



REQUIREMENTS AND CONDITIONS

Delegated administration in the Reporting Portal

FINANSINSPEKTIONEN

5/14/2024

Version 2.3



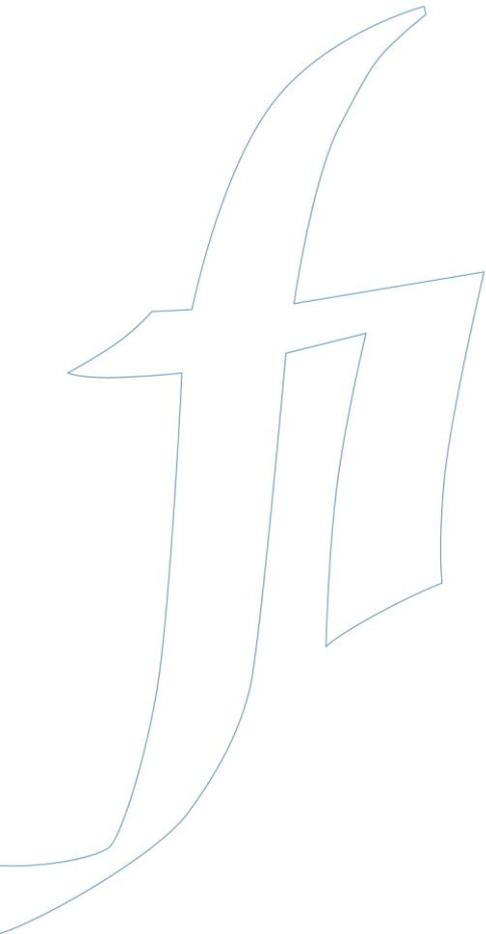


TABLE OF CONTENTS

Delegated administration	3
Registration in the authorisation system	3
Different types of users	3
Information from authorisation registration	4
Registration – New users	5
Login	6
Reporting by caregivers	6
Audit of authorisations	6
When using the Reporting Portal	7
User terms and conditions	7
Contact information	7

Delegated administration

Companies (legal persons) that are obligated to report to FI will now be able to delegate this task to specific (natural) persons. These persons are referred to as “rapporteurs”. An authorised signatory assigns the authorisations to relevant persons via a new system on FI’s website that has a secure log-in process.

This new procedure for the delegated administration of reporting is part of FI’s efforts to improve information security. This makes the reporting to Finansinspektionen more secure and more efficient.

REGISTRATION IN THE AUTHORISATION SYSTEM

Authorised signatories, business administrators and rapporteurs must start by completing the authorisation registration that is accessed via FI’s website. Instructions on how to complete this registration are available there as well.

The system identifies users with the help of e-identification (BankID or Mobilt BankID). Persons who do not have a Swedish personal ID number and thus cannot use BankID will use an SMS code (two-factor authentication) to log in. There is an extra level of security in that the user must not only log in using a User ID and password but also enter a pin code that is sent by SMS.

The new system is linked to the Swedish Tax Agency and retrieves correct information about persons with Swedish personal ID numbers as well as information about caregivers and children. The system is also linked to the Swedish Companies Registration Office, from which FI retrieves information about Swedish legal persons and CINs, an FI’s internal Institution Register, from which FI retrieves correct information about funds and Swedish fund management companies.

DIFFERENT TYPES OF USERS

Authorised signatory

An *authorised signatory* is able to both report to FI and assign or remove the authorisations for other natural persons holding the roles of *business administrator* or *rapporteur*.

Information about authorised signatories is retrieved from the Swedish Companies Registration Office's database. The authorised signatory is thus linked automatically to the legal person. Authorised signatories have the highest level of authorisation in the new system for delegated administration and can appoint business administrators and rapporteurs. Only Swedish or otherwise validated legal persons can have authorised signatories.

Business administrator

A business administrator can both report to FI and assign or withdraw authorisation for other natural persons acting as rapporteurs. Currently, authorisation can be assigned for PDMR Reporting or Periodic Reporting. More types of reporting will be added to the Authorisation Registration page in the future.

The role of business administrator is assigned via the Authorisation Registration page by the authorised signatory or, in exceptional cases, by an FI administrator.

If an authorised signatory or business administrator handles the reporting to FI, they do so in the role of rapporteur, and not in their role as authorised signatory or business administrator.

Rapportör eller ombud

Rapporteurs are entitled to report on behalf of themselves or a third party after having been assigned authorisation by an authorised signatory or business administrator. Authorised signatories and business administrators can appoint themselves to be rapporteurs.

INFORMATION FROM AUTHORISATION REGISTRATION

It is possible in Authorisation Registration to see what personal information FI has stored about the user and make some changes to the information the users themselves have entered the system.

An authorised signatory can change the information about a legal person to whom the authorised signatory is linked. This link is created automatically in the system or by an FI administrator.

Users can see the authorisations they have assigned and the authorisations they have received, as well as information about the legal persons to which they are linked and the role they hold for each company (legal person).

It is possible to inactivate the accounts (for individuals) that are no longer active. However, it is not possible to completely delete them from the system. This is because of the Archives Act, which requires all government authorities to save their archives. The identification step is part of the reports and registrations that are submitted to FI and therefore must be archived.

Protected personal information

For Swedish persons with protected personal information, according to the Swedish Tax Agency, is the information not retrieved or displayed in the system. If a disclosure request is made regarding information relating to individuals with protected personal information, such information may be subject to confidentiality, according to the Publicity and Confidentiality Act (2009:400).

Inactive accounts

A registered account (for individuals) that has not been used for 18 months is automatically deactivated. If an account has been deactivated, all permissions and authorizations are removed, but the account is automatically reactivated upon login. Permissions and authorizations must be delegated again. For an account to remain active, the person needs to log in at least once every 18 months.

Accounts that are no longer active will remain disabled after 18 months, they cannot be completely deleted from the system. This is because of the Archives Act (1990:782), which requires all government authorities to save their archives. The identification step is part of the reports and registrations that are submitted to FI and therefore must be archived.

Staff at FI can deactivate an account manually if the account holder wishes. It is the account holder themselves who must contact FI in this case.

REGISTRATION – NEW USERS

All users responsible for, or who will be assigned authorisation for, reporting to FI must start by completing the authorisation registration that is accessed via FI's website.

This registration is only required once; users create an account that they then use for logging in. After completing the authorisation registration, users receive a confirmation email with a link that they must click to verify the email address entered during registration. Users who do not have a Swedish personal ID number or BankID must register using their email address and mobile number.

Some foreign legal persons are not registered through the Swedish Companies Registration Office. They are instead registered in the portal through an authorised signatory, business administrator or rapporteur. If the authorised signatory cannot be verified and kept up-to-date automatically (via the Swedish Companies Registration Office), the highest level of authorisation for the company will be held by the business administrator. The business administrator for a newly registered foreign company that is not registered with the Swedish Companies Registration Office must currently be delegated by an FI administrator. The business administrator will then be able to appoint rapporteurs for the company.

Verification of company information and representatives

Information about companies and representatives that cannot be verified via the Swedish Companies Registration Office will be verified manually by FI. This applies primarily to foreign companies and persons who do not have a Swedish personal ID number. Contact reporting@fi.se for help verifying company information and the contact details of the company's representatives.

LOGIN

The Reporting Portal uses BankID, Mobilt BankID or two-factor authentication to identify users.

Users who do not have a Swedish personal ID number and thus cannot use BankID or Mobilt BankID must use two-factor authentication, which means that they must enter a pin code in addition to their UserID and password. The pin code is sent to the mobile telephone number the user entered when completing the authorisation registration. A new pin code is sent every time the user logs in. The password is sent via a verification email. Users who have forgotten their password must click on *Forgot password?* for help.

REPORTING BY CAREGIVERS

Children are occasionally subject to a reporting obligation. Their caregiver must then report on their behalf. Information about caregivers is not retrieved automatically; rather, the caregiver must request authorisation to report on behalf of the child. This authorisation is granted via FI's link to the Swedish Tax Agency or, if the child is not Swedish, by the parent registering the child.

Once the child turns 18, the caregiver may no longer report on behalf of the child. The 18-year-old must then log in to his/her account using BankID or Mobilt BankID.

AUDIT OF AUTHORISATIONS

FI strongly recommends that the signatory or company administrator at least once a year review the rights distributed to legal entities (authorisations), to ensure that the correct information is given to the correct individual.

WHEN USING THE REPORTING PORTAL

All traffic between users' computers and FI's systems are encrypted for security reasons. This is also why all activity in the Reporting Portal is registered and saved.

The system should not be used as an alternative channel for other storage or distribution of information. It is therefore important that authorisations for persons who have terminated their employment or changed positions be removed immediately.

The use of e-identification is the equivalent of identification in a traditional, physical environment, i.e. using a driver's license or a passport. It is therefore of utmost important that unauthorised persons are prevented from being able to give the appearance of being the holder of the e-identification. Report any misuse to FI.

USER TERMS AND CONDITIONS

FI handles sensitive information. Secure use of information is a prerequisite for the authority's activities.

FI recommends the following rules for users of the Reporting Portal:

- Computers should be locked when users no longer are able to monitor them.
- Mobile telephones should have a pin code and the telephone lock should be time-activated.
- Passwords for two-factor authentication should be changed immediately following any suspicions of misuse.
- Log-in information may not be shared with other users

CONTACT INFORMATION

For questions or help, contact Finansinspektionen.

reporting@fi.se

Telephone hours: M-F 9 a.m. - 11 a.m., +46 8 408 980 37



Finansinspektionen
Box 7821, 103 97 Stockholm
Besöksadress Brunnsgatan 3
Telefon +46 8 408 980 00
Fax +48 8 24 13 35
finansinspektionen@fi.se

www.fi.se