



Quick guide to registering in the Customer Centre

Content

This guide gives a short overview of the functions of the Customer Centre at <https://www.igl-center.com>. The basic functions and menu items are shown in the form of screenshots and the individual functions are explained.

Registration

You will receive an invitation link to the e-mail address you have deposited with IGL Labor GmbH. Clicking on the link in the email will take you to the registration process. You will be guided through the process step-by-step and will need to assign a secure password as well as activate the two-factor authentication.

Step 1: Email verification

You will receive an email with a link to verify your email address:

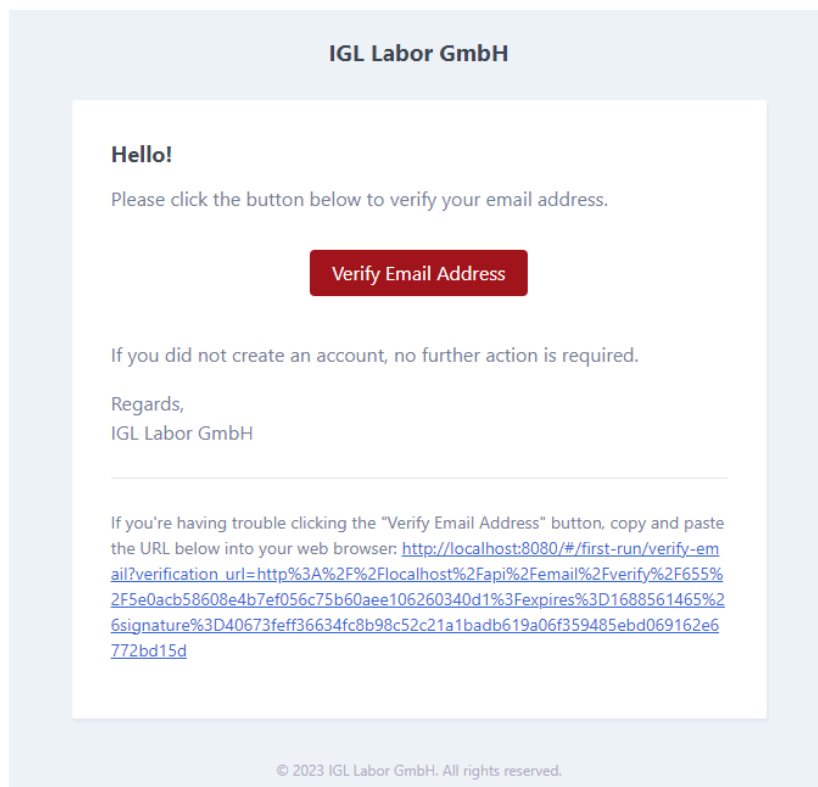



Figure 1: Verification email

Clicking the button or pasting the link will take you to the registration process:



Verify email address



Your email address was successfully verified. 

Figure 2: Email verification

You will automatically be forwarded to the next point.

Step 2: Assign user name and password

In this step, you define your user name and your secure password.




Set login data

Hello Mr. Friedrichsen

welcome to the customer center of IGL Labor GmbH.

This is your first login, so please set your username and a **strong** password.

Username

Password 


Password confirmation 

Figure 3: Set password

You will have to log in to the Customer Centre with the user name and password in future.

The secure password must fulfil the following conditions:

Password rules

Your strong password should:

- ✗ Be at least 8 characters long
- ✗ Contain uppercase and lowercase
- ✗ Contain numbers
- ✗ Contain special characters (!?\$%#...)
- ✗ Match with the confirmation

Figure 4: Password rules

The markings in front of the text serve as an indicator. These change when the corresponding condition is fulfilled:

Password rules

Your strong password should:

- ✓ Be at least 8 characters long
- ✓ Contain uppercase and lowercase
- ✓ Contain numbers
- ✓ Contain special characters (!?\$%#...)
- ✗ Match with the confirmation

Figure 5: Password rules indicators

Step 3: Activate two-factor authentication (2FA)

In this step you activate the 2FA for your access to the Customer Centre. The 2FA is an additional safeguard for your account in case your password is compromised. Each time you log in, you enter a six-digit sequence of numbers in addition to your login data (e-mail address and password), similar to a TAN in online banking.

Activating the 2FA is essential and a requirement for using the Customer Centre.

You can choose whether you want to receive the six-digit code by e-mail or by app:

Progress bar: 1. Verify email address (checked), 2. Set login data (checked), 3. 2-Factor-Authentication (2FA) (active), 4. Newsletter

2-Factor-Authentication (2FA)

☐ E-Mail ☐ App


 The two-factor-authentication is inactive. Choose one of the variants below.


Figure 6: Two-factor authentication

Select one of the two variants and click on the ACTIVATE 2FA button. A window will then appear for you to enter the password you have just given. After entering the password, you will either receive an e-mail with your code (e-mail variant) or a QR code will appear (app variant):

Progress bar: 1. Verify email address (checked), 2. Set login data (checked), 3. 2-Factor-Authentication (2FA) (active), 4. Newsletter

2-Factor-Authentication (2FA)

☐ E-Mail ☒ App

 Please scan this QR-code with an authenticator app on your smartphone.


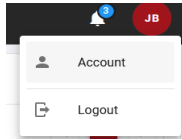


Figure 7: Two-factor authentication via app

If you prefer the app variant, we recommend the following apps for two-factor authentication: Google Authenticator, Microsoft Authenticator or Authy. Simply search for "Authenticator" in your App Store / Play Store.

When you log in for the first time, scan the QR code with your authentication app on your smartphone. You will then be shown the six-digit code which you enter in the fields below the QR code. For subsequent registrations, no new QR code will be displayed. Here you still use your app, in which the six-digit code to be entered for the respective use is displayed.



It is still possible to change the two-factor authentication from app to email or from email to app after the first login. This is done via "Settings" -> "Security" in the top right area of your account view.

Following the two-factor authentication, you will be shown recovery codes. Make a note of these codes (e.g. copy them into a file) and keep them safe. These codes will allow you to log in if you ever lose access to your device:

Recovery codes



Please note the following codes carefully and store them safely. You can use these codes to login, if you lose your smartphone or your authentication app is not working.

XYNSnZ18Jc-mDU6tV9mS9
JfDFaDBMn3-eD1SocteAb
CCsnX28suN-fXInCO28jP
ujszKtp61e-zBdRnhn1tK
tY8Zq0ynUW-iZmUILCeIE
BsmrpzkjMv-rdKukcgeIV
gKsfX7NpKb-htKuNb81B9
cZZ5942JXp-h2SOXmcKQY

☐ I have noted the codes and can access them at any time.

NEXT

Figure 8: Back up recovery codes

Note: Forgotten your password?

If you have **forgotten your password**, you can click on the "Forgotten password" link on the login page. There you enter your e-mail address and receive a link for resetting / reissuing your password.