Privātuma politika

SIGNET BANK

Saturs

I Izmantotie termini

1. **Datu subjekts** – identificēta vai identificējama fiziska persona.
2. **Datu valsts inspekcija** - personas datu apstrādes uzraudzības iestāde Vispārīgās datu aizsardzības regulas[1] (turpmāk - Datu regula) izpratnē.
3. **Informācijas resursu turētājs** – Pārziņa darbinieks, kurš atbilstoši kompetencei atbild par personas datu apstrādi atbilstoši attiecīgajam datu apstrādes mērķim Pārziņa struktūrvienībā, nosaka Prsonas datu drošības prasības un apstiprina vai noraida citu Pārziņa struktūrvienību darbinieku piekļuves tiesības.
4. **Informācijas sistēmu kontrole** – metode, pasākums vai to kopums personas datu apstrādes risku mazināšanai informācijas sistēmās.
5. **Pārzinis** – personas datu apstrādes pārzinis, Signet Bank AS.
6. **Personas datu aizsardzības pārkāpums** – personas datu drošības pārkāpums (apdraudējums), kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem, kā arī Datu regulas 5. pantā noteikto datu apstrādes principa pārkāpums.
7. **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.
8. **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).
9. **Politika** – Bankas iekšējais normatīvais dokuments „Privātuma politika”.

[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)

II Vispārīgā informācija

10. Politikā ir sniegta informācija par Signet Bank AS (turpmāk – Banka) kā datu pārziņa veiktās personas datu apstrādes nolūkiem (mērķiem), īstenotajiem pasākumiem Datu regulas prasību nodrošināšanai, tostarp Datu subjektu tiesību īstenošanai.
11. Bankai ir svarīga godprātīga un likumīga personas datu apstrāde, atbilstīgu personas datu aizsardzības pasākumu nodrošināšana un Datu subjektu tiesību ievērošana.
12. Ar informāciju par personas datu apstrādi iespējams iepazīties pie katra personas datu apstrādes mērķa (1. pielikums„Datu apstrādes veidlapa"), kā arī papildu informācija, atkarībā no izmantotā Bankas pakalpojuma veida, var būt ietverta līgumos un ar tiem saistītajos dokumentos. Privātuma politikas pielikums ietver arī sīkdatņu izmantošanas pamatnosacījumus (2. pielikums „Sīkdatņu izmantošana").
13. Pārziņa kontaktinformācija:
    - Signet Bank AS;
    - adrese: Antonijas iela 3, Rīga, LV 1010, Latvija;
    - tālrunis: +371 67 080 000;
    - e-pasts: *info@signetbank.com*.

III Privātuma politikas pamatnolūks un tā īstenošana

14. 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 piedāvātajiem produktiem un pakalpojumiem.
15. Politikas mērķis ir nodrošināt tādu Personas datu apstrādi un Personas datu apstrādes tehnoloģisko vidi, lai Bankas rīcībā esošā informācija, tai skaitā personas dati, un tehnoloģiskie resursi būtu aizsargāti pret ārējiem un iekšējiem drošības riskiem, un vienlaikus nodrošinātu Datu subjektu tiesības un brīvības, kā arī atbilstu Bankas mērķu un uzdevumu īstenošanai.
16. Bankā ir noteikta iekšējā kontroles sistēma un regulāri tiek pārskatīts iekšējo procedūru kopums, tai skaitā Personas datu drošības jomā, tādējādi nodrošinot Politikas pamatnolūka sasniegšanu.
17. Īstenojamo tehnisko, tehnoloģisko un organizatorisko pasākumu izmaksas ir samērojamas ar iespējamiem zaudējumiem, kas varētu rasties Personas datu apstrādē izmantojamās informācijas sistēmas drošības riska notikuma gadījumā (ja ir apdraudēta informācijas resursu konfidencialitāte, integritāte vai pieejamība).
18. Banka nodrošina personāla izpratni par katra darbinieka pienākumiem Personas datu drošības nodrošināšanā, tai skaitā veic atbilstošas uzdevumu izpildes kontroles, pēcpārbaudes un nodrošina regulārus apmācību pasākumus.
19. Konstatējot Personas datu aizsardzības pārkāpumu, Banka 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.
20. Politiku, kā arī tās grozījumus akceptē Bankas valde un apstiprina Bankas padome.

21. Politika stājas spēkā tās apstiprināšanas brīdī un ar tās apstiprināšanu spēku zaudē 21.02.2023. apstiprinātais Bankas iekšējais normatīvais dokuments „Privātuma politika".
22. Politika ir saistoša visiem Bankas darbiniekiem.

IV Personas datu klasifikācija

23. Personas datu klasifikācijas mērķis ir identificēt Bankā apstrādājamo personas datu nozīmīgumu, lai tiem piemērojamie aizsardzības pasākumi būtu atbilstoši aizsargājamo perosnas datu vērtībai.
24. Personas datus klasificē atkarībā no kaitējuma, kas var tikt nodarīts Datu subjekta tiesībām uz savu personas datu aizsardzību un brīvībām, ja nav nodrošināta konfidencialitāte, integritāte un pieejamība.
25. Augsta riska personas dati ir tādi personas dati, kas Personas datu aizsadzības 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 un personas dati, kas saistīti ar pārkāpumiem.
26. Augsta riska personas datu apstrāde ir personas datu apstrāde plašā mērogā, tai skaitā, kas saistīta ar novērošanu, un jaunu tehnoloģiju vai programmatūras izmantošana personas datu apstrādē.

V Personas datu drošības pārvaldība

27. Bankas iekšējos normatīvajos dokumentos personas datu apstrādes un aizsardzības un informācijas sistēmu lietošanas un drošības jomā ir noteikti šādi pasākumi:
    - 27.1. Informācijas sistēmu kontroles pasākumi, tai skaitā piekļuve personas datiem tikai identificētiem un autorizētiem darbiniekiem; informācijas sistēmu lietotāju tiesību piešķiršana, inventarizācijas un anulēšanas kārtība; informācijas sistēmu lietotāja tiesību piešķiršanas kārtība, ievērojot informācijas apjoma nepieciešamību darba pienākumiem;
    - 27.2. darbinieku apmācības par datu apstrādes pamatprincipiem, piekļuves kārtību personas datiem un informācijas sistēmu lietošanas nosacījumiem;
    - 27.3. informācijas sistēmu funkcionalitāte, konfigurācijas un tehnoloģiskie risinājumi, lai mazinātu un novērstu neautorizētu personu piekļuvi Bankas resursiem;
    - 27.4. informācijas sistēmās izmantojamie šifrēšanas un citi atbilstoši aizsardzības līdzekļi, datu pseidonimizācija un minēto procesu pārskatīšanas kārtība, lai nodrošinātu Personas datu drošību un atbilstošu aizsardzību visā to apstrādes laikā;
    - 27.5. informācijas sistēmu izmaiņu kārtība, produkcijā ieviešot tikai testētas, novērtētas un akceptētas izmaiņas;
    - 27.6. Personas datu aizsardzības pārkāpumu un informācijas sistēmu drošības incidentu pārvaldība, lai mazinātu to ietekmi uz Personas datu apstrādi un aizsardzību un Bankas procesiem kopumā, kā arī to atkārtošanās risku.
28. Novērtējums par ietekmi uz datu aizsardzību ir, tai skaitā, risku analīzes rīks, lai

noteiktu esošas vai plānotas Personas datu apstrādes atbilstību Datu regulai un citiem saistošajiem normatīvajiem aktiem personas datu aizsardzības jomā, apzinātu apdraudējuma īstenošanās varbūtību un šāda apdraudējuma ietekmi uz Datu subjekta tiesībām uz savu datu aizsardzību.

29. Personas datu apstrādes risku vadības un Personas datu apstrādē izmantojamo tehnoloģiju risku vadības pasākumus un izmantojamās tehnoloģijas nosaka Bankas valde, tai skaitā nosakot Informācijas resursu turētājus un ieceļot informācijas sistēmu drošības pārvaldnieku.
30. Novērtējumu par ietekmi uz datu aizsardzību augsta riska personas datu apstrādes jomās veic ne retāk kā vienu reizi divos gados un tā rezultātus izmanto, plānojot vai nosakot aizsardzības līdzekļus un risku mazinošos pasākumus, kā arī konkrētus uzdevumus un termiņus to izpildei.
31. Lai nodrošinātu informācijas sistēmu darbības nepārtrauktību un atjaunošanu incidentu gadījumā, Bankā ir izveidots „Darbības nepārtrauktības nodrošināšanas plāns" un noteikta informācijas sistēmu atjaunošanas kārtība.
32. Informācijas sistēmu darbības nepārtrauktības nodrošināšanai un atjaunošanai Banka veic regulāru informācijas sistēmas personas datu rezerves kopēšanu, nodrošinot rezerves kopijas glabāšanu citā ģeogrāfiskajā atrašanās vietā, kā arī nodrošina informācijas sistēmas atjaunošanas pārbaudes, lai gūtu pārliecību par atjaunotās informācijas sistēmas darbspēju un datu integritāti.

VI Datu subjekta tiesības

33. Datu subjektam attiecībā uz Bankā apstrādātajiem personas datiem ir šādas tiesības:
    - 33.1. saņemt informāciju, vai Banka apstrādā Datu subjekta personas datus, un apstiprinošā gadījumā atbilstoši Datu subjekta pieprasījumam, nodrošināt piekļuvi tiem;
    - 33.2. labot personas datus, ja šie dati ir neatbilstoši, nepareizi vai neprecīzi;
    - 33.3. prasīt ierobežot datu apstrādi, lai nodrošinātu personas datu precizitāti vai citos Datu regulā noteiktajos gadījumos, kas skar pārziņa un Datu subjekta attiecības;
    - 33.4. 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);
    - 33.5. iebilst Personas datu apstrādei mārketinga nolūkos;
    - 33.6. 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, lūgt nodot šādus datus citam komersantam, tādējādi nodrošinot personas datu pārnesamību.
34. Lai īstenotu savas tiesības, Datu subjekts var sagatavot un iesniegt pieprasījumus veidā, kas ļauj Pārzinim identificēt konkrēto Datu subjektu, izmantojot internetbankas iespējas, iesniedzot ar drošu elektronisko parakstu parakstītu pieprasījumu vai iesniedzot šādu pieprasījumu klātienē Bankas darbiniekiem.
35. 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.

36. Atbildi uz Datu subjekta pieprasījumu sniedz bez liekas kavēšanās, bet ne vēlāk kā viena mēneša laikā. Ja nepieciešams, Banka Datu subjektam var lūgt iesniegt papildu informāciju, kā arī pagarināt atbildes sniegšanas termiņu par vēl diviem mēnešiem, ņemot vērā pieprasījuma sarežģītību vai šādu pieprasījumu skaitu.
37. 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. Tas nozīmē, ka Banka sniedz Datu subjektam tikai to informāciju, ko neaizliedz normatīvie akti un kādu faktiski vai veicot tiesību samērīguma vērtējumu ir iespējams sniegt.
38. Datu subjektam ar Personas datu apstrādi un aizsardzību saistītos jautājumos ir iespējams sazināties ar Bankas datu aizsardzības speciālistu, nosūtot elektroniskā pasta ziņojumu vai elektroniski parakstītu vēstuli uz adresi: *datuaizsardziba@signetbank.com*.

VII Noslēguma noteikumi

39. Lai nodrošinātu šīs Politikas aktualitāti un atbilstību, ievērojot pārmaiņas Bankas darbībā vai izmaiņas ārējos normatīvajos aktos, Banka to pārskata ne retāk kā reizi gadā.
40. Banka nodrošina aktuālās Privātuma politikas publicēšanu savā tīmekļvietnē.
41. Būtisku pretenziju vai domstarpību gadījumā Datu subjekts var iesniegt sūdzību Datu valsts inspekcijā, izmantojot e-pastu: *pasts@dvi.gov.lv* vai nosūtot vēstuli uz adresi: Elijas iela 17, Rīga, LV-1050.

VIII Pielikumi

N. p. k.	Nosaukums
1.	Datu apstrādes veidlapa
2.	Sīkdatņu izmantošana

* * * * *