

TERMS AND CONDITIONS

These terms and conditions for Aktia Mobile Bank (hereafter "Aktia Mobile Bank" or "the service") are in addition to the general terms of contract applied to the online bank agreement and use of the online bank and online banking codes as well as the identification service. The customer commits to following the terms regarding the service and the general terms of contract mentioned above as well as following the instructions for use, safety and other instructions in the service. If the terms and conditions conflict with the general terms of contract for the Online bank, these terms and conditions for Aktia Mobile Bank are applied primarily.

Aktia Mobile Bank is a mobile service maintained by Aktia Bank Ltd (hereafter "Aktia" or "the bank"), which enables Aktia's customer to use the Online bank and functions for daily banking with a mobile device. The customer can use the Online bank with a mobile device for which Aktia has published an application intended for using the service. A mobile device in these terms and conditions means a smart phone or another distance communicator that is suited for use of the service.

Version 2.0 of Aktia Mobile bank is an update which expands the functionality of the service and enables confirming banking transactions with a PIN code, fingerprint, face recognition or another biometric identification without a key code card.

With the update, Aktia Mobile bank becomes a tool for strong electronic identification mentioned in the online banking agreement. With Aktia Mobile Bank the consumer customer can identify themselves also in another service using strong electronic identification as stated in the Act of Strong Electronic Identification and Electronic Signatures (7.8.2009/617) (hereafter "strong electronic identification").

If the consumer customer uses Aktia Mobile Bank for strong electronic identification in another service provider's service, on legal consequences of using the identification method and on the obligations and responsibilities between the consumer customer and the service provider that uses a separate identification service which is offered by the bank, the agreement between the consumer customer and service provider, of which Aktia is not a party, is applied.

The service is enabled by installing Aktia Mobile Bank on a mobile device which uses the iOS or Android operating system from the device's official application store and by confirming the enabling with Aktia's Online banking codes.

The service is in use when the customer next logs into Aktia Mobile Bank. The contract of service is effective until further notice.

The customer must keep the PIN code defined in the service with care so that other persons cannot misuse the service. The PIN code cannot be told to others, not even persons in the same family, or written down in an easily identifiable format nor be kept in a mobile device. When keying in the PIN code the customer must protect the keyboard e.g. with his or her hand so that nobody else has the possibility to obtain the PIN code.

The customer can log in to Aktia Mobile Bank also with the fingerprint identification on a mobile device and/or with face recognition (hereafter together as "biometric identification"). Biometric identification means that a person's identity is verified with the help of the user's physical features, such as a fingerprint or facial features. By enabling this function, the customer can identify him or herself in the service with biometric identification details instead of the PIN code.

It is voluntary to use biometric identification in the service and does not limit using other identification methods, such as the PIN code.

Another identification method which the service accepts, such as the PIN code, still needs to be used when using some functions. The customer also needs to confirm enabling biometric identification in the service with another identification method accepted by the service.

Biometric identification is based on technology used in the customer's mobile device. Aktia does not have access to the biometric details saved onto the customer's device and Aktia can therefore not handle or administer biometric details. It also depends on the manufacturer and device whether biometric identification can be enabled on a mobile device.

The customer can log in to the service with all the biometric identification details saved onto the device before enabling the function. Due to this reason, the customer must ensure that no fingerprints and/or facial recognition details by other users have been saved onto the device. Fingerprint and facial recognition details by all other users must be deleted from the device before enabling the function. If facial recognition is used as a identification method, to protect his or her customer details and to prevent misuse of the service, the user cannot let another person use the mobile device.

All actions completed using biometric identification are binding to the customer.

If the function enabling biometric recognition does not verify the customer's fingerprint and/or facial features, the customer must log in to the service with another identification method which the service accepts, such as the PIN code.

Aktia always has the right to, without separate notification, stop the login onto the service or some functionalities in the service using biometric identification.

Biometric identification meant for using Aktia's service cannot be used for identification in third party services.

The customer must keep his or her mobile device so that outsiders cannot use Aktia Mobile Bank. The mobile device must be protected with a personal key code or with a key lock.

The customer is responsible for keeping and using the online banking codes as stated in the general terms of contract for the Online bank. What is stated about the online banking codes is applied to a mobile device using a PIN code or biometric identification. The customer is responsible for unauthorized use of the online banking codes if he or she has handed the codes over to another person or if the codes have been made available to another person due to the customer's negligence. The customer is also responsible for unauthorized use if he or she without unjustified delay has neglected to inform the bank about misplacing the codes, about if the codes unjustly have been made available to another person or about unauthorized use of the codes.

Aktia is at any given time entitled to change the contents of the service, its availability and the requirements for devices and applications needed for using the service. Aktia is also at any given time entitled to change the terms and conditions of the service.