1 Privacy Policy: SecuIAM GO (english)

This privacy policy sets out how the app provider will treat users' personal data. If you do not agree to the terms of this policy, please do not install or use the app.

1.1 THE APP PROVIDER

OEDIV SecuSys GmbH
Brückenweg 5
18146 Rostock

Further details about the app provider can be found in the Legal Notice on our website:
http://www.secusys.de/impressum

1.2 PERSONAL DATA

This app has been designed to collect as little personal data as possible. It collects only the data required for the app to function correctly.

1.2.1 DATA COLLECTION AND STORAGE

The app needs to collect the following data in order to function properly:

- The device ID is collected and temporarily stored each time the app is launched.
- The device name is collected by the device management system and transmitted to the specified server.
- In order to ensure the correct language is used, the user language setting is checked each time the app is launched, and this is also transmitted to the requested website.
- The server address is stored after initialisation and thereafter used as the start address for the in-app browser.
- Optionally, the username for logging on to the SecuIAM Web Portal can be stored locally.

As soon as a connection to a website has been made, the terms of that website's privacy policy apply. In order to create the connection, the necessary data (e.g. the user's IP address) is passed to the website requested.

Please note:
OEDIV SecuSys GmbH does not collect any data during installation of the app; the installation process does not require users to register with us. App store operators may collect data in the course of app installation; this is something over which we have no control. We therefore recommend that you read your app store's Privacy Policy carefully.
Local data storage: Username, server address and cookies are stored locally. Use of the download function will result in the downloaded data (e.g. documents) also being stored on the device. No log data is written to the mobile device.
Locally stored data is retained permanently until the app is uninstalled. Downloaded files are stored in the selected directory.

1.2.2 DATA TRANSFERS TO THIRD PARTIES

We will never pass your data to third parties for any purpose whatsoever.

As part of the normal functioning of the software, data will be transferred to the relevant SecuIAM database.

1.3 SECURITY

The software will prompt for passwords. Password rules are defined on the SecuIAM server by the user's company and the app will check that these are complied with.

The SecuIAM administrator can block the user in the SecuIAM system and/or adjust their permissions so that access via the app is no longer possible.

Integrated website call-up: the SecuIAM Web Portal is called up via an integrated web browser.

1.4 PERMISSIONS ENABLED

In order to function properly the app requires the following permissions on the user's mobile device:

- Device identification: access required for dual authentication.
- Internet: access required for initialisation. Use of the app functions willl require a permanent internet connection.
- Local memory: access required for the storage of username and server address.
- SD card: write access to the SD card is required for the download function.

The user's rights to delete and correct data:

The user has the right to delete the app at any time, together with all associated data on the device. It is not possible to delete or correct data in the associated database, as this would defeat the purpose of the app.
A different approach is used for data deletion in the associated database, in line with legal and/or corporate requirements.

1.5 CONTACT

For more information about this app, please contact OEDIV SecuSys GmbH. Contact details can be found in our Legal Notice. Please send any data protection queries to privacy@secusys.de.

Privacy policy version: 27.05.2020

2 Datenschutzerklärung: SecuIAM GO (deutsch)

Diese Datenschutzerklärung erläutert, wie der Anbieter der App mit personenbezogenen Daten der Nutzer umgeht. Wenn Sie mit dieser Datenschutzerklärung nicht einverstanden sind, sollten Sie die App nicht installieren und nicht nutzen.

2.1 ANBIETER DER APP

OEDIV SecuSys GmbH
Brückenweg 5
18146 Rostock

Nähere Angaben zum Anbieter finden Sie im Impressum der Webseite:
http://www.secusys.de/impressum

2.2 PERSONENBEZOGENE DATEN

Diese App ist so konzipiert, dass so wenig personenbezogene Daten wie möglich erhoben werden. Grundsätzlich werden nur Daten erhoben, die für die technische Funktionsfähigkeit der App erforderlich sind.

2.2.1 DATENERHEBUNG UND -SPEICHERUNG

Für die Nutzung der App-Funktionen ist die Erhebung folgender Daten erforderlich:

- Die Geräte-ID wird bei jedem App-Start ermittelt und zwischengespeichert.
- Der Gerätename wird zur Geräteverwaltung ausgelesen und an den angegebenen Server übermittelt.
- Zur korrekten Sprachausgabe wird bei jedem Starten der App die Benutzersprache abgeprüft und auch an die aufgerufene Webseite übermittelt.
- Die Serveradresse wird nach der Initialisierung gespeichert und danach als Startadresse für den In-App-Browser verwendet.
- Der Username kann optional für die Anmeldung am SecuIAM Web Portal lokal gespeichert werden.

Sobald auf Webseiten verlinkt wird, gelten die Bestimmungen der dortigen Datenschutzerklärung:
Für den Aufbau der Verbindung werden die erforderlichen Daten (z.B. die IP-Adresse des Nutzers) an den Dienst weitergegeben.

Hinweise:
Die OEDIV SecuSys GmbH erhebt bei der Installation der App keine Daten; eine Anmeldung bei der OEDIV SecuSys GmbH ist nicht erforderlich. Möglicherweise erheben die App-Store-Betreiber bei der Installation Daten; hierauf hat die OEDIV SecuSys GmbH keinen Einfluss. Wir bitten deshalb um Beachtung der Datenschutz-Hinweise des genutzten App Store.
Lokale Datenspeicherung: Der Nutzername, die Serveradresse und Cookies werden lokal gespeichert. Bei Nutzung der Downloadfunktionalität werden die heruntergeladenen Dateien (z. B. Dokumente) ebenfalls auf dem Gerät hinterlegt. Auf dem mobilen Gerät erfolgt keine Logschreibung.

Die lokal gesicherten Daten werden bis zur Deinstallation der App dauerhaft gespeichert. Heruntergeladene Dateien bleiben im gewählten Verzeichnis erhalten.

2.2.2 DATENÜBERMITTLUNG AN DRITTE

Es erfolgt keine Datenübertragung an Dritte, z.B. zur Erstellung von Nutzungsprofilen auf der Basis von Nutzungsdaten für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung von Telemedien unter Pseudonym.

Als Softwarefunktionalität werden Daten an die entsprechende bi Cube Datenbank übertragen.

2.3 SICHERHEIT

Als Softwarefunktionalität werden Passwörter abgefragt. Die Passwortrichtlinien werden auf dem SecuIAM Server vom Unternehmen festgelegt, müssen erfüllt sein und werden geprüft.

Der jeweilige SecuIAM Administrator kann den Nutzer im SecuIAM System sperren bzw. die Berechtigungen so anpassen, dass der Zugriff über die App nicht mehr möglich ist.

Eingebundener Webseitenaufruf: Das SecuIAM Web Portal wird über einen integrierten Web-Browser aufgerufen.

2.4 FÜR DIE APP FREIGESCHALTETE BERECHTIGUNGEN

Für den ordnungsgemäßen Betrieb der App werden folgende Berechtigungen auf dem mobilen Gerät des Nutzers benötigt:

- Gerätekennung: Für die duale Authentifizierung benötigt die App Zugriff auf die Gerätekennung.
- Internetzugriff: Für die Initialisierung ist ein Internetzugriff zwingend erforderlich. Für die Nutzung der App-Funktionalitäten ist eine dauerhafte Verbindung zu einem SecuIAM Server erforderlich.
- Speicherzugriff: Für das Speichern von Nutzername und Serveradresse benötigt die App Zugriff auf den lokalen Speicher.
- SD-Kartenzugriff: Für die Nutzung der Downloadfunktionalität ist schreibender Zugriff auf die SD-Karteninhalte erforderlich.

Rechte des Nutzers bezüglich Löschung, Berichtigung der Daten:
Der Nutzer hat jederzeit das Recht, die App und damit alle Daten auf dem Gerät zu löschen.
Eine Löschung und Berichtigung von Daten in der angeschlossenen Datenbank ist nicht möglich und unzulässig, da es der inhaltlichen Funktionalität der App widerspricht.
Die Datenlöschung in der angeschlossenen Datenbank erfolgt nach einem separaten Löschkonzept gemäß gesetzlichen oder unternehmerischen Vorgaben.

2.5 KONTAKT

Für Auskünfte zu dieser App können Sie sich stets an die OEDIV SecuSys GmbH wenden. Die Kontaktdaten finden Sie im Impressum.
Datenschutzfragen senden Sie bitte an datenschutz@secusys.de

Stand der Datenschutzerklärung: 27.05.2020