Installing the Authentication Application on Mobile Devices

INSTALLING THE AUTHENTICATION APPLICATION

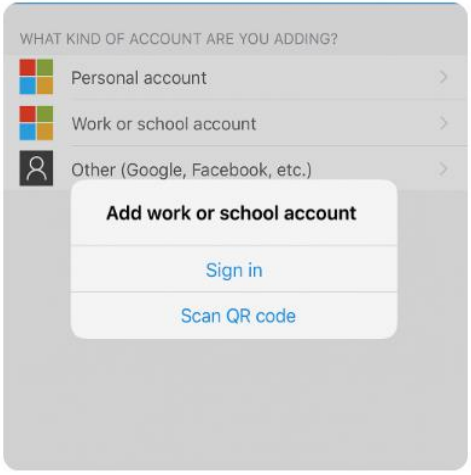
- Before setting up a password for the System, the User should install the Microsoft Authenticator application from Microsoft Corporation on their mobile device.
- The Microsoft Authenticator can be downloaded free of charge from:
- Play store for mobile devices with Android operating system
- AppStore for iOS mobile devices

The Microsoft Authenticator app supports multi-factor authentication for business and non-Microsoft accounts. Once the password is entered in the app, a second security layer is activated in the form of a generated code that constitutes the second login factor of the GPW DATA portal.

Key information

- Once you have installed the Microsoft Authenticator app on your mobile device (phone), launch it and select the account you want to use to verify the user - the default selection is: Business account.

  After selecting the account on the mobile device, a screen appears with the following message:



Key information

- In the next step, select the option Scan QR code.
- After selecting this option, you will be redirected to the camera screen.
- Point the camera at the QR code which appears on the Screen.
- A 6-digit code appears on the mobile device, which must be entered into the code field at the bottom of the Screen.

Key information

Note:

- The first login requires user authentication with MS Authenticator.
- Subsequent logins do not require user authentication with MS Authenticator.
- Multi-factor login is only required:

✓ at first login,

✓ on password reset,

✓ cyclically according to the currently adopted rules, i.e. every 30 days; the parameter can be modified to 30/60/90/360 days