Privātuma politika

Apstiprināts

Signet Bank AS	
Padomes sēde:	07.11.2025.
Protokola numurs:	1-3/36

Akceptēts

Signet Bank AS	
Valdes sēde:	02.10.2025.
Protokola numurs:	2-1/47

Dokumenta īpašnieks:	Datu aizsardzības speciālists
Dokumenta rekvizīti:	5.4-1.1/POL.016
Konfidencialitātes pakāpe:	☑ Dienesta lietošanai ☐ Ierobežotas pieejas
Pamatdokuments:	
Grupas sabiedrības, uz kurām attiecas:	☑ Signet Bank AS; ☐ Visas Grupas sabiedrības; ☑ Atsevišķas Grupas sabiedrības, uzskaitīt: Signet Asset Management Latvia IPS, Citra Development SIA, AgroCredit SIA
Struktūrvienības, uz kurām attiecas:	Politika ir saistoša visiem Bankas darbiniekiem.
Saskaņots ar:	• Darbības atbilstības kontroles daļas vadītāja; • Bankas drošības daļas vadītājs; • Bankas risku direktors (CRO); • Komunikāciju un mārketinga daļas vadītāja; • Signet Asset Management Latvia IPS; • Citra Development SIA; • AgroCredit SIA.
Dokumenta nākamās aktualizācijas datums:	06.11.2026.

Saturs

I. Izmantotie termini

1. Dokumentā izmantoti šādi termini un saīsinājumi:
   1.1. **Banka** – Signet Bank AS;
   1.2. **Datu subjekts** (arī – **persona)** – identificēta vai identificējama fiziska persona, tai skaitā, klients, darbinieks, apmeklētājs un citi;
   1.3. **Datu valsts inspekcija** - personas datu apstrādes uzraudzības iestāde Vispārīgās datu aizsardzības regulas[1] (turpmāk - **Datu regula**) izpratnē;
   1.4. **Grupa** (šīs Politikas izpratnē) - Signet Bank AS grupā ietilpstošās juridiskās personas, kurām šī Politika ir tieši piemērojama, ir Signet Asset Management Latvia IPS, SIA Citra Development, SIA AgroCredit;
   1.5. **Informācijas resursu turētājs** – Pārziņa darbinieks, kurš savas kompetences ietvaros atbild par personas datu apstrādi atbilstoši attiecīgajam datu apstrādes mērķim (nolūkam) Pārziņa struktūrvienībā, nosaka Personas datu drošības prasības un apstiprina vai noraida citu Pārziņa struktūrvienību darbinieku piekļuves tiesības;
   1.6. **Kiberhigiēna** – ikdienas prakšu un paradumu kopums, kuru mērķis ir mazināt kiberapdraudējumus, nodrošināt datu aizsardzību un saglabāt informācijas un komunikāciju tehnoloģiju resursu pieejamību, integritāti un konfidencialitāti;
   1.7. **Pārzinis** – personas datu apstrādes pārzinis, Signet Bank AS vai attiecīgā gadījumā cita Grupas sabiedrība. Pārziņa kontaktinformācija pieejama tīmekļvietnes sadaļā Kontakti un Politikas 9. punktā;
   1.8. **Personas dati** (procedūras izpratnē – **fiziskas personas dati**) – jebkura informācija, ko apstrādā Banka un kas attiecas uz identificētu fizisku personu vai personu, kuru var tieši vai netieši identificēt, atsaucoties uz informāciju par to, tai raksturīgiem parametriem vai citiem identifikatoriem;
   1.9. **Personas datu aizsardzības pārkāpums** – personas datu drošības pārkāpums (apdraudējums), kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto

[1] Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula).

vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem, kā arī Datu regulas 5. pantā noteikto datu apstrādes principa pārkāpums;

1.10. **Personas datu apstrāde** - jebkura ar personas datiem veikta darbība vai darbību kopums, ko veic ar automatizētiem līdzekļiem vai kura veido daļu no kartotēkas, ja datu apstrādi neveic ar automatizētiem līdzekļiem;

1.11. **Personas datu drošība** – personas datu konfidencialitāte (personas datu apstrāde veidā, kas nodrošina piekļuvi šiem datiem tikai Pārziņa darbiniekiem ar atbilstošām pilnvarām), integritāte (iespēja nodrošināt personas datu saglabāšanu neizmainītā veidā, neatkarīgi no apstrādes metodēm) un pieejamība (autorizētai personai – Pārziņa darbiniekam iespēja piekļūt datiem noteiktā laikā un vietā noteikta uzdevuma izpildei);

1.12. **Politika** – iekšējais normatīvais dokuments "Privātuma politika".

II. Mērķis

2. Politikas mērķis ir nodrošināt tādu Personas datu apstrādi un šīs apstrādes tehnoloģisko vidi, lai Bankas un Grupas sabiedrības pamatdarbībai un ar pamatdarbību saistīto uzdevumu īstenošanai apstrādātā informācija, kas ietver Personas datus, un tehnoloģiskie resursi, kur informācija un dati tiek apstrādāti, būtu aizsargāti pret ārējiem un iekšējiem apdraudējumiem un vienlaikus būtu nodrošinātas Datu subjektu tiesības un brīvības.
3. Grupas mērķis ir nodrošināt vienotu Personas datu pārvaldības ietvaru. Vienlaikus Grupā ietilpst Politikas 1.4 punktā uzskaitītās juridiskās personas, uz kurām attiecas šīs Politikas principi, kā arī tādas juridiskās personas kā AS Primero Finance un AS Magnetiq Bank, kurām ir plašs klientu loks, konkrēti un specifiski, no Bankas atšķirīgi darbības virzieni, tādēļ tām ir izveidotas šai Politikai līdzvērtīgas un Datu regulai atbilstošas Privātuma politikas.

III. Vispārīgā informācija

4. Politikā ir sniegta informācija par Bankas un Grupas sabiedrības kā Pārziņa veiktās personas datu apstrādes nolūkiem (mērķiem), īstenotajiem pasākumiem Datu regulas prasību nodrošināšanai, tostarp, Kiberhigiēnas ievērošanai un Datu subjektu tiesību īstenošanai.
5. Bankai ir svarīga godprātīga un likumīga personas datu apstrāde, atbilstīgu un vispusīgu Personas datu aizsardzības pasākumu nodrošināšana un Datu subjektu tiesību ievērošana visos Bankas vai Grupas sabiedrības pamatdarbības un to atbalsta procesu īstenošanas posmos.
6. Ar informāciju par Personas datu apstrādi iespējams iepazīties tīmekļvietnes sadaļā "Personas datu apstrāde". Pie katra personas datu apstrādes nolūka (mērķa) atbilstoši 1. pielikumam "Datu apstrādes veidlapa", ir norādīta uz to attiecināmā papildu informācija. Atkarībā no izmantotā Bankas vai Grupas sabiedrības pakalpojuma veida šāda informācija var būt ietverta arī līgumā un ar to saistītajos dokumentos.
7. Datu apstrādes veidlapa pēc tās aizpildīšanas un apstiprināšanas valdē ir publiskojama

Bankas tīmekļvietnē viegli pārskatāmā veidā. Tā var tikt papildināta vai mainīta atbilstoši faktiskajiem apstākļiem, neatkarīgi no Politikas pārskatīšanas. Pēc veikto izmaiņu apstiprināšanas Bankas vai Grupas sabiedrības valdē, aktuālā, Datu apstrādes veidlapā atspoguļotā informācija ir publiskojama.

8. Ar informāciju par tīmekļvietnē izmantotajām sīkdatnēm un sīkdatņu izmantošanas pamatnosacījumiem iespējams iepazīties tīmekļvietnes sadaļā "Personas datu apstrāde", izvēloties "Sīkdatņu atruna" (2. pielikums "Sīkdatņu izmantošana"). Sīkdatņu informāciju ir pienākums atjaunot, atbilstoši to faktiskajām izmaiņām.
9. **Pārziņa kontaktinformācija:**
    - 9.1. Signet Bank AS
      adrese: Antonijas iela 3, Rīga, LV 1010, Latvija
      e-pasts: *info@signetbank.com*;
    - 9.2. Signet Asset Management Latvia IPS
      adrese: Antonijas iela 3-1, Rīga, LV 1010, Latvija
      e-pasts: *info@signetam.com*;
    - 9.3. Citra Develpoment SIA
      adrese: Antonijas iela 3-5, Rīga, LV 1010, Latvija
      e-pasts: *info@signetbank.com*;
    - 9.4. AgroCredit SIA
      Adrese: Ziedleju ielas 6, Mārupe, LV 2167, Latvija
      e-pasts: *birojs@agrocredit.lv.*

IV. Privātuma politikas pamatprincipi

10. Politika ir izstrādāta saskaņā ar Datu regulā, Fizisko personu datu apstrādes likumā, Kredītiestāžu likumā un citos Latvijas Republikā spēkā esošajos saistošajos normatīvajos aktos noteikto, atbilstoši Bankas un Grupas sabiedrības piedāvātajiem produktiem un pakalpojumiem.
11. Bankā un Grupā ir izveidota iekšējā kontroles sistēma, kas ietver iekšējo normatīvo aktu regulāru pārskatīšanu un atjaunināšanu, Kiberhigiēnas ievērošanu kā būtisku Personas datu aizsardzības elementu, tehnoloģisko aizsardzības līdzekļu un procesu uzlabošanu un ne retāk kā reizi gadā tiek organizētas personāla apmācības Personas datu apstrādes, aizsardzības un kiberdrošības jomās. Savstarpējā saistībā šīs jomas veido atbilstīgu drošības kultūru, nodrošina Personas datu aizsardzību un Politikas mērķa īstenošanu.
12. Banka un Grupa apstrādā Personas datus tikai tad, ja nolūku (mērķi) nav iespējams pienācīgi sasniegt citiem līdzekļiem, tikai tādā apjomā, kādā tas ir nepieciešams šī nolūka (mērķa) sasniegšanai, kā arī neizmanto Personas datus citiem, ar sākotnējo nolūku (mērķi) nesaistītiem uzdevumiem.
13. Banka un Grupa galvenokārt veic Personas datu apstrādi tādēļ, lai sniegtu pakalpojumu atbilstoši uzņēmējdarbības veidam, noslēgtu un izpildītu līgumu un sniegtu pakalpojumus klientiem, tai skaitā, nodrošinātu atbildīgu kreditēšanu, investīciju pakalpojumus un/vai ikdienas finanšu pakalpojumus, kā arī atbilstoši normatīvajos aktos noteiktajam, izpildītu juridisko pienākumu, īstenotu sabiedrības intereses un

nodrošinātu pamatdarbības atbalsta procesus.

14. Banka un Grupas sabiedrība nodrošina, lai īstenojamo tehnisko, tehnoloģisko un organizatorisko pasākumu izmaksas ir samērojamas ar iespējamiem zaudējumiem, kas varētu rasties Personas datu aizsardzības pārkāpuma dēļ, tostarp, ja nav ievērota Kiberhigiēna (apdraudēta informācijas resursu konfidencialitāte, integritāte vai pieejamība).
15. Grupa veicina personāla izpratni par katra darbinieka pienākumiem un atbildību Personas datu aizsardzības nodrošināšanā, tai skaitā veic atbilstošas uzdevumu izpildes kontroles, pēcpārbaudes un nodrošina regulārus apmācību pasākumus. Tāpat Banka un Grupa izglīto darbiniekus Kiberhigiēnas jomā.
16. Ja ir konstatēts Personas datu aizsardzības pārkāpums, Banka vai Grupas sbiedrība veic vispusīgu notikuma izmeklēšanu, pierādījumu saglabāšanu un notikušā seku novēršanu vai mazināšanu, kā arī Datu regulā noteiktajos gadījumos Datu valsts inspekcijas un Datu subjekta informēšanu. Grupas sabiedrības sadarbojas un sniedz savstarpēju palīdzību, lai savlaicīgi identificētu riskus, mazinātu iespējamās sekas vai novērstu apdraudējumu.
17. Politiku, kā arī tās grozījumus akceptē Bankas valde un apstiprina Bankas padome.

V. Personas datu klasifikācija

18. Personas datu klasifikācijas mērķis ir identificēt Bankā apstrādājamo personas datu nozīmīgumu, lai tiem piemērojamie fiziskie un loģiskie aizsardzības pasākumi būtu atbilstoši aizsargājamo Personas datu vērtībai.
19. Personas datus klasificē atkarībā no kaitējuma, kas var tikt nodarīts Datu subjekta tiesībām uz savu personas datu aizsardzību un brīvībām, ja nav nodrošināta informācijas, tai skaitā Personas datu konfidencialitāte, integritāte un pieejamība.
20. Augsta riska personas dati ir tādi personas dati, kas Personas datu aizsardzības pārkāpuma gadījumā Datu subjektam var izraisīt materiālu vai nemateriālu kaitējumu (piemēram, kontroles zaudēšanu pār saviem personas datiem, identitātes zādzību, kaitējumu reputācijai), kā arī īpašu kategoriju personas dati. Šādiem datiem Grupā piemēro pastiprinātus aizsardzības līdzekļus.
21. Augsta riska personas datu apstrāde ir personas datu apstrāde plašā mērogā, tai skaitā, kas saistīta ar personu novērošanu vai novērtēšanu, un jaunu vai inovatīvu tehnoloģisko risinājumu izmantošana personas datu apstrādē. Piemēram, profilēšana – ja Banka vai Grupas sabiedrība nolemj to izmantot pakalpojuma sniegšanai, tā rūpīgi novērtē iespējamo Datu subjekta tiesību aizskārumu.

VI. Personas datu drošības pārvaldība

22. Bankas iekšējos normatīvajos dokumentos Personas datu apstrādes un aizsardzības un Kiberhigiēnas jomā ir noteikti šādi pasākumi:
    22.1. Informācijas sistēmu kontroles pasākumi, tai skaitā piekļuve personas datiem tikai identificētiem un autorizētiem darbiniekiem; informācijas lietotāju diferenciācija un informācijas sistēmu lietotāja tiesību piešķiršanas inventarizācijas un anulēšanas kārtība;

22.2. regulāras darbinieku apmācības tai skaitā par Personas datu apstrādes pamatprincipiem, piekļuves kārtību Personas datiem, "tīrā galda politikas" ievērošana un informācijas sistēmu un tehnoloģisko rīku lietošanas nosacījumi;
22.3. informācijas sistēmu pilnvērtīgas funkcionalitātes nodrošināšana, atbilstošas konfigurācijas un tehnoloģiskie drošības risinājumi, lai mazinātu vai novērstu neautorizētu personu piekļuvi Bankas vai Grupas sabiedrības resursiem;
22.4. informācijas sistēmās izmantojamie šifrēšanas un citi aizsardzības līdzekļi, datu pseidonimizācija un minēto procesu pārskatīšanas kārtība, lai nodrošinātu Personas datu drošību un atbilstošu aizsardzību visā to apstrādes ("dzīves cikla") laikā;
22.5. informācijas sistēmu izmaiņu kārtība, produkcijā ieviešot tikai pilnvērtīgi testētas, novērtētas un akceptētas izmaiņas;
22.6. Personas datu aizsardzības pārkāpumu un informācijas un komunikāciju tehnoloģiju drošības incidentu pārvaldība, lai mazinātu to ietekmi uz katru individuālu Datu subjektu, Personas datu apstrādi, Bankas un Grupas pamatdarbības procesiem, kā arī novērstu vai mazinātu šādu gadījumu atkārtošanās iespēju.

23. Banka un Grupa katru novērtējumu par ietekmi uz datu aizsardzību īstenotajiem Personas datu apstrādes procesiem izmanto kā konstruktīvu risku analīzes rīku, lai noteiktu esošas vai plānotas Personas datu apstrādes atbilstību Vispārīgajā datu aizsardzības regulā un citos saistošajos normatīvajos aktos, kas attiecināmi uz personas datu apstrādi un aizsardzību finanšu un kreditēšanas jomā noteiktajam. Pilnvērtīgs Personas datu apstrādes novērtējums ļauj apzināties apdraudējumu, tā īstenošanās varbūtību un šāda apdraudējuma iespējamo ietekmi uz Datu subjekta tiesībām uz savu datu aizsardzību.
24. Personas datu apstrādes pārvaldības un Personas datu apstrādē izmantojamo tehnoloģiju risku vadības pasākumus un rīkus nosaka Bankas un katras Grupas sabiedrības valde savos lēmumos.
25. Novērtējumu par ietekmi uz datu aizsardzību augsta riska personas datu apstrādes jomās veic atbilstoši Vispārīgās datu aizsardzības regulas 35. punktā noteiktajam un saskaņā ar Bankas iekšējo normatīvo dokumentu "Personas datu apstrādes un aizsardzības procedūra" un tā rezultātus izmanto, plānojot vai nosakot aizsardzības līdzekļus un risku mazinošos pasākumus, kā arī konkrētus uzdevumus un termiņus to izpildei.
26. Lai nodrošinātu informācijas sistēmu darbības nepārtrauktību un atjaunošanu incidentu gadījumā, Bankā ir izveidots "Darbības nepārtrauktības nodrošināšanas plāns", kā arī izstrādāti iekšējie normatīvie dokumenti, kur noteikta informācijas sistēmu un tehnoloģisko resursu atjaunošanas vai aizstāšanas kārtība. Bankas un Grupas sabiedrības informācijas sistēmas, tehnoloģiskie elementi un personāls tiek regulāti apmācīti, lai nodrošinātu pakalpojumu sniegšanas nepārtrauktību un saglabātu augstu informācijas, un personas datu aizsardzības līmeni.
27. Informācijas sistēmu darbības nepārtrauktības nodrošināšanai un atjaunošanai Banka veic regulāru personas datu rezerves kopēšanu, nodrošina rezerves kopijas glabāšanu

citā ģeogrāfiskajā atrašanās vietā un to pārbaudes, lai gūtu pārliecību par atjaunotās informācijas sistēmas darbspēju un datu integritāti.

28. Ja Banka vai Grupa ieviešjaunas informācijas sistēmas, tehnoloģiskos rīkus, izstrādā vai attīsta jaunus produktus, šajos procesos ievēro integrētu parsonas datu aizsardzību un īsteno personas datu aizsardzību pēc noklusējuma.

VII. Datu subjekta tiesības

29. Datu subjektam attiecībā uz Bankā apstrādātajiem personas datiem ir šādas tiesības:
    29.1. pieprasīt un saņemt informāciju no Bankas vai Grupas sabiedrības kā atsevišķa Pārziņa par Personas datu apstrādi un, nepieciešamības gadījumā, lūgt nodrošināt piekļuvi tiem;
    29.2. izteikt lūgumu labot personas datus, ja šie dati ir neatbilstoši, nepareizi vai neprecīzi;
    29.3. prasīt ierobežot datu apstrādi, lai nodrošinātu Personas datu precizitāti vai citos Vispārīgajā datu aizsardzības regulā noteiktajos gadījumos, kas skar pārziņa un Datu subjekta attiecības;
    29.4. atsaukt iepriekš sniegtu Datu subjekta piekrišanu savu Personas datu apstrādei un pieprasīt dzēst attiecīgos personas datus (ja vien nav cita likumīga pamata šo personas datu apstrādei); piekrišanas atsaukums neattiecas uz Personas datu apstrādi laikā pirms atsaukuma;
    29.5. iebilst Personas datu apstrādei mārketinga nolūkos;
    29.6. saņemt personas datus, ko Datu subjekts ir sniedzis, pamatojoties uz piekrišanu vai kas ir nepieciešami ar Datu subjektu noslēgta līguma izpildei, un tiek izmantoti strukturētā veidā, plaši izmantojamā elektroniskā formātā; kā arī, ja tas ir tehniski iespējams un juridiski pieļaujams, lūgt nodot šādus datus citam komersantam, tādējādi nodrošinot personas datu pārnesamību.
30. Lai īstenotu savas tiesības, Datu subjekts var sagatavot un iesniegt iesniegumu veidā, kas ļauj Pārzinim identificēt konkrēto Datu subjektu. Tas ir, izmantojot internetbankas iespējas, iesniedzot ar drošu elektronisko parakstu parakstītu iesniegumu vai iesniedzot šādu pieprasījumu klātienē Bankas vai Grupas klientu apkalpošanas darbiniekiem.
31. Datu subjekta pieprasījumā vēlams norādīt precīzu laika posmu un informāciju par Personas datiem, kurus Datu subjekts vēlas saņemt, kā arī šāda pieprasījuma pamatojumu. Minētā informācija ļauj Pārzinim sagatavot precīzāku atbildi īsākā laika posmā.
32. Atbildi uz Datu subjekta pieprasījumu sniedz bez liekas kavēšanās, bet ne vēlāk kā viena mēneša laikā. Ja nepieciešams, Banka vai Grupas sabiedrība Datu subjektam var lūgt iesniegt papildus informāciju, kā arī pagarināt atbildes sniegšanas termiņu par vēl diviem mēnešiem, ņemot vērā iesnieguma sarežģītību vai līdzīgu pieprasījumu skaitu.
33. Tiesības uz Personas datu aizsardzību nav absolūtas un normatīvajos aktos noteiktajos gadījumos, kā arī noteiktās situācijās tās var tikt ierobežotas, tai skaitā, lai neietekmētu citu personu tiesības un brīvības, nodrošinātu komercnoslēpuma un intelektuālā īpašuma aizsardzību. Vienlaikus tas nozīmē, ka Banka sniedz Datu subjektam tikai to informāciju, ko neaizliedz normatīvie akti un kādu faktiski vai veicot tiesību

samērīguma vērtējumu ir iespējams izsniegt.

34. Datu subjektam ar Personas datu apstrādi un aizsardzību saistītos jautājumos ir iespējams sazināties ar Bankas datu aizsardzības speciālistu, tostarp uzdodot jautājumus par Personas datu apstrādi Grupā, nosūtot elektroniskā pasta ziņojumu vai elektroniski parakstītu vēstuli uz adresi: *datuaizsardziba@signetbank.com*.

VIII. Noslēguma noteikumi

35. Lai nodrošinātu šīs Politikas aktualitāti un atbilstību, ievērojot pārmaiņas Bankas vai Grupas darbībā, kā arī izmaiņas ārējos normatīvajos aktos, to pārskata ne retāk kā reizi gadā.
36. Banka nodrošina aktuālās Privātuma politikas publicēšanu savā tīmekļvietnē.
37. Banka un Grupa augstu vērtē konfidencialitāti un katra Datu subjekta tiesību aizsardzību un ir ieinteresēta rast konstruktīvu risinājumu domstarpību gadījumos. Tomēr, ja Datu subjektam ir būtiskas pretenzijas, tas var vērsties ar iesniegumu Datu valsts inspekcijā
    37.1. izmantojot e-pastu: *pasts@dvi.gov.lv;*
    37.2. vai nosūtot vēstuli uz adresi: Elijas iela 17, Rīga, LV-1050.

IX. Saistītie iekšējie normatīvie Dokumenti

1. "Darbības nepārtrauktības nodrošināšanas plāns"(PLA.002).
2. "Personas datu apstrādes un aizsardzības procedūra"(PRO.124).
3. "Kiberdrošības un digitālās darbības noturības stratēģija" (STR.005).

X. Piemērojamie ārējie normatīvie akti

1. Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula).
2. Fizisko personu datu apstrādes likums.
3. Kredītiestāžu likums.

XI. Pielikumi

1. Datu apstrādes veidlapa.
2. Sīkdatņu izmantošana.

Versiju hronoloģija:

Versija	Spēkā no	Komentāri	Dokumenta izstrādātājs
03	07.11.2025.	Aktualizēta versija, papildināta ar Grupas sabiedrībām uz kurām tieši attiecināma (vai nav attiecināma) Politika. Ņemtas vērā izmaiņas Bankas iekšējā normatīvā dokumenta formā un izmaiņas ārējā normatīvajā regulējumā, kas attiecināmas uz kiberdrošības jomu, taču tieši skar arī personas datu aizsardzības jautājumus. Noteikta kārtība, kādā publiskojama informācija, kas atspoguļota Politikas pielikumu aizpildītajās veidnēs.	I.Grūberte, Datu aizsardzības speciāliste

2.0.	28.05.2024	Jauna redakcija. Ar mērķi izpildīt Vispārīgajā datu aizsardzības regulā noteikto pienākumu datu subjekta informēšanai. Izveidoti jauni pielikumi „Datu apstrādes veidlapa” (Nr.1), „Sīkdatņu izmantošana” (Nr. 2).	
1.4.	21.02.2023.	Vispārējā rakstura grozījumi. Papildināts, ka starp personas datu kategorijām, kuras apstrādā Grupa, ir arī auditācijas pieraksti.	
1.3.	22.12.2021.	Vispārējā rakstura grozījumi. Precizēta Grupas mēroga pieeja.	
1.2.	18.12.2020.	Vispārējā rakstura grozījumi. Ir papildināts saraksts ar personas datu apstrādes tiesiskajiem pamatiem.	
1.1.	19.12.2019.	Vispārējā rakstura grozījumi.	
1.0.	21.12.2018.	Sākotnējā versija.	

* * * * *