenen Benutzerkonto-Daten weiterzugeben oder das Benutzerkonto zu teilen und damit Unbefugten Einsicht in die Daten von Testpersonen zu gewähren.
Die einzelnen Lizenzen können Sie in unserem Webshop erwerben.

Warum muss ich mich bei jedem Login mit der Zwei-Faktor-Authentifizierung anmelden?
Bei Anwendungen, die sensible personenbezogene Daten speichern, dient die Zwei-Faktor-Authentifizierung als weiterer Schutzmechanismus dieser Daten, der den Zugriff Unbefugter verhindern soll.

Ist die Zwei-Faktor-Authentifizierung identisch mit der zweistufigen Authentifizierung und der zweistufigen Verifizierung?
Ja. Es gibt mehrere Begriffe für die gleiche Authentifizierungsmethode, wie beispielsweise zweistufige Authentifizierung, zweistufige Verifizierung oder Multi-Faktor-Authentifizierung.

Warum hat sich Pearson für die Implementierung der Zwei-Faktor-Authentifizierung für Q-global und Q-interactive entschieden?
Pearson hat auf diesen beiden digitalen Plattformen eine Zwei-Faktor-Authentifizierung implementiert, um die erhöhten Anforderungen an die Sicherheit gemäß der Datenschutzgrundverordnung DSGVO zu erfüllen. Die DSGVO ist eine EU-Rechtsvorschrift, die ab 25. Mai 2018 in Kraft tritt und eine strikte Authentifizierung erfordert, um den Schutz personenbezogener Daten innerhalb der EU zu gewährleisten. Die Zwei-Faktor-Authentifizierung wurde gemäß der Empfehlung von AAL2 (Authenticator Assurance Level 2) NIST 800-63B entwickelt und vom Gesetzgeber als ein zufriedenstellender Weg zur Erfüllung der Authentifizierungsanforderungen angesehen.

Stand: 14. Mai 2018

Ihr Kontakt zu uns: Pearson Beratungsservice | Tel.: 069/756 146-17/-25/-32 | beratungsservice.de@pearson.com