NB! *These rules apply to service agreements, within which an account with letters "**RIKO**" (LVxx**RIKO**xxxxxxxxxxx) in number is opened, managed or serviced, or which specify that primarily an account with such a number is to be used for settlement. In any case these rules apply to any service agreement that contains a reference to these terms.*

(D)

Luminor Bank AS
EASY LOGIN SERVICE RULES

APPROVED
Edition of 24.11.2015, by the decision of the Management Board of AS DNB banka,
dated 25.11.2015
Effective from 02.12.2015

The Easy Login Service is a service of the Bank that allows a Customer who is a User of the Bank's Internetbank (hereinafter referred to as the "System") to access the System and use certain Services from the Mobile Application, using the PIN Code of Mobile Application for verifying their identity and approving orders and other Messages (hereinafter referred to as the "Easy Login Service").

The User may apply for the Easy Login Service if an Agreement on the Use of Means of Remote Access Instruments (hereinafter referred to as the "Agreement") has been concluded between the User as the Customer, and the Bank.

These rules (hereinafter referred to as the "Rules") shall regulate the legal relationship between the User and the Bank as related to the Easy Login Service.

The legal relations between the User and the Bank as related to the Easy Login Service shall also be subject to the provisions of the Agreement, unless these Rules specify otherwise.

Unless specified otherwise in these Rules, the terms and definitions used in the Rules shall correspond to the terms and definitions used in the Bank's Rules on Use of Remote Access Instruments (hereinafter referred to as the "Rules on Use of Remote Access Instruments").

To commence using the Easy Login Service, the User shall, in accordance with the procedure specified by the Bank, create a PIN Code of Mobile Application and use the System to register the relevant mobile device with which the User will be using the System (hereinafter referred to as the "Mobile Device").

With the PIN Code of Mobile Application, the User shall receive access to the following Services:

- viewing information available at System about Account balance, Accounts and linked payment cards, the last 10 (ten) Payments made from an Account and received on an Account, and other information specified by the Bank;

- approving Payment Orders which the User has included in the list of allowed Payments. The User shall approve the list of allowed Payments with appropriate Means of Identification which the User uses in accordance with the Rules on Use of Remote Access Instruments, in order to prove their identity and approve Notices within the System (such as their Login Name, Login Password, identification code from the Code Card, or an identification code generated by the Code Calculator) (hereinafter referred to as "Means of Full Authentication");

- sending the Customer's name, surname or company name and Account number to the e-mail address specified by the User.

The PIN Code of Mobile Application should not be easy to guess for anyone. The User shall store their Mobile Device and PIN Code of Mobile Application securely, preventing access by third parties. The User shall memorise the PIN Code of Mobile Application, and may not write it down in any way, including within the Mobile Device itself.

It is recommended that the User install automatic locking of the Mobile Device screen when idle (e.g. by setting up an access code), ensuring that third parties are unable to access functions of the Mobile Device or the Mobile Application. Prior to transferring (e.g. selling or gifting) the Mobile Device to a third

party, the User shall register with the System the fact that use of the relevant Mobile Device is being discontinued, verifying this using Means of Full Authentication.

If the Mobile Device has been lost, stolen or otherwise become accessible to a third party, or if the User suspects that it will become accessible to a third party, if a third party has found out the PIN Code of Mobile Application, or if the User suspects that this has happened, the User shall immediately notify the Bank by calling the Bank at 1880 or +371 6717 1880, or some other telephone number previously provided by the Bank for this purpose, or by submitting a written application at a Place of Service during the Bank's Working Hours. In such cases, the User may themselves block the use of the Mobile Device that has become accessible to a third party for use of the Easy Login Service.

The Bank shall be entitled to, without warning the User in advance, block the PIN Code of Mobile Application due to security concerns (e.g. if the Bank suspects that the System is being used by a third party via Mobile Application).

The Bank shall be entitled to block the PIN Code of Mobile Application and prohibit its use if, upon connecting to the System, the PIN Code of Mobile Application has been entered incorrectly five consecutive times. If the PIN Code of Mobile Application has been blocked, the User may unblock it in the System by logging in and verifying the unblocking using Means of Full Authentication.

The limit for Payments using the PIN Code of Mobile Application shall be EUR 300.00 per payment and EUR 1000.00 per day (both hereinafter referred to as "Limits"). The User may reduce the Limits specified by the Bank using procedures specified by the Bank. If any of the Limits exceeds the relevant System Use Limit specified in accordance with the Rules on Use of Remote Access Instruments, the relevant System Use Limit shall apply.

The Bank shall be entitled to unilaterally specify what Services are accessible to the User using the PIN Code of Mobile Application. The Bank shall be entitled to restrict or discontinue provision of the Easy Login Service without prior notice to the User.

If the User has verified their identity for the Easy Login Service using the PIN code of Mobile Application, no Login Name shall be necessary for accessing Services available using Means of Full Authentication.

The Arrangement between the User and the Bank regarding use of the Easy Login Service (hereinafter referred to as the "Arrangement") shall come into force once the User consents to these Rules and creates a PIN code of Mobile Application, verifying these activities within the System using Means of Full Authentication.

The Arrangement and the Rules shall constitute integral part of the Agreement.

The Bank shall be entitled to amend these Rules unilaterally in accordance with the General Terms and Conditions.

The User shall be entitled to discontinue use of the Easy Login Service at any time by submitting the notification to the Bank at any Place of Service or within the System.