TERMS AND CONDITIONS OF FINGERPRINT AUTHENTICATION IN THE CODE APP

Users can also log into Nordea's Mobile Bank app and Netbank by using the fingerprint authentication in the code app. To do this, users must accept these additional terms and conditions supplementing the identification data. The use of the fingerprint authentication is voluntary and it does not restrict the use of other identification data.

When the user has activated the fingerprint authentication in the code app, logging into Netbank or Mobile Bank is possible with the user's fingerprint instead of a code. Some of the services, such as confirmation of payments or transfers to other accounts than the user's own, still require the use of another authentication method (PIN code etc.) accepted by the service. The fingerprint authentication in the code app cannot be used to identify the user via Nordea's e-identification service in services offered by a third party.

The fingerprint authentication is based on technology used by the manufacturer of the device and Nordea cannot process fingerprint data or control them.

The user can log into Netbank or Mobile Bank with all fingerprints saved in the mobile device before the activation of the function. This is why the user must ensure that only his/her fingerprint has been saved in the device before activating the fingerprint authentication. All other fingerprints must be deleted from the device before the function is activated.

All actions made by using fingerprint authentication bind the user as Nordea's customer.

If the device's fingerprint authentication function does not identify the user's finger, he/she must log into the service with another authentication method (PIN code etc.) accepted by the service.

Nordea has the right at any time without a separate notification to prevent login with the fingerprint authentication function to one or more services or block the use of the function altogether.

The customer must confirm the activation of the fingerprint authentication in the code app with another authentication method accepted by the code app (PIN code etc.).

If fingerprints are added to the fingerprint authentication function of the device, the fingerprint authentication in the code app must be activated again. If fingerprints are deleted, the user must, in some devices, also activate the fingerprint authentication in the code app again.

The fingerprint authentication in the code app can be deactivated in the following ways:

- By deactivating the fingerprint authentication function in the code app's settings. After this, the fingerprint authentication function can no longer be used in the code app. As the use of the fingerprint authentication is still possible in other apps, such as Mobile Bank, the function must be separately deleted from these.
- By deleting the fingerprint authentication from the settings of the device in which the fingerprint authentication has been installed. After this, the fingerprint authentication can no longer be used on the device in question.

In addition to these terms and conditions, the following will be applied to the use of the fingerprint authentication:

- General agreement terms and conditions governing services with access codes and [link]
- Instructions on the safe use of access codes [link]