Attālinātās pieejas līdzekļu noteikumi

Rules of Remote Access Instruments

Redakcija spēkā no 01.11.2018.

Version effective as of 01.11.2018

1. NOTEIKUMOS LIETOTIE TERMINI

Ja vien nav noteikts citādi, minētajiem terminiem ir šāda nozīme:

1.1. **Attālinātās pieejas līdzekļi** – Digitālie kanāli un Attālinātā apkalpošana.
1.2. **Attālinātā apkalpošana** – Pakalpojums, kura ietvaros Lietotājam ir iespēja veikt darījumus attālināti, ļaujot to paveikt bez vienlaicīgas Bankas pārstāvja un Lietotāja klātbūtnes.
1.3. **Autentifikācijas līdzekļi** – elementi, kas, ievērojot Bankas noteikto kārtību, sniedz iespēju veikt personas autentifikāciju un/vai pārbaudīt konkrētā maksājuma instrumenta, tostarp personalizēto autentifikācijas datu, izmantošanas derīgumu, piemēram, lietotāja (klienta) numurs, ieejas vārds, kods, parole, tālruņa numurs, iekārtas dati (piemēram, sērijas numurs, IMEI numurs), personas dati (piemēram, vārds, uzvārds, personas kods), tostarp biometrijas dati (piemēram, pirkstu nospiedumi, sejas digitālais attēls, acs varavīksnenes attēls, balss ieraksts u.c.), kā arī elektroniskais paraksts (elektroniskie dati var ietvert jebkuru no uzskaitītajiem elementiem un/vai citus elektroniskos datus), drošs elektroniskais paraksts u.c.
1.4. **Konts** – atbilst definīcijai Bankas Pakalpojumu noteikumos, kas reglamentē kontu uzturēšanu.
1.5. **Lietotājs:**
1.5.1. fiziska persona, kas ir Konta turētājs;
1.5.2. fiziska persona, kuru Konta turētājs saskaņā ar Noteikumiem pilnvaro lietot Attālinātās pieejas līdzekļus piekļūšanai Konta turētāja Kontam.
1.6. **Konta turētājs –** Klients, kura Kontam piekļūst, izmantojot Attālinātās pieejas līdzekļus.
1.7. **Līgums –** Pakalpojumu līgums (vienošanās) starp Līdzējiem par Attālinātās pieejas līdzekļu lietošanu.
1.8. **Noteikumi** – šie Attālinātās pieejas līdzekļu noteikumi.
1.9. **Attālinātās pieejas līdzekļa limits** – maksimālā viena tāda darījuma summa, kas veikts, izmantojot vienu vai vairākus Attālinātās pieejas līdzekļus (maksājuma limits), vai maksimālā šādu darījumu summa diennaktī (dienas limits).
1.10. **Rīkojums** – jebkurš ar Pakalpojuma saņemšanu saistīts Lietotāja un/vai Konta turētāja rīkojums (arī maksājuma rīkojums), pieteikums, pieprasījums vai cits paziņojums.
Termini, kuri lietoti ar lielo sākumburtu, bet nav skaidroti šajos Noteikumos, ir skaidroti Luminor Vispārējos darījumu noteikumos. Citi termini atbilst to lietojumam normatīvajos aktos, kas reglamentē kredītiestāžu darbību un maksājumu pakalpojumu sniegšanu.

2. VISPĀRĪGIE JAUTĀJUMI

2.1. Noslēdzot Līgumu, Līdzēji vienojas savstarpējām attiecībām, kas izriet no Attālinātās pieejas līdzekļu lietošanas, piemērot Luminor Vispārējos darījumu noteikumus, Noteikumus un Cenrādi, kas kopā ar Līgumu veido pilnīgu vienošanos starp Līdzējiem par attiecīgo Pakalpojumu.
2.2. Atsauce uz dokumentu, noteikumiem vai nosacījumiem, kuru mērķis ir regulēt Attālinātās pieejas līdzekļu lietošanu (piemēram, "Attālinātās pieejas līdzekļu izmantošanas noteikumi", "Vispārīgie noteikumi pakalpojumiem, kas pieejami ar elektroniskās identifikācijas kodiem" u.c.), kas lietota jebkurā dokumentā, nozīmē atsauci uz šiem Noteikumiem, ciktāl šajos Noteikumos nav noteikts citādi.
2.3. Pakalpojumiem, kurus Klients izmanto, bet kas nav aprakstīti šajos Noteikumos, tiek piemēroti attiecīgie Pakalpojumu noteikumi.
2.4. Jautājumus, kas nav atrisināti šajos Noteikumos, Līdzēji risina Luminor Vispārējos darījumu noteikumos noteiktajā kārtībā. Luminor Vispārējie darījumu noteikumi piemērojami Līdzēju

1. DEFINITIONS AND INTERPRETATION

Unless otherwise provided, these terms have the following meanings:
1.1. **Remote Access Instruments** – Digital Channels and Remote Channel.
1.2. **Remote Channel** – a Service, within the scope of which the User is able to perform transactions remotely, without the simultaneous presence of Bank's representative and the User.
1.3. **Authentication Instruments** – elements, which in accordance with the procedures of the Bank enable to authenticate a person and/or verify validity of use of a specific payment instrument, including personalized authentication data, for example, user (customer) number, login, code, password, phone number, data of the device (for example, serial number, IMEI number), personal data (for example, name, surname, personal code), including biometric data (for example, fingerprints, digital image of the face, iris image, voice recording, etc.), as well as electronic signature (electronic data may constitute any of the aforementioned elements and/or other electronic data), secure electronic signature etc.
1.4. **Account** – corresponds to the definition of the Bank's Service Terms, which regulate maintenance of accounts;
1.5. **User**:
1.5.1. a natural person, which is an Account Holder;
1.5.2. a natural person, whom the Account Holder according to the Rules authorises to use Remote Access Instruments to access the Account Holder's Account;
1.6. **Account Holder** – the Customer, whose Account is accessed using Remote Access Instruments.
1.7. **Agreement** – a Service Agreement (contract) between Parties on the use of Remote Access Instruments;
1.8. **Rules** – these Rules of Remote Access Instruments;
1.9. **Remote Access Instrument Limit** – the maximum amount of the transaction made using one or more Remote Access Instruments (payment limit), or the maximum total amount of such transactions per day (daily limit).
1.10. **Order** – any order of the User and/or Account Holder related to reception of the Service (also a payment order), an application, a request or other notice.
The capitalized terms, which are not defined in these Rules, are defined in Luminor General Business Terms. Other terms correspond to their use in regulatory enactments regulating operation of credit institutions and provision of payment services.

2. GENERAL PROVISIONS

2.1. By concluding an Agreement, the Parties agree to apply to the mutual relationship arising from the use of Remote Access Instruments Luminor General Business Terms, Rules and the Price List, which together with the Agreement form a complete agreement between the Parties on the respective Service.
2.2. Any reference to a document, terms or conditions, the purpose of which is to regulate the use of Remote Access Instruments (for example, "Rules on Use of Remote Access Instruments", "General Terms on Services Accessible with Electronical Identification Codes" etc.), which is used in any document, means a reference to these Rules, unless otherwise provided in these Rules.
2.3. The Services, which are used by the Customer, but are not described in these Rules, are subject to the respective Service Terms.
2.4. The issues, which are not regulated in these Rules, shall be resolved by the Parties according to Luminor General Business Terms. Luminor General Business Terms are applicable to mutual

savstarpējām tiesiskajām attiecībām, kas saistītas ar Pakalpojumu, ciktāl Noteikumos nav noteikts citādi.
2.5. Noteikumi, kā arī to grozījumi ir publicēti Bankas tīmekļa vietnē un pēc Klienta pieprasījuma ir pieejami izdrukas veidā Bankas klientu apkalpošanas vietā tās darba laikā. Papildu noteikumi, kas attiecas uz konkrētu Attālinātās pieejas līdzekli un/vai Autentifikācijas līdzekli, var būt pieejami attiecīgā Attālinātās pieejas līdzekļa vidē un/vai Bankas tīmekļa vietnē. Lietotājam ir pienākums ievērot arī šādus papildu noteikumus.

2.6. Noteikumos sadaļu, punktu un citi virsraksti ir norādīti tikai ērtības nolūkos un neietekmē Noteikumu interpretāciju.

2.7. Bankas darbības uzraudzību atbilstoši kredītiestāžu darbību regulējošajiem normatīvajiem aktiem veic Eiropas Centrālā banka sadarbībā ar Finanšu un kapitāla tirgus komisiju (adrese: Kungu iela 1, Rīga, LV-1050; mājas lapa: www.fktk.lv).

3. ATTĀLINĀTĀS PIEEJAS LĪDZEKĻU LIETOŠANAS TIESĪBU PIEŠĶIRŠANA, APTURĒŠANA, IZMAIŅAS UN ANULĒŠANA

3.1. Lietotāja tiesību apjomu saņemt Pakalpojumus, izmantojot Attālinātās pieejas līdzekļus, nosaka Attālinātās pieejas līdzekļa lietošanas režīms.
3.2. Konta turētājs nosaka un maina katram Lietotājam Attālinātās pieejas līdzekļa lietošanas režīmu, iesniedzot Bankai pēc formas un satura pieņemamu pilnvaru vai šo pilnvarojumu fiksējot citā Bankas noteiktā dokumentā un/vai Digitālajā kanālā. Bankai ir tiesības pieprasīt, lai šāds pilnvarojums tiek iesniegts rakstveidā un/vai parakstīts Bankas pārstāvja klātbūtnē.

3.3. Lai noteiktu kārtību, kādā Lietotāji ir tiesīgi apstiprināt un iesniegt Bankai Konta turētāja vārdā jebkādu rīkojumu, kas saistīts ar Pakalpojuma saņemšanu, Banka var pieprasīt noslēgt papildu vienošanos. Lai mainītu šā punkta kārtībā noteiktās Lietotāja tiesības, Banka var pieprasīt noslēgt jaunu vienošanos.

3.4. Konta turētājs var apturēt un atjaunot apturētās, kā arī izbeigt Lietotājam piešķirtās Attālinātās pieejas līdzekļu lietošanas tiesības, iesniedzot Bankai attiecīgu rīkojumu. Bankai ir tiesības pieprasīt, lai šāds rīkojums tiek iesniegts rakstveidā un/vai parakstīts Bankas pārstāvja klātbūtnē.

3.5. Bankai ir tiesības apturēt Lietotāja tiesības lietot Attālinātās pieejas līdzekli šādos gadījumos:
3.5.1. Bankai kļuvuši zināmi draudi Konta turētāja naudas līdzekļu nelikumīgai izmantošanai;
3.5.2. Konta turētājs vai Lietotājs nepilda Līguma noteikumus;

3.5.3. Bankai ir radušās pamatotas šaubas par Lietotāja tiesībām saņemt Pakalpojumus Konta turētāja vārdā;
3.5.4. citos gadījumos saskaņā ar Luminor Vispārējiem darījumu noteikumiem.
3.6. Banka aktivizē, aptur, atjauno un izbeidz Lietotājam iespēju lietot Attālinātās pieejas līdzekļus saprātīgā termiņā pēc tam, kad izpildīti Noteikumos paredzētie nosacījumi. Lietotāja tiesības saņemt Pakalpojumus, izmantojot Attālinātās pieejas līdzekļus, kā arī izmaiņas tajās stājas spēkā ar brīdi, kad tās ir reģistrētas Bankas informācijas sistēmā.
3.7. Lietotājam, kurš nav Konta turētājs, ir tiesības jebkurā brīdī atteikties no tam piešķirtajām Attālinātās pieejas līdzekļa lietošanas tiesībām, rakstiski par to paziņojot Bankai.

4. ATTĀLINĀTĀS PIEEJAS LĪDZEKĻU LIETOŠANAS REŽĪMI

4.1. Lietotājs var lietot Digitālo kanālu vienā no šādiem režīmiem:

4.1.1. informatīvajā režīmā, kas paredz tiesības saņemt informāciju par Konta turētāja Kontiem un darījumiem tajos;

legal relationship of the Parties related to the Service to the extent the Rules do not provide otherwise.
2.5. The Rules, as well as amendments thereto are published on the Bank's website and upon Customer's request are available in the form of a printout in the Bank's customer service location during its office hours. Additional rules applicable to the specific Remote Access Instrument and/or Authentication Instrument, may be available in the environment of the respective Remote Access Instrument and/or on the Bank's website. The User is obliged to observe also such additional rules.
2.6. Headings of section, paragraphs and other headings in the Rules are indicated for convenience only and do not affect the interpretation of the Rules.
2.7. Supervision of the Bank activities in accordance with the regulatory enactments regulating activities of credit institutions is carried out by the European Central Bank in cooperation with the Financial and Capital Market Commission (address: Kungu iela 1, Riga, LV-1050, Latvia, homepage address: www.fktk.lv).

3. GRANTING, SUSPENDING, CHANGING AND ANNULLING THE USAGE RIGHTS OF REMOTE ACCESS INSTRUMENTS

3.1. The scope of User's rights to receive the Services using the Remote Access Instruments shall be determined by the mode of use of Remote Access Instruments.
3.2. The Account Holder shall determine and change the mode of use of a Remote Access Instruments for each User by submitting a power of attorney acceptable for the Bank by form and content or recording this authorisation in other document defined by the Bank and/or the Digital Channel. The Bank is entitled to request that such an authorisation is submitted in writing and/or signed in the presence of a representative of the Bank.
3.3. In order to determine the procedure, according to which Users are entitled to confirm and submit to the Bank on behalf of the Account Holder any order, which is related to reception of the Service, the Bank may request to conclude an additional agreement. In order to change the User rights defined according to this clause, the Bank may request to conclude a new agreement.
3.4. The Account Holder may suspend and restore suspended, as well as terminate the usage rights of Remote Access Instruments assigned to a User by submitting a respective order to the Bank. The Bank is entitled to request that such an order is submitted in writing and/or signed in the presence of a representative of the Bank.
3.5. The Bank shall be entitled to suspend the User rights to use a Remote Access Instrument in the following cases:
3.5.1. the Bank has learned about threats of illegal use of the Account Holder's money;
3.5.2. the Account Holder or the User does not fulfil provisions of the Agreement;
3.5.3. the Bank has reasonable doubts about the User's right to receive the Services on behalf of the Account Holder;
3.5.4. in other cases according to the Luminor General Business Terms.
3.6. The Bank shall activate, suspend, restore and terminate the User's possibility to use Remote Access Instruments within reasonable deadline after the conditions envisaged in the Rules are fulfilled. The User rights to receive the Services using Remote Access Instruments, as well as changes thereto shall enter into force, when those are registered in the Bank's information system.
3.7. The User, who is not an Account Holder, shall be entitled to waive the Remote Access Instrument usage rights at any time notifying the Bank thereof in writing.

4. MODES OF USE OF REMOTE ACCESS INSTRUMENTS

4.1. The User may use the Digital Channel in one of the following modes:
4.1.1. informative mode which envisages the right to receive information about the Account Holder's Accounts and transactions in these Accounts;

4.1.2. sagatavošanas režīmā, kas papildus Noteikumu 4.1.1. punktā minētajam paredz tiesības sagatavot maksājuma rīkojumus;
4.1.3. maksājumu režīmā, kas papildus Noteikumu 4.1.2. punktā minētajam paredz tiesības apstiprināt (autorizēt) un iesniegt maksājuma rīkojumus Bankai;
4.1.4. pilnajā režīmā, kas paredz tiesības izmantot visas attiecīgā Digitālā kanāla funkcijas, tostarp tās, kas minētas Noteikumu 4.1.3. punktā.
4.2. Ja Konta turētāja Konta numurā ir burti "NDEA" (LVxxNDEAxxxxxxxxxxxxx), Lietotājs var lietot Digitālo kanālu piekļuvei šādam Kontam vienā no šādiem režīmiem:

4.2.1. ierobežotajā (informatīvajā) režīmā, kas paredz tiesības izmantot visas attiecīgā Digitālā kanāla funkcijas, izņemot tiesības sagatavot, apstiprināt (autorizēt) un iesniegt maksājuma rīkojumus Bankai;
4.2.2. pilnajā režīmā, kas paredz Noteikumu 4.1.4. punktā noteiktās tiesības.
4.3. Lietotājs var lietot Attālināto apkalpošanu vienā no šādiem režīmiem:
4.3.1. ierobežotajā (limitētajā) režīmā, kas papildus Noteikumu 4.1.1. punktā minētajam paredz tiesības:
4.3.1.1. pieteikties un atteikties no Bankas noteiktiem Pakalpojumiem;
4.3.1.2. vienoties ar Banku par Bankas noteiktu Pakalpojumu līgumu grozījumiem;
4.3.1.3. veikt maksājumus starp Konta turētāja Kontiem, maksājumus Bankai, kā arī trešajai personai – Bankas sadarbības partnerim – uz tā Kontu saistībā ar Konta turētāja pieteiktajiem vai izmantotajiem Pakalpojumiem;
4.3.1.4. izmantot citus Bankas noteiktus Pakalpojumus.
4.3.2. pilnajā režīmā, kas papildus Noteikumu 4.3.1. punktā minētajam paredz tiesības sagatavot, apstiprināt (autorizēt) un iesniegt Rīkojumus Bankai.
4.4. Bankai ir tiesības vienpusēji noteikt, ka noteiktiem Attālinātās pieejas līdzekļiem ir pieejami viens vai vairāki šajos Noteikumos paredzētie lietošanas režīmi, nav lietošanas režīmu vai ir pieejami īpaši, no šiem Noteikumiem atšķirīgi lietošanas režīmi.
4.5. Lietotājam noteiktie lietošanas režīmi attiecas uz visiem Konta turētāja Kontiem. Konta turētājs var piešķirt Lietotājam tiesības saņemt tikai noteiktus Pakalpojumus un/vai rīkoties tikai ar noteiktiem Konta turētāja Kontiem, ja Banka šādu iespēju nodrošina un Banka tam piekrīt.
4.6. Ja Lietotājam ir noteikts konkrēts Attālinātās pieejas līdzekļa lietošanas režīms, Lietotājam nav tiesību saņemt un Bankai ir tiesības atteikties sniegt Pakalpojumu, kura saņemšanu attiecīgais lietošanas režīms neparedz.
4.7. Ja Lietotājam noteiktais Attālinātās apkalpošanas lietošanas režīms paredz plašākas tiesības, nekā tam pašam Lietotājam noteiktais Digitālā kanāla lietošanas režīms, Banka attiecībā uz konkrēto Lietotāju piemēro Digitālā kanāla lietošanas režīmu un ir tiesīga atteikties sniegt tādu Attālinātās apkalpošanas Pakalpojumu, kura saņemšanu neparedz Lietotājam noteiktais Digitālā kanāla lietošanas režīms.

5. ATTĀLINĀTĀS PIEEJAS LĪDZEKĻU FUNKCIONALITĀTE

5.1. Attālinātās pieejas līdzekļu funkcionalitāte (tostarp Pakalpojumu veids un apjoms, kas Lietotājam pieejams ar Attālinātās pieejas līdzekli) un pieejamība (tostarp Pakalpojumu sniegšanas laiks un ierobežojumi) noteikta attiecīgā Attālinātās pieejas līdzekļa vidē, attiecīgā Pakalpojuma noteikumos un/vai Bankas tīmekļa vietnē, kā arī pēc pieprasījuma šāda informācija ir pieejama Bankas klientu apkalpošanas vietā tās darba laikā. Lietotājam ir pienākums ievērot Bankas norādījumus Attālinātās pieejas līdzekļu un ar tiem pieejamo Pakalpojumu lietošanā.

5.2. Bankas noteiktos gadījumos Lietotājam ir tiesības,

4.1.2. drafting mode, which, in addition to provisions of clause 4.1.1 of the Rules, envisages the right to prepare payment orders;

4.1.3. payment mode, which, in addition to provisions of clause 4.1.2 of the Rules, envisages the right to confirm (authorise) and submit payment orders to the Bank;
4.1.4. full mode, which envisages the right to use all the functions of the respective Digital Channels, including those referred to in clause 4.1.3 of the Rules.
4.2. If the Account Holder's Account number contains letters "NDEA" (LVxxNDEAxxxxxxxxxxxxx), the User may use the Digital Channel for access to such an Account in one of the following modes:
4.2.1. restricted (informative) mode, which envisages the right to use all the functions of the respective Digital Channel, with the exception of the right to confirm (authorise) and submit payment orders to the Bank;
4.2.2. full mode, which envisages the rights under clause 4.1.4 of the Rules.
4.3. The User may use the Remote Channel in one of the following modes:
4.3.1. restricted (limited) mode, which, in addition to provisions of clause 4.1.1 of the Rules envisages the rights:
4.3.1.1.to apply for and opt out of the Services defined by the Bank;
4.3.1.2.to agree with the Bank on amendments to the Service Agreements defined by the Bank;
4.3.1.3.to make payments between Account Holder's Accounts, payments to the Bank, as well as to a third party – a Bank's cooperation partner – to its Account in relation to the Services applied for or used by the Account Holder;
4.3.1.4.to use other Services defined by the Bank.
4.3.2. full mode, which, in addition to provisions of clause 4.3.1 of the Rules envisages the rights to prepare, confirm (authorise) and submit Orders to the Bank.
4.4. The Bank shall be entitled to unilaterally set that for a particular Remote Access Instrument one or more usage modes defined in these Rules, no usage modes or special usage modes differing from these Rules are available.

4.5. The usage modes set for the User are applicable to all Accounts of the Account Holder. The Account Holder may grant the User the right to receive only certain Services and/or handle only certain Accounts of the Account Holder, if the Bank ensures such a possibility and the Bank agrees with this.
4.6. If a certain Remote Access Instrument usage mode is set for the User, the User shall not be entitled to receive and the Bank shall be entitled to refuse to provide the Service, the reception of which is not envisaged by the respective usage mode.
4.7. If the Remote Channel usage mode set for the User envisages more extensive rights than the Digital Channel usage mode set for the User, the Bank shall apply the Digital Channel usage mode with regard to the specific User and shall be entitled to refuse to provide such a Remote Channel Service, the reception of which is not envisaged by the Digital Channel usage mode.

5. FUNCTIONALITY OF REMOTE ACCESS INSTRUMENTS

5.1. The functionality (including the type and scope of Services, which is available to the User with a Remote Access Instrument) and availability (including the time and restrictions of provision of the Services) of Remote Access Instruments shall be determined in the environment of the respective Remote Access Instrument, in the Service Terms of the respective Service and/or on the Bank's website, as well as upon request such information is available in the Bank's customer service location during its office hours. The User shall be liable to observe instructions of the Bank in the use of Remote Access Instruments and Services available via them.
5.2. In the cases set by the Bank the User shall be entitled to

izmantojot Bankas noteiktus Attālinātās pieejas līdzekļus, saņemt trešo personu pakalpojumus. Gadījumā, ja, izmantojot Attālinātās pieejas līdzekļus, ir pieejami trešo personu pakalpojumi, Banka neatbild par šādu pakalpojumu netraucētu un/vai pareizu darbību, kā arī neatbild par zaudējumiem, kas radušies Konta turētājam un/vai Lietotājam saistībā ar šādu trešo personu pakalpojumu lietošanu.
5.3. Bankai un trešo personu pakalpojuma sniedzējiem, kuru pakalpojumi pieejami, izmantojot attiecīgo Attālinātās pieejas līdzekli, ir tiesības bez iepriekšējas paziņošanas vienpusēji izdarīt izmaiņas piedāvāto pakalpojumu klāstā, saturā un funkcionalitātē.

5.4. Lietotājs var lietot Attālinātās pieejas līdzekli, izmantojot savietojamu iekārtu un programmatūru, kuru nodrošina Lietotājs. Attālinātās pieejas līdzekļa funkcionalitāte un saturs var atšķirties atkarībā no programmatūras un/vai iekārtas, kas tiek izmantota, lietojot Attālinātās pieejas līdzekli.
5.5. Banka var noteikt konkrētus tehniskos parametrus, kuri Lietotājam jāievēro, lai izmantotu un/vai piekļūtu Attālinātās pieejas līdzekļiem. Piemēram, Banka var noteikt konkrētu tālruņa numuru vai tīmekļa adresi, kas izmantojama Attālinātās apkalpošanas Pakalpojuma saņemšanai; konkrētu tīmekļa vietnes, servera adresi, programmatūru, kas izmantojama Digitālā kanāla lietošanas nolūkā u.tml. Informācija par šādiem parametriem ir pieejama Bankas tīmekļa vietnē, kā arī pēc pieprasījuma Bankas klientu apkalpošanas vietā tās darba laikā.
5.6. Banka negarantē Lietotāja aprīkojuma un/vai datu saglabāšanas vai ielādes (eksporta/importa) atbalsta formāta savietojamību ar Attālinātās pieejas līdzekli.

5.7. Bankai ir tiesības jebkurā brīdī pārtraukt nodrošināt noteiktu Attālinātās pieejas līdzekli un/vai aizstāt vienu Attālinātās pieejas līdzekli ar citu. Bankai šādā gadījumā nav pienākuma nodrošināt identisku vai identiskas funkcionalitātes Attālinātās pieejas līdzekli.
5.8. Bankai ir tiesības bez iepriekšējas brīdināšanas mainīt Attālinātās pieejas līdzekļa funkcionalitāti un pieejamību.

6. PIEKĻUVES IEROBEŽOŠANA ATTĀLINĀTĀS PIEEJAS LĪDZEKĻIEM

6.1. Piekļuves ierobežošana Attālinātās pieejas līdzeklim nozīmē, ka Lietotājam ir pilnībā vai daļēji ierobežota iespēja saņemt Pakalpojumu, izmantojot vienu vai vairākus Attālinātās pieejas līdzekļus.
6.2. Bankai ir tiesības nekavējoties ierobežot piekļuvi Attālinātās pieejas līdzeklim šādos gadījumos:
6.2.1. Konta turētājs vai Lietotājs neievēro Līguma noteikumus;

6.2.2. Konta turētājs 3 (trīs) kalendāros mēnešus pēc kārtas nav izmantojis nevienu no Attālinātās pieejas līdzekļiem;
6.2.3. tiek slēgti visi Konta turētāja Konti vai Attālinātās pieejas līdzekļiem piesaistītais Konts;
6.2.4. Attālinātās pieejas līdzekļa programmatūras modernizēšanas, sistēmas ekspluatācijas izmaiņu vai citos līdzīgos gadījumos;
6.2.5. ja aprīkojums, programmatūra vai datu pieslēgumi, kurus izmanto Lietotājs, apdraud Attālinātās pieejas līdzekļa drošību un/vai darbību;
6.2.6. tehnisku traucējumu gadījumos;
6.2.7. ja pastāv risks, ka Banka, tās klienti vai trešās personas var ciest zaudējumus Attālinātās pieejas līdzekļu pakalpojuma sniegšanas rezultātā;
6.2.8. ja Bankai ir aizdomas par neautorizētu vai krāpniecisku Attālinātās pieejas līdzekļu izmantošanu;
6.2.9. notiek atkārtoti neveiksmīgi mēģinājumi lietot vienu vai vairākus Autentifikācijas līdzekļus;
6.2.10. tiek uzsākts Konta turētājs maksātnespējas process;

6.2.11. tiek apturēta Konta turētāja maksājumu izpilde Bankas

receive third-party services via Remote Access Instruments defined by the Bank. If third-party services are available via the Remote Access Instruments, the Bank is not responsible for undisturbed and/or correct operation of such services, as well as the Bank is not liable for the damages incurred by the Account Holder and/or the User in relation to the use of such third-party services.
5.3. The Bank and providers of a third-party service, whose services are available via the respective Remote Access Instrument, shall be entitled without prior notification to make amendments unilaterally to the range, content and functionality of offered services.
5.4. The User may use the Remote Access Instrument, using a compatible equipment and software, which the User shall provide. Functionality and content of a Remote Access Instrument may differ depending on software and/or equipment, which is used using Remote Access Instruments.
5.5. The Bank may set specific technical parameters, which the User shall observe to use and/or access the Remote Access Instruments. For example, the Bank may determine a specific phone number or website, which can be used to receive a Remote Channel Service; a specific website, server address, software, which shall be used for the purposes of use of a Digital Channel, etc. Information about such parameters is available on the Bank's website, as well as in the Bank's customer service location during its office hours.
5.6. The Bank does not guarantee compatibility of the User's equipment and/or data storage, upload or download (export/import) support format with the Remote Access Instrument.
5.7. The Bank shall be entitled to terminate the provision of a certain Remote Access Instrument and/or replace one Remote Access Instrument with another. In this case the Bank shall not be liable to ensure an identical Remote Access Instrument or identical functionality of the Remote Access Instrument.
5.8. The Bank shall be entitled to change the functionality and availability of the Remote Access Instrument without prior notification.

6. RESTRICTION OF ACCESS TO REMOTE ACCESS INSTRUMENTS

6.1. Restriction of access to a Remote Access Instrument means that the User has been fully or partially limited the possibility to receive the Service, using one or more Remote Access Instruments.
6.2. The Bank shall be entitled to restrict access to a Remote Access Instrument immediately in the following cases:
6.2.1. the Account Holder or the User does not comply with provisions of the Agreement;
6.2.2. the Account Holder has not used any Remote Access Instrument for 3 (three) calendar months in a row;
6.2.3. all the Account Holder's Accounts are closed or the Account linked to the Remote Access Instruments is closed;
6.2.4. modernisation of Remote Access Instrument software, system operation changes or in other similar cases;

6.2.5. if the equipment, software or data connections used by the User endanger safety and/or operation of a Remote Access Instrument;
6.2.6. in case of technical disturbances;
6.2.7. if there is a risk that the Bank, its customers or third parties may suffer losses as a result of provision of a Remote Access Instrument service;
6.2.8. if the Bank has suspicions about unauthorised or fraudulent use of Remote Access Instruments;
6.2.9. there are repeated unsuccessful attempts to use one or more Authentication Instruments;
6.2.10. insolvency proceedings of the Account Holder are initiated;
6.2.11. execution of Account Holder's payments is suspended in

Pakalpojumu noteikumos minētajos gadījumos;
6.2.12. iestājušies nepārvaramas varas apstākļi, līdz šie apstākļi un sekas, ko tie radījuši, ir novērstas.
6.2.13. tiek izbeigts Līgums;
6.2.14. citos gadījumos, kad saskaņā ar Luminor Vispārējiem darījumu noteikumiem Bankai ir tiesības vienpusēji atkāpties no Pakalpojumu līguma.
6.3. Piekļuvi Attālinātās pieejas līdzeklim var atjaunot, ja vairs nepastāv apstākļi, kas bijuši par pamatu piekļuves ierobežošanai.

7. AUTENTIFIKĀCIJAS LĪDZEKĻI, LIETOTĀJA AUTENTIFIKĀCIJA UN DARĪJUMA AUTORIZĀCIJA

7.1. Lietotāju, kurš vēlas izmantot Attālinātās pieejas līdzekli, Banka pēc tās ieskatiem autentificē ar vienu vai vairākiem Autentifikācijas līdzekļiem. Lai veiktu darījumu (tostarp iesniegtu Rīkojumu izpildei, apstiprinātu līgumu), izmantojot Attālinātās pieejas līdzekli, Lietotājs šādu darījumu autorizē ar Autentifikācijas līdzekli.
7.2. Bankai ir tiesības jebkurā brīdī pieprasīt Lietotājam atkārtoti autentificēties vai atkārtoti autorizēt darījumu (tostarp Rīkojumu) ar to pašu vai citu Autentifikācijas līdzekli. Bankai ir tiesības pieprasīt un Lietotājam šādā gadījumā ir pienākums veikt autentifikāciju un/vai darījuma autorizāciju ar Autentifikācijas līdzekli, kuru nosaka Banka vai par kuru vienojušies Līdzēji.

7.3. Lai izmantotu Autentifikācijas līdzekli, Lietotājam var būt nepieciešams uzstādīt noteiktu programmatūru un/vai lietot noteiktu iekārtu. Bankai ir tiesības noteikt prasības šādai programmatūrai un iekārtai, kā arī jebkurā brīdī šādas prasības mainīt, tostarp noteikt, ka Autentifikācijas līdzekļa izmantošanai ir nepieciešama konkrēta programmatūra un/vai iekārta. Lietotājs šo prasību izpildi nodrošina uz sava rēķina.
7.4. Bankai ir tiesības noteikt, ka noteiktu Pakalpojumu saņemšanai un/vai noteiktu darījumu (Rīkojumu) autorizēšanai ir izmantojami noteikti Autentifikācijas līdzekļi, programmatūra un/vai iekārtas. Tāpat Bankai ir tiesības noteikt, ka, izmantojot noteiktu Autentifikācijas līdzekli, ir pieejami noteikti Pakalpojumi un/vai pieejamo Pakalpojumu funkcionalitāte ir ierobežota un/vai atšķirīga, tostarp ir atšķirīgi Attālinātās pieejas līdzekļa limiti.

7.5. Ja Autentifikācijas līdzekli, iekārtu un/vai programmatūru, kas rada, reģistrē, pārbauda un/vai veic citas darbības saistībā ar Autentifikācijas līdzekli, izsniedz Banka, Lietotājs to var saņemt pēc tam, kad ir izpildīti Noteikumos paredzētie nosacījumi. Konta turētājs maksā Bankai Cenrādī norādīto maksu par šāda līdzekļa, iekārtas un/vai programmatūras nodrošināšanu, ja Līdzēji nevienojas citādi.
7.6. Ja Autentifikācijas līdzekli, iekārtu un/vai programmatūru, kas rada, reģistrē, pārbauda un/vai veic citas darbības saistībā ar Autentifikācijas līdzekli, izsniedz trešā persona, Banka neatbild par to darbību un drošību, kā arī nesedz jebkādus zaudējumus, kas Lietotājam, Konta turētājam un/vai trešajai personai radušies saistībā ar šāda Autentifikācijas līdzekļa, iekārtas un/vai programmatūras lietošanu.
7.7. Ja Autentifikācijas līdzeklī izmantotos datus norāda Lietotājs, Lietotājam ir tiesības tos mainīt, iesniedzot Bankai paziņojumu Bankas noteiktā kārtībā.

7.8. Lietotāja autentifikācijai un darījuma (tostarp Rīkojuma) autorizācijai var izmantot tikai Bankas izsniegtu vai Bankas akceptētu Autentifikācijas līdzekli, iekārtu un/vai programmatūru, kas rada, reģistrē, pārbauda un/vai veic citas darbības saistībā ar Autentifikācijas līdzekli. Bankai ir tiesības jebkurā brīdī atteikties pieņemt vai pārtraukt jebkura Autentifikācijas līdzekļa, iekārtas un/vai programmatūras pieņemšanu vai izsniegšanu, kā arī noteikt Noteikumu 7.4. punktā paredzētos ierobežojumus, nepaskaidrojot iemeslu.

the cases referred to in the Bank's Service Terms;
6.2.12. force majeure event has set in, until these conditions and consequences thereof are eliminated.
6.2.13. the Agreement is terminated;
6.2.14. in other cases, when according to the Luminor General Business Terms the Bank is entitled to unilaterally withdraw from the Service Agreement.
6.3. Access to a Remote Access Instrument may be restored, if the conditions, which have been the basis for restriction of access, no longer exist.

7. AUTHENTICATION INSTRUMENTS, USER AUTHENTICATION AND TRANSACTION AUTHORISATION

7.1. The Bank authenticates the User, who wants to use a Remote Access Instrument, at its discretion by one or more Authentication Instruments. In order to execute a transaction (including submit an Order for execution, approve a contract) using a Remote Access Instrument, the User authorises such a transaction by an Authentication Instrument.
7.2. The Bank shall be entitled to request the User to authenticate repeatedly or to authorise a transaction (including an Order) repeatedly using the same or other Authentication Instrument. The Bank shall be entitled to request and in this case the User shall be liable to perform authentication and/or transaction authorisation using an Authentication Instrument, which is determined by the Bank or which was agreed between the Parties.
7.3. In order to use an Authentication Instrument, the User may need to install a certain software and/or use certain equipment. The Bank shall be entitled to set requirements to such a software and equipment, as well as change such requirements at any time, including to define that the use of an Authentication Instrument requires a specific software and/or equipment. The User shall ensure the fulfilment of these requirements on its expenses.
7.4. The Bank shall be entitled to define that certain Authentication Instruments, software and/or equipment must be used for reception of particular Services and/or authorisation of particular transactions (Orders). The Bank is also entitled to define that using a certain Authentication Instrument, certain Services are available and/or the functionality of available Services is limited and/or differ, including that Remote Access Instruments Limits are differ using a certain Authentication Instrument.
7.5. If the Authentication Instrument, equipment and/or software, which creates, registers, validates and/or performs other actions in relation to an Authentication Instrument, is issued by the Bank, the User may receive it after the conditions envisaged in the Rules are met. The Account Holder shall pay to the Bank the fee indicated in the Price List for provision of such an instrument, equipment and/or software, unless the Parties agree otherwise.
7.6. If the Authentication Instrument, equipment and/or software, which creates, registers, validates and/or performs other actions in relation to an Authentication Instrument, is issued by a third party, the Bank shall not be liable for their operation and security, as well as shall not be liable for any damages incurred by the User, Account Holder and/or a third party in relation to the use of such an Authentication Instrument, equipment and/or software.
7.7. If the data used in the Authentication Instrument are indicated by the User, the User shall be entitled to change them by submitting a notice to the Bank according to the procedure set by the Bank.
7.8. Only the Authentication Instrument, equipment and/or software, which creates, registers, validates and/or performs other actions in relation to an Authentication Instrument, issued by the Bank or accepted by the Bank can be used for User authentication and transaction (including Order) authorisation. The Bank shall be entitled at any time to refuse to accept or terminate acceptance or issuing of any Authentication Instrument, equipment and/or software as well as define the restrictions envisaged in clause 7.4 of the Rules without providing reasoning

7.9. Ja atbilstoši Autentifikācijas līdzekļa izmantošanas nosacījumiem to paredzēts nosūtīt uz Lietotāja iekārtu (piemēram, SMS koda nosūtīšana uz mobilo tālruni), tad Lietotājs ir atbildīgs par Bankai norādītā identifikatora, kas izmantojams šādas informācijas nosūtīšanai, (piemēram, tālruņa numura) pareizību. Ja Lietotājs maina iekārtu un/vai tās identifikatoru, Lietotājs par to nekavējoties paziņo Bankai. Kamēr šāds paziņojums nav saņemts, Banka turpina attiecīgā Autentifikācijas līdzekļa sūtīšanu, izmantojot Bankas rīcībā esošo identifikatoru. Šādā gadījumā Banka neatbild par Konta turētājam, Lietotājam un/vai trešajām personām radītajiem zaudējumiem.

7.10. Bankai ir tiesības pieprasīt un Lietotājam šādā gadījumā ir pienākums nomainīt Autentifikācijas līdzekli pret Bankas norādītu Autentifikācijas līdzekli un/vai nomainīt Autentifikācijas līdzeklī izmantotos datus.
7.11. Lietotājam, kurš izmanto Autentifikācijas līdzekli, ir pienākums ievērot attiecīgā Autentifikācijas līdzekļa lietošanas nosacījumus, kā arī tā izsniedzēja norādījumus, tostarp nodrošināt savietojamu iekārtu un/vai programmatūru Autentifikācijas līdzekļa sekmīgai pielietošanai, kā arī ievērot šādas iekārtas un/vai programmatūras ražotāja un/vai izsniedzēja noteikumus un norādījumus.
7.12. Bankai ir tiesības atteikt Pakalpojuma sniegšanu, izmantojot Attālinātās pieejas līdzekļus, ja Lietotājs neizpilda šīs sadaļas nosacījumus.
7.13. Ja piekļuvei Attālinātās pieejas līdzeklim un/vai jebkura darījuma (tostarp Rīkojuma) un/vai līguma autorizācijai (parakstīšanai) ir sekmīgi izmantots Autentifikācijas līdzeklis, uzskatāms, ka Lietotājs, kuram attiecīgais Autentifikācijas līdzeklis atbilst (ir piederīgs, reģistrēts, izsniegts, atrodas tā lietošanā u.tml.), šādu dokumentu (piekļuves dokumentu, darījuma dokumentu, līgumu u.tml.) ir parakstījis pašrocīgi (tostarp elektroniskais dokuments, kurš parakstīts ar Autentifikācijas līdzekli – elektronisko parakstu –, atbilstoši Elektronisko dokumentu likumam uzskatāms par parakstītu pašrocīgi). Šāds dokuments (tostarp Rīkojums) ir saistošs Konta turētājam, Lietotājam un Bankai.
7.14. Ja Lietotājs, izmantojot Attālinātās pieejas līdzekli, iesniedz maksājuma rīkojumu, Bankai ir tiesības pieprasīt Lietotājam un/vai Konta turētājam to atkārtoti autorizēt Bankas noteiktā kārtībā.
7.15. Bankai ir tiesības neizpildīt Rīkojumu arī šādos gadījumos:

7.15.1. Lietotājs un/vai Konta turētājs neievēro Attālinātās pieejas līdzekļu lietošanas kārtību, Līgumu, Noteikumus un/vai citus Bankas Pakalpojumu noteikumus;
7.15.2. Lietotājs un/vai Konta turētājs pēc Bankas pieprasījuma nav atkārtoti apstiprinājis Rīkojumu;
7.15.3. Bankai radušās aizdomas par Lietotāja identitāti un/vai gribas īstumu, un Bankai nav izdevies sazināties ar Konta turētāju, lai apstiprinātu Rīkojuma saturu;
7.15.4. citos gadījumos, kas paredzēti Bankas Pakalpojumu noteikumos, kas attiecas uz Pakalpojumu, kuru Lietotājs vēlas saņemt, izmantojot Attālinātās pieejas līdzekļus;
7.15.5. Kontā nav pietiekams daudzums naudas līdzekļu Rīkojuma izpildei un samaksai par sniegtajiem Pakalpojumiem;
7.15.6. Rīkojums ir neskaidrs vai izkropļots sakaru traucējumu dēļ;
7.15.7. Bankai ir radušās aizdomas par prettiesisku darbību veikšanu;
7.15.8. ja saskaņā ar Līdzēju vienošanos Rīkojuma izpildei nepieciešams vairāku Lietotāju apstiprinājums;
7.15.9. šādas tiesības paredzētas Luminor Vispārējos darījumu noteikumos, attiecīgā Pakalpojuma noteikumos vai normatīvajos aktos.
7.16. Visa informācija, ko Banka sniedz, izmantojot Attālinātās pieejas līdzekļus, ir saistoša Lietotājam un Konta turētājam un pielīdzināma Bankas parakstītam dokumentam.

thereof.
7.9. If according to the conditions of the use of the Authentication Instrument, it is envisaged to be sent to the User's equipment (for example, sending an SMS code to a mobile phone), then the User shall be responsible for the correctness of the identifier provided to the Bank, which is used for sending of such information (for example, a phone number). If the User changes the equipment and/or its identifier, the User shall notify the Bank thereof immediately. Until such a notice is received, the Bank continues sending of the respective Authentication Instrument, using the identifier available to the Bank. In such a case, the Bank shall not be liable for any damages incurred by the Account Holder, the User and/or third parties.
7.10. The Bank shall be entitled to request and in this case the User shall be liable to replace the Authentication Instrument with the Authentication Instrument indicated by the Bank and/or change the data used in the Authentication Instrument.
7.11. The User which uses an Authentication Instrument, shall be liable to observe usage conditions of the respective Authentication Instrument, as well as issuer's instructions, including to ensure compatible equipment and/or software for successful use of the Authentication Instrument, as well as to observe rules and/or instructions of the manufacturer and/or issuer of such equipment and/or software.
7.12. The Bank shall be entitled to refuse to provide a Service using Remote Access Instruments, if the User does not fulfil conditions of this section.
7.13. If an Authentication Instrument has been successfully used to access a Remote Access Instrument and/or authorise any transaction (including Order), it is considered that the User, whom the respective Authentication Instrument corresponds (belongs, is registered, has been issued, is at its disposal etc.), has signed such document (access document, transaction document, agreement etc.) in person (including that the electronic document which is signed by an Authentication Instrument – electronic signature –, according to Law on Electronic Documents shall be considered to have been signed by hand). Such a document (including Order) is binding on the Account Holder, the User and the Bank.
7.14. If the User, using a Remote Access Instrument, submits a payment order, the Bank shall be entitled to request the User and/or the Account Holder to reauthorise it according to the procedure set out by the Bank.
7.15. The Bank shall be entitled to decline execution of an Order in the following cases:
7.15.1. the User and/or Account Holder does not observe the procedure of use of Remote Access Instruments, the Agreement, the Rules and/or other Service Terms of the Bank;
7.15.2. the User and/or Account Holder has not reconfirmed the Order upon Bank's request;
7.15.3. the Bank has suspicions about the User's identity and/or authenticity of intention, and the Bank did not succeed to contact the Account Holder to confirm the content of the Order;
7.15.4. in other cases, envisaged in the Bank's Service Terms, which are applicable to the Service the User wants to receive using Remote Access Instruments;
7.15.5. the Account has insufficient amount of money to execute an Order and pay for the provided Services;
7.15.6. the Order is unclear or distorted due to faulty communications;
7.15.7. the Bank suspects illegal actions;

7.15.8. if according to the agreement between the Parties the execution of the Order requires a confirmation of several Users;
7.15.9. such rights are envisaged in Luminor General Business Terms, Service Terms of the respective Service or in regulatory enactments.
7.16. All the information provided by the Bank using Remote Access Instruments, is binding on the User and the Account Holder and is equivalent to a document signed by the Bank.

7.17. Ja Lietotājs izmanto Autentifikācijas līdzekļus, lai piekļūtu vai saņemtu trešo personu pakalpojumus, Banka neatbild par šādiem pakalpojumiem, kā arī neatlīdzina zaudējumus, kas Lietotājam, Konta turētājam un/vai trešajai personai radušies saistībā ar šādu pakalpojumu lietošanu vai šādu trešo personu darbību vai bezdarbību.

8. ATTĀLINĀTĀS PIEEJAS LĪDZEKĻA LIMITS

8.1. Bankas noteiktos gadījumos Konta turētājs var noteikt Attālinātās pieejas līdzekļa limitu, noslēdzot ar Banku vienošanos. Ja vienošanās nav noslēgta, tiek piemērots Bankas noteiktais Attālinātās pieejas līdzekļa limits.
8.2. Informācija par Attālinātās pieejas līdzekļa limitu ir pieejama attiecīgajā Digitālajā kanālā, Bankas tīmekļa vietnē vai Bankas klientu apkalpošanas vietā tās darba laikā.
8.3. Bankai ir tiesības noteikt, ka maksājumu rīkojumu izpilde no viena vai vairākiem Kontiem, izmantojot Attālinātās pieejas līdzekli, ir iespējama tikai pēc tam, kad Līdzēji ir noslēguši vienošanos par Attālinātās pieejas līdzekļa limitu.
8.4. Banka nepieņem un/vai neizpilda maksājuma rīkojumu, ja, izpildot šādu maksājuma rīkojumu, tiktu pārsniegts Attālinātās pieejas līdzekļa limits.
8.5. Attālinātās pieejas līdzekļa limits netiek piemērots šādiem darījumiem, kas veikti, izmantojot Digitālo kanālu:
8.5.1. maksājuma rīkojumam par termiņnoguldījuma veikšanu vai papildināšanu (izņemot gadījumu, ja Lietotājs šāda maksājuma rīkojuma iesniegšanai izmanto kādu no Digitālajā kanālā speciāli maksājumu veikšanai paredzētajām tiešsaistes formām);
8.5.2. maksājuma rīkojumam trešo personu rēķinu automātiskai apmaksāšanai saskaņā ar vienošanos starp Līdzējiem;
8.5.3. maksājuma rīkojumam, kas iesniegts Bankai, izmantojot Digitālā kanāla sadaļā "Ziņojumi" pieejamo tiešsaistes formu;
8.5.4. maksām, kuras Banka noraksta no Konta turētāja Konta saistībā ar tādu maksājuma rīkojumu izpildi, kas iesniegti Bankai Digitālajā kanālā;
8.5.5. maksājuma rīkojumam par maksājuma veikšanu uz jebkuru Konta turētāja Kontu Bankā, ja maksājuma rīkojums tiek iesniegts Bankai, izmantojot Digitālā kanāla sadaļā "Valūtas maiņa" vai "Maksājums uz savu kontu" pieejamo tiešsaistes formu;
8.5.6. citiem maksājuma rīkojumiem, ja par to Līdzēji panākuši vienošanos.
8.6. Bankai ir tiesības jebkurā brīdī vienpusēji mainīt Attālinātās pieejas līdzekļa limitu, kuru noteikusi Banka vai par kuru Līdzēji iepriekš vienojušies.

9. AUTOMATIZĒTI PAKALPOJUMI

9.1. Ja Banka piedāvā Pakalpojumu, kas ietver maksājuma rīkojumu automātisku iepriekšēju aizpildīšanu un/vai citus automatizētus tehnoloģiskus risinājumus (šajos Noteikumos – **Automatizēts Pakalpojums**) un kas pieejams, izmantojot Bankas noteiktu Attālinātās pieejas līdzekli, Lietotājs ir atbildīgs, ka tā informācija un/vai dokumenti, kas iesniegti Bankai Automatizēta Pakalpojuma saņemšanas nolūkā, ir salasāmi, pareizi un pilnīgi.
9.2. Lietotājam ir pienākums pārbaudīt visu informāciju, kas sagatavota un/vai automātiski aizpildīta Automatizēta Pakalpojuma rezultātā (tostarp informāciju par maksājumu kontu, no kura un uz kuru paredzēts veikt maksājumu, maksājuma rīkojuma detaļas, maksājuma summu u.c.) pirms darījuma, kas izveidots ar Automatizēta Pakalpojuma starpniecību, autorizācijas.
9.3. Bankai nav pienākuma un tā neuzņemas atbildību pārbaudīt Automatizēta Pakalpojuma rezultāta pareizību, precizitāti un/vai atbilstību Lietotāja sniegtajai informācijai šāda Pakalpojuma saņemšanas nolūkā.
9.4. Šajos Noteikumos paredzētajā kārtībā autorizējot jebkuru darījumu (tostarp Rīkojumu), kas izveidots ar Automatizēta Pakalpojuma starpniecību, Lietotājs apstiprina un apliecina, ka informācija, kas sagatavota un/vai automātiski aizpildīta

7.17. If the User uses Authentication Instruments to access or receive third-party services, the Bank shall not be responsible for such services, as well as shall not compensate damages, which the User, the Account Holder and/or a third party incurred in relation to the use of such services or activity or inactivity of such third parties.

8. REMOTE ACCESS INSTRUMENT LIMIT

8.1. In the cases defined by the Bank the Account Holder may set a Remote Access Instrument Limit by concluding an agreement with the Bank. If no agreement is concluded, the Remote Access Instrument Limit set by the Bank is applicable.
8.2. Information about the limit of the Remote Access Instrument is available in the respective Digital Channel, Bank's website or Bank's customer service location during its office hours.
8.3. The Bank may be entitled to define that execution of payment orders from one or more Accounts, using a Remote Access Instrument, is possible only when the Parties have concluded an agreement on Remote Access Instrument Limit.
8.4. The Bank shall not accept and/or shall not execute a payment order, if, when executing such a payment order, the Remote Access Instrument Limit would be exceeded.
8.5. The Remote Access Instrument Limit is not applicable to the following transactions made via a Digital Channel:
8.5.1. to a payment order on making or supplementing a term deposit (with the exception of the cases, when in order to submit such a payment order the User uses any online form specifically intended for the payments in the Digital Channel);
8.5.2. to a payment order for automatic payment of third-party invoices according to the Agreement between the Parties;
8.5.3. to a payment order submitted to the Bank, using the online form available in the "Reports" section of the Digital Channel;
8.5.4. to the fees debited by the Bank from the Account Holder's Account in relation to execution of payment orders, which were submitted to the Bank via a Digital Channel;
8.5.5. to a payment order on making a payment deposit to any Account Holder's Account at the Bank, if the payment order is submitted to the Bank, using the online form available in Section "Currency exchange" or "Payment to own account" if the Digital Channel;
8.5.6. to other payment orders, if the Parties have reached an agreement about this.
8.6. the Bank shall be entitled to unilaterally change the Remote Access Instrument Limit, which was defined by the Bank or on which the Parties have previously agreed.

9. AUTOMATED SERVICES

9.1. If the Bank offers a Service, which includes automatic pre-filling of payment orders and/or other automated technological solutions (in these Rules – **Automated Service**) and which is available via a Remote Access Instrument defined by the Bank, the User shall be responsible that information and/or documents submitted to the Bank for the purpose of receiving an Automated Service, are readable, correct and complete.
9.2. The User shall be liable to check all the information prepared and/or automatically filled as a result of an Automated Service (including information about the payment account, from which and to which the payment is intended, details of the payment order, payment amount etc.), before authorising transaction which was created through mediation of an Automated Service.
9.3. The Bank shall not be liable and it shall not undertake responsibility to verify the correctness, accuracy and/or compliance of the Automated Service result with the information provided by the User for the purposes of receiving such a Service.
9.4. When authorising any transaction (including an Order) according to the procedure set out in these Rules, which was created through mediation of an Automated Service, the User confirms and certifies that the information prepared and/or

Automatizēta Pakalpojuma rezultātā un/vai jebkurš cits Automatizēta Pakalpojuma rezultāts (tostarp maksājuma konta numurs, no kura un uz kuru paredzēts veikt maksājumu, izpildot attiecīgo maksājuma rīkojumu), ir pareizs un pilnīgs un Bankai ir tiesības šādu darījumu (tostarp Rīkojumu) izpildīt saskaņā ar attiecīgajam darījumam atbilstošajiem Bankas Pakalpojumu noteikumiem.
9.5. Banka neatbild par zaudējumiem, kas radušies Konta turētājam, Lietotājam un/vai trešajai personai saistībā ar kļūdainu, neprecīzu, nepilnīgu vai nepareizu Automatizēta Pakalpojuma rezultātu, tostarp Banka nav atbildīga par šādiem zaudējumiem, ja Lietotājs rezultātu apstiprinājis (darījumu autorizējis) Noteikumos paredzētajā kārtībā un Banka šādu darījumu izpildījusi.

9.6. Ja Automatizēta Pakalpojuma rezultāts var būt vai ir nesavietojams ar attiecīgajam darījumam piemērojamiem noteikumiem (piemēram, Automatizēta Pakalpojuma rezultātā automātiski aizpildīts maksājuma rīkojums satur rakstzīmes, kuras nav atļautas saskaņā ar šādam maksājuma rīkojumam piemērojamiem noteikumiem), Bankai ir tiesības, taču tas nav Bankas pienākums, aizstāt šādu Automatizēta Pakalpojuma rezultātu tādā veidā, lai nodrošinātu atbilstību attiecīgajam darījumam piemērojamiem noteikumiem un/vai atteikt Automatizēta Pakalpojuma sniegšanu.
9.7. Banka negarantē, ka Automatizēts Pakalpojums tiks sniegts nekavējoties pēc tā pieprasīšanas un/vai ierosināšanas.

10. ATBILDĪBA

10.1. Konta turētājs ir pilnībā atbildīgs par visiem darījumiem un Rīkojumiem (tostarp tādiem, kurus veicis vai devis Lietotājs, kas nav Konta turētājs), kas veikti, izmantojot Attālinātās pieejas līdzekļus (tostarp Automatizētus Pakalpojumus), un visu saistību izpildi, kuras izriet no šādiem darījumiem.

10.2. Lietotājam ir pienākums Autentifikācijas līdzekļus glabāt slepenībā atsevišķi vienu no otra un nepieļaut to vai informācijas par tiem nonākšanu trešo personu rīcībā, tostarp Lietotājam ir pienākums nodrošināt, ka programmatūra un iekārta, kas tiek izmantota autentifikācijas vai darījumu autorizācijas nolūkā nenonāk trešo personu rīcībā.

10.3. Ja programmatūra, kas tiek izmantota autentifikācijas vai darījumu autorizācijas nolūkā, ir uzstādīta uz noteiktas iekārtas, tad Lietotājam ir pienākums nodrošināt šādas iekārtas un programmatūras uzstādījumu nepieejamību trešajām personām. Ja šādu iekārtu nodod trešajai personai vai Lietotājs vēlas šādu programmatūru uzstādīt citai iekārtai, tad Lietotājam ir pienākums dzēst esošajā iekārtā uzstādīto programmatūru, kā arī citu iekārtā un/vai programmatūrā saglabāto informāciju, kas tiek izmantota autentifikācijas vai darījumu autorizācijas nolūkā.

10.4. Informācija par darījumiem ir pieejama Konta izrakstā atbilstoši Bankas noteikumiem, kas reglamentē Kontu uzturēšanu. Brīdī, kad Banka Konta izrakstu dara pieejamu Konta turētājam, uzskatāms, ka Konta turētājam ir kļuvusi zināma informācija par darījumiem, kas norādīti šajā Konta izrakstā.

10.5. Konta turētājam ir pienākums ne retāk kā vienu reizi kalendārajā mēnesī iepazīties ar Konta izrakstu un citiem Bankas paziņojumiem, kas saistīti ar veiktajiem darījumiem, un pārliecināties par to pareizību un atbilstību autorizētajiem darījumiem.
10.6. Lietotājs Bankas Maksājumu noteikumos noteiktajā kārtībā ziņo Bankai par maksājuma instrumenta (tostarp jebkura Autentifikācijas līdzekļa, informācijas par šādu Autentifikācijas līdzekli, kā arī programmatūras un/vai iekārtas, kas tiek izmantota autentifikācijas vai darījumu autorizācijas nolūkā) nozaudēšanu, nolaupīšanu vai citādi prettiesisku piesavināšanos, kā arī neautorizētu vai kļūdaini izpildītu maksājumu.
10.7. Gadījumos, kas nav paredzēti Noteikumu 10.6. punktā,

automatically filled as a result of an Automated Service and/or any other result of an Automated Service (including the payment account number, from which and to which the payment is intended by executing a respective payment order) is correct and complete and the Bank shall be entitled to execute such a transaction (including an Order) according to the Bank's Service Terms applicable to the respective transaction.
9.5. The Bank shall not be liable for the damages incurred by the Account Holder, the User and/or a third party in relation to an erroneous, inaccurate, incomplete or incorrect Automated Service result, including the Bank shall not be responsible for such damages, if the User has confirmed the result (authorised the transaction) according to the procedure defined in the Rules and the Bank has executed such a transaction.
9.6. If the Automated Service result can be or is incompatible with the rules applicable to the respective transaction (for example, a payment order filled automatically as a result of the Automated Service contains characters, which are not permitted according to the rules applicable to such a payment order), the Bank shall be entitled, yet not obligated to replace such an Automated Service result in such a way to ensure compliance with the rules applicable to the respective transaction and/or refuse the provision of the Automated Service.

9.7. The Bank shall not guarantee that the Automated Service will be provided immediately after being requested and/or initiated.

10. LIABILITY

10.1. The Account Holder shall be fully liable for all the transactions and Orders (including those executed or given by the User, who is not an Account Holder), which have been executed using Remote Access Instruments (including Automated Services), and the fulfilment of all the obligations arising from such transactions.
10.2. The User is obligated to store Authentication Instruments in secret separately from one another and to prevent that they or information about them comes into possession of third parties, including the User is obligated to ensure that the software and equipment, which is used for the purposes of authentication or transaction authorisation, does not come into possession of third parties.
10.3. If the software, which is used for the purposes of authentication or transaction authorisation, is installed on a certain equipment, then the User shall be obligated to ensure unavailability of such equipment and software settings to third parties. If such an equipment is transferred to a third party or the User wants to install such a software on another equipment, the User shall be obligated to delete the software installed on the existing equipment, as well as the information saved on the equipment and/or software, which is used for the purposes of authentication or transaction authorisation.
10.4. Information on transactions is accessible through the Account statement pursuant to the Bank's rules that regulate maintaining the Account. As soon as the Bank makes the Account statement accessible to the Accout Holder, it is assumed that the Account Holder has become aware of information on transactions indicated therein.
10.5. The Account Holder is obliged to get acquainted with an Account statement and other Bank's notices, which are related to the transactions made, and to ascertain correctness of the transactions and their compliance with authorised transactions at least once within every calendar month.
10.6. The User shall inform the Bank according to the procedure defined in Bank's Payment Rules about loss, theft or other misappropriation of a payment instrument (including any Authentication Instrument, information about such an Authentication Instrument, as well as software and/or equipment, which are used for authentication or transaction authorisation), as well as unauthorised or incorrectly executed payment.
10.7. In the cases, which are not envisaged in clause 10.6 of the

Konta turētājam ir pienākums nekavējoties, tiklīdz Konta turētājs ir uzzinājis par nepareizu darījumu vai pamanījis citas kļūdas saistībā ar darījuma (tostarp Rīkojuma) izpildi, bet ne vēlāk kā 15 (piecpadsmit) dienu laikā pēc tam, kad Banka Noteikumu 10.4. punktā noteiktajā kārtībā ir darījusi pieejamu Konta izrakstu vai nosūtījusi citu dokumentu, kurā atspoguļota attiecīgā informācija, rakstveidā paziņot par to Bankai. Banka ir tiesīga uzskatīt, ka Konta turētājam nav iebildumu pret darījuma pareizību, ja šajā punktā noteiktajā termiņā pretenzija nav iesniegta. Pretenzijas, kas iesniegtas pēc noteiktā termiņa, Banka var noraidīt vai atteikties pieņemt.

10.8. Atbildība par maksājumiem, maksājumu izpildi, kā arī neautorizētiem maksājumiem, tostarp tādiem, kas veikti maksājuma instrumenta nozaudēšanas, nolaupīšanas vai citādas prettiesiskas piesavināšanās dēļ, paredzēta Bankas Maksājumu noteikumos.

10.9. Banka neatbild par zaudējumiem gadījumos, ja Autentifikācijas līdzekļi, programmatūra un/vai iekārta, kas tiek izmantota autentifikācijas vai darījumu autorizācijas nolūkā, nonāk trešo personu rīcībā, ja vien normatīvajos aktos nav paredzēts citādi.

10.10. Konta turētājam ir pienākums iepazīstināt Lietotāju, kas nav Konta turētājs, ar Līgumu, Cenrādi, Noteikumiem, Luminor Vispārējiem darījumu noteikumiem, kā arī tiem Pakalpojumu noteikumiem, kas attiecas uz Pakalpojumu, kuru, izmantojot Attālinātās pieejas līdzekļus, lieto šāds Lietotājs. Konta turētājs uzņemas atbildību par to, ka šāds Lietotājs ievēro iepriekš minētajos dokumentos noteiktos pienākumus.

10.11. Banka nav atbildīga par zaudējumiem, kas radušies Konta turētājam, Lietotājam vai trešajai personai arī šādos gadījumos:

10.11.1. Konta turētājs un/vai Lietotājs nav ievērojis Līgumu, Noteikumus, Luminor Vispārējos darījumu noteikumus vai citus Bankas Pakalpojumu noteikumus;

10.11.2. trešo personu prettiesiskas darbības rezultātā līdz brīdim, kad Noteikumos paredzētajā kārtībā Attālinātās pieejas līdzekļa darbība ir ierobežota, ja vien Lietotājs pats nav rīkojies prettiesiski;

10.11.3. Lietotāja izmantoto sakaru līdzekļu vai tehniskā aprīkojuma bojājumu vai traucējumu dēļ, kā arī gadījumos, ja tehnisku iemeslu dēļ Attālinātās pieejas līdzeklis, Autentifikācijas līdzeklis vai atsevišķas to funkcijas nav pieejamas;

10.11.4. Lietotājs nodevis iekārtu un/vai programmatūru, kas izmantojama autentifikācijas un/vai darījumu autorizācijas nolūkā, trešajai personai;

10.11.5. trešā persona, kuras pakalpojumi pieejami, izmantojot Attālinātās pieejas līdzekli, nepilda vai nepienācīgi pilda savas saistības, tostarp nesniedz vai nekvalitatīvi sniedz šādus pakalpojumus;

10.11.6. saskaņā ar Noteikumiem ir ierobežota piekļuve Attālinātās pieejas līdzeklim;

10.11.7. Lietotājs pārkāpis tam doto Konta turētāja pilnvarojumu;

10.11.8. Konta turētājs nav paziņojis Bankai par Lietotājam dotā pilnvarojuma (tostarp piešķirto lietošanas tiesību) izmaiņām, tostarp izbeigšanos.

10.12. Banka neatbild par zaudējumiem, kas radušies Konta turētājam, Lietotājam un/vai trešajai personai gadījumos, kad Banka izmanto šajos Noteikumos paredzētās tiesības.

10.13. Lietotājam ir pienākums nodrošināt, ka trešās personas nevar piekļūt Digitālajam kanālam, tostarp jebkuram Pakalpojumam, kas pieejams, izmantojot Digitālo kanālu.

11. LĪGUMA IZBEIGŠANA

11.1. Konta turētājam ir tiesības jebkurā brīdī izbeigt Līgumu, par to rakstveidā paziņojot Bankai. Banka pārtrauc attiecīgā Pakalpojuma sniegšanu 1 (vienas) Darba dienas laikā no paziņojuma saņemšanas brīža. Līguma izbeigšana neierobežo

Rules, the Account Holder is obliged to notify the Bank immediately, as soon as the Account Holder has learned about an incorrect transaction or noticed other errors in relation to the execution of a transaction (including Order), but no later than within 15 (fifteen) days after the Bank according to the procedure defined in clause 10.4 of the Rules has made available an Account statement or sent other document, where the respective information is reflected. The Bank shall be entitled to consider that the Accout Holder has no objections against the correctness of a transaction, if no claim has been submitted within the deadline set in this clause. The Bank may reject claims or refuse to accept claims submitted after the set deadline.

10.8. Liability for payments, execution of payments, as well as unauthorised payments, including those made due to loss, theft or other misappropriation of a payment instrument, is envisaged in the Bank's Payment Rules.

10.9. The Bank shall not be liable for damages in cases, when Authentication Instruments, software and/or equipment, which are used for authentication or transaction authorisation, come into possession of third parties, unless regulatory enactments provide otherwise.

10.10. The Account Holder is obligated to familiarise the User other than the Account Holder with the Agreement, the Price List, the Rules, Luminor General Business Terms as well as the Service Terms applicable to Services that such User is using by Remote Access Instruments. The Account Holder shall assume liability for the User's compliance with duties stipulated in the above documents.

10.11. The Bank shall not be liable for the damages incurred by the Account Holder, the User or the third party also in the following cases:

10.11.1. The Account Holder and/or the User has not observed the Agreement, the Rules, Luminor General Business Terms or other Service Terms of the Bank;

10.11.2. as a result of wrongful activities of third parties up to the moment, when the access to the Remote Access Instrument is restricted according to the procedure envisaged in the Rules, unless the User has acted illegally;

10.11.3. due to damages or interferences in the means of communication or technical equipment, as well as in the cases, when due to technical reasons a Remote Access Instrument, Authentication Instrument or individual functions thereof are not available;

10.11.4. the User has transferred equipment and/or software, which is used for the purposes of authentication and/or transaction authorisation, to a third party;

10.11.5. a third person, services of which are available via a Remote Access Instrument, does not fulfil or improperly fulfils its obligations, including does not provide such services or provides them in an inadequate quality;

10.11.6. access to Remote Access Instrument is restricted according to the Rules;

10.11.7. the User has violated the authorisation given to it by the Account Holder;

10.11.8. the Account Holder has not notified the Bank about changes in the authorisation (including granted usage rights) given to the User, including termination of such authorisation.

10.12. The Bank shall not be liable for the damages incurred by the Account Holder, the User and/or the third party in the cases, when the Bank exercises the rights envisaged in these Rules.

10.13. The User shall be liable to ensure that third parties cannot access the Digital Channel, including any Service, which is available via the Digital Channel.

11. TERMINATION OF THE AGREEMENT

11.1. The Account Holder may terminate the Agreement at any time, notifying the Bank thereof in writing. The Bank shall stop provision of the respective Service within 1 (one) Business Day from the time of receipt of the notification. Termination of the

Konta turētāja tiesības arī turpmāk saņemt Attālinātās apkalpošanas pakalpojumu, ievērojot Noteikumu nosacījumus.

11.2. Ja tiek izbeigts Līgums par konkrēta Attālinātās pieejas līdzekļa lietošanu, tas neizbeidz Līgumu par cita Attālinātās pieejas līdzekļa lietošanu, ja vien Līdzēji nevienojas citādi. Tāpat šādā gadījumā Banka neveic darbības, lai dzēstu programmatūru, kas izmantojama autentifikācijas nolūkā. Šādas darbības Lietotājs veic pats uz sava rēķina.
11.3. Ja normatīvajos aktos nav noteikts citādi, Bankai ir tiesības jebkurā brīdī vienpusēji atkāpties no Līguma un/vai pārtraukt Pakalpojuma sniegšanu, Konta turētājam, kurš ir patērētājs, par to paziņojot vismaz 2 (divus) mēnešus iepriekš. Citos gadījumos Banka par atkāpšanos paziņo saprātīgā termiņā. Ja Bankai saskaņā ar normatīvajiem aktiem ir pienākums izbeigt darījuma attiecības, Banka ir tiesīga neievērot termiņus iepriekšējai brīdināšanai.

11.4. Ciktāl normatīvajos aktos nav noteikts citādi, Bankai ir tiesības nekavējoties vienpusēji atkāpties no Līguma bez iepriekšēja paziņojuma, ja Konta turētājs un/vai Lietotājs neievēro Līguma noteikumus un/vai piekļuve Attālinātās pieejas līdzeklim saskaņā ar Noteikumiem ir ierobežota, kā arī citos gadījumos, kas paredzēti Luminor Vispārējos darījumu noteikumos vai normatīvajos aktos.
11.5. Izbeidzot Pakalpojumu līgumu, Konta turētājam pēc Bankas pieprasījuma Bankas noteiktā termiņā jāsamaksā visas attiecīgajā Pakalpojumu līgumā un Cenrādī noteiktās un Bankas aprēķinātās maksas, kā arī jāizpilda citas no Pakalpojumu līguma izrietošās saistības.

12. NOTEIKUMU GROZĪJUMU STĀŠANĀS SPĒKĀ

12.1. Noteikumus un Cenrādi Banka groza Luminor Vispārējos darījumu noteikumos paredzētajā kārtībā.

12.2. Ja Klients, kas ir patērētājs, nepiekrīt ierosinātajiem Noteikumu un/vai Cenrāža grozījumiem, šādam Klientam ir tiesības līdz attiecīgo grozījumu spēkā stāšanās brīdim iesniegt Bankai rakstisku paziņojumu par Līguma izbeigšanu, ievērojot to, ka šādā gadījumā Klientam pēc Bankas pieprasījuma Bankas noteiktā termiņā jāsamaksā visas attiecīgajā Pakalpojumu līgumā un Cenrādī noteiktās un Bankas aprēķinātās maksas, kā arī jāizpilda citas no Pakalpojumu līguma izrietošās saistības. Ja Banka līdz Noteikumu vai Cenrāža grozījumu spēkā stāšanās dienai nav saņēmusi šajā punktā minēto rakstisko paziņojumu, uzskatāms, ka Klients ir pilnībā piekritis attiecīgajiem grozījumiem.

12.3. Ja brīdī kad Noteikumi un/vai Cenrādis tiek grozīti un ir spēkā stāšanās procesā, Klients noslēdz Līgumu vai uzsāk lietot Pakalpojumu, tad Noteikumi un Cenrādis ir saistoši tādā redakcijā, kādā tie ir spēkā stāšanās procesā.

12.4. Bankai ir tiesības grozīt Noteikumus un Cenrādi bez iepriekšēja paziņojuma Klientam, ja attiecīgie grozījumi:

12.4.1. ir izdarīti par labu Klientam;
12.4.2. tieši izriet no normatīvo aktu prasībām;

12.4.3. saskaņā ar piemērojamiem normatīvajiem aktiem Bankai ir tiesības paziņot Klientam par attiecīgajiem grozījumiem citā termiņā vai ir tiesības izdarīt šādus grozījumus bez iepriekšējas paziņošanas Klientam.
12.5. Noteikumu 12.4. punktā paredzētajā gadījumā Klients, kurš ir patērētājs, var atbilstoši Noteikumu 12.2. punkta noteikumiem nekavējoties vienpusēji atkāpties no Līguma.

13. STRĪDU RISINĀŠANAS KĀRTĪBA

13.1. Papildu informācija par kārtību, kādā Banka izskata Klientu

Agreement does not restrict the rights of the Account Holder to continue receiving the Remote Service, observing conditions of the Rules.
11.2. If an Agreement on the use of a specific Remote Access Instrument is terminated, it shall not terminate the Agreement on the use of other Remote Access Instruments, unless the Parties agree otherwise. Also, in this case the Bank shall not take actions to delete software used for the purposes of authentication. The User shall take such actions at its account.
11.3. Unless regulatory enactments provide otherwise, the Bank shall be entitled to unilaterally withdraw from the Agreement and/or to suspend the provision of the Service at any time notifying the Account Holder, who is a consumer, at least 2 (two) months in advance. In other cases, the Bank shall notify about the withdrawal within a reasonable time. If the Bank pursuant to regulatory enactments is obligated to terminate a business relationship, the Bank shall be entitled not to observe the deadlines for prior notification.
11.4. Unless otherwise provided in the regulatory enactments, the Bank shall be entitled to withdraw from the Agreement unilaterally without a prior notice, if the Account Holder and/or the User does not observe provisions of the Agreement and/or access to the Remote Access Instrument according to the Rules is restricted, as well as in other cases envisaged in Luminor General Business Terms or regulatory enactments.
11.5. When terminating a Service Agreement, the Account Holder upon Bank's request within the deadline set by the Bank shall pay all the fees defined in the Service Agreement and the Price List and calculated by the Bank, as well as shall fulfil other obligations arising from the Service Agreement.

12. ENTRY OF AMENDMENTS OF THE RULES INTO FORCE

12.1. The Rules and the Price List shall be amended by the Bank according to the procedure laid down in Luminor General Business Terms.
12.2. If the Customer, who is a consumer, does not agree to the proposed amendments to the Rules and/or the Price List, such a Customer shall be entitled until the date of their proposed date of entry into force to submit to the Bank a written notice of termination of the Agreement, observing that in this case the Customer upon Bank's request within the deadline set by the Bank shall pay all the fees defined in the Service Agreement and the Price List and calculated by the Bank, as well as fulfil other liabilities arising from the Service Agreement. If the Bank has not received the written notice referred to in this clause by the day of entry of amendments to the Rules or the Price List into force, it is deemed that the Customer has fully agreed to the respective amendments.
12.3. If at the time, when the Rules and/or the Price List are amended and are in the process of entry into force, the Customer shall conclude the Agreement, then the Rules and the Price List are binding in the edition, in which they are in the process of entry into force.
12.4. The Bank shall be entitled to amend the Rules and the Price List without a prior notice to the Customer, if the respective amendments:
12.4.1. are made in favour of the Customer;
12.4.2. directly arise from the requirements of regulatory enactments;
12.4.3. according to applicable regulatory enactments the Bank has the right to notify the Customer about respective amendments within other period of time or has the right to make such amendments without prior notification to the Customer.
12.5. In the case referred to in clause 12.4 of the Rules the Customer, who is a consumer, may according to provisions of clause 12.2 of the Rules withdraw unilaterally from the Agreement immediately.

13. DISPUTE SETTLEMENT PROCEDURE

13.1. Additional information about the procedure for consideration

sūdzības, pēc Klienta pieprasījuma ir pieejama Bankas klientu apkalpošanas vietā tās darba laikā un Bankas tīmekļa vietnē.

13.2. Klientam ir tiesības izmantot šādus sūdzību ārpustiesas izskatīšanas mehānismus:
13.2.1. Klients var iesniegt sūdzību Latvijas Komercbanku asociācijas ombudam (adrese: Pērses ielā 9/11, Rīgā LV-1011) saskaņā ar tā nolikumu un reglamentu, kas ir pieejami Latvijas Komercbanku asociācijas mājas lapā (https://www.lka.org.lv/ombuds/), ja sūdzība ietilpst ombuda kompetencē. Sūdzības iesniegšana ombudam nav priekšnosacījums prasības celšanai Latvijas Republikas tiesā vai Latvijas Komercbanku asociācijas šķīrējtiesā. Tāpat normatīvajos aktos noteiktajos gadījumos Klients var iesniegt sūdzību Finanšu un kapitāla tirgus komisijai;

13.2.2. Patērētājs normatīvajos aktos noteiktajos gadījumos var iesniegt sūdzību Patērētāju tiesību aizsardzības centram.

13.3. Attiecībā uz Klientiem, kuri nav uzskatāmi par patērētājiem, strīdi pēc prasītāja izvēles izskatāmi Latvijas Republikas tiesā vai Latvijas Komercbanku asociācijas šķīrējtiesā, vienotās reģistrācijas Nr. 40003746396, Rīgā, Latvijā, saskaņā ar tās nolikumu un reglamentu. Šķīrējtiesnešu skaits – 1 (viens), kuru ieceļ Latvijas Komercbanku asociācijas šķīrējtiesas priekšsēdētājs. Šķīrējtiesas izskatīšanas valoda – latviešu.

13.4. Pirms strīda nodošanas izskatīšanai tiesā vai šķīrējtiesā, Līdzēji ievēro Bankas noteikto sūdzību un pretenziju izskatīšanas kārtību.

14. CITI NOTEIKUMI

14.1. Klients, piesakoties un/vai lietojot Pakalpojumu ar Attālinātās pieejas līdzekļa starpniecību, kā arī lietojot jebkuru Attālinātās pieejas līdzekli, piekrīt šāda Pakalpojuma, kā arī attiecīgā Attālinātās pieejas līdzekļa noteikumiem.
14.2. Banka var ierakstīt un reģistrēt darbības, kas veiktas, izmantojot Attālinātās pieejas līdzekļus un glabāt šo informāciju Bankas un/vai trešo personu datubāzēs. Šādi ieraksti uzskatāmi par pierādījumu un apliecinājumu Klienta gribai un var kalpot par pierādījumu starp pusēm esošo strīdu risināšanai, tostarp tiesā. Bankai ir tiesības, taču tas nav Bankas pienākums, glabāt ierakstus 10 (desmit) gadus pēc Līdzēju darījumu attiecību izbeigšanas. Klients var lūgt Bankai darījuma pierādīšanas nolūkos izsniegt Klientam Bankas rīcībā esošus ierakstus Bankas noteiktā formātā. Par ierakstu izsniegšanas pakalpojumu Banka var piemērot maksu.

14.3. Banka veic personas datu apstrādi saskaņā ar Luminor Privātuma politiku, kas pieejama Bankas tīmekļa vietnē (https://www.luminor.lv/lv/privatuma-politika). Banka Līguma ietvaros neapstrādā, tostarp neuzglabā personas biometrijas datus.
14.4. Līdzēju tiesiskajām attiecībām, kas saistītas ar Pakalpojuma „Uzņēmuma banka" un "Gateway" izmantošanu, Noteikumi piemērojami tiktāl, ciktāl attiecīgā Pakalpojuma noteikumos nav noteikts citādi.

of Customer complaints by the Bank, upon Customer's request is available at the Bank's customer service location during its office hours and on the Bank's website.
13.2. The Customer has the right to use the following alternative dispute resolution procedures:
13.2.1. The Customer may submit a complaint to the Ombudsman of the Association of Latvian Commercial Banks (address: Pērses iela 9/11, Riga, LV-1011, Latvia) according to its regulations and rules, which are available on the website of the Association of Latvian Commercial Banks (https://www.lka.org.lv/en/ombudsman/), if the complaint is in competence of the ombudsman. Submission of the complaint to the ombudsman is not a precondition for bringing an action before the court of the Republic of Latvia or the Arbitration Court of the Association of Latvian Commercial Banks. Also in the cases envisaged in regulatory enactments the Customer may submit a complaint to the Financial and Capital Market Commission;
13.2.2. in the cases envisaged by regulatory enactments the consumer may submit a complaint to the Consumer Rights Protection Centre.
13.3. With regard to the Customers, who are not considered consumers, disputes at the plaintiff's choice shall be resolved in a court of the Republic of Latvia or in the Court of Arbitration of the Association of Latvian Commercial Banks, unified registration No. 40003746396, Riga, Latvia, according to its regulations and rules. The number of arbitrators – 1 (one), who is appointed in accordance with the Regulations of the Court of Arbitration of the Association of Latvian Commercial Banks. The language of the arbitration proceedings shall be Latvian.
13.4. Prior to the transfer of a dispute for examination in a court or an arbitration court, the Parties shall observe the procedure for examination of complaints and claims defined by the Bank.

14. OTHER PROVISIONS

14.1. The Customer, when applying for and/or using the Service by means of a Remote Access Instrument, as well as using any Remote Access Instruments, agrees to the Service Terms of such Service, as well as the respective Remote Access Instrument.
14.2. The Bank may record and register actions performed using Remote Access Instruments and store this information in databases of the Bank and/or third parties. These records are considered to be evidences and certification of the Customer's will and may serve as an evidence for resolution of disputes between the parties, including in a court. The Bank shall be entitled, yet not obligated to store the records for 10 (ten) years after termination of the business relationship between the Parties. The Customer may ask the Bank for the purposes of proof of a transaction to issue to the Customer records available at the Bank in the format defined by the Bank. A fee may be applied for the records issue service.
14.3. The Bank performs Processing of Personal Data according to Luminor Privacy Policy, which is available on the Bank's website (https://www.luminor.lv/en/privacy-policy).The Bank within the execution of the Agreement does not process and does not store biometric data of a person.
14.4. These Rules are applicable to the legal relationship between the Parties which concerns Services "Uzņēmuma banka" and "Gateway" to the extent that the respective Service Terms provide otherwise.