

Kā ievērot datu aizsardzību, NOVĒRŠOT NAUDAS ATMAZGĀŠANAS RISKUS

2022. gada 1. janvārī stājas spēkā Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas (NILLTPFN) likuma 9. panta redakcija, saskaņā ar kuru katram šī likuma subjektam ir pienākums nodrošināt, ka tā darbinieki atbilstoši viņu amata pienākumiem pārzina arī personas datu aizsardzības prasības, kas attiecas uz likuma regulēto jomu. To atgādināja arī zvērinātu advokātu biroja (ZAB) SORAINEN tiesību eksperti, kuri tiešsaistes seminārā skaidroja, kā salāgot NILLTPFN un personas datu aizsardzības prasības.



VIOLETA
ZEPPA-
PRIEDĪTE

Zvērinātu
advokātu
biroja
Sorainen
Latvijas biroja
korporatīvo
noziegumu
izmeklēšanas
un atbilstības
prakses
vadītāja

„Līdz šim prasība par zināšanām noziedzīgi iegūtu līdzekļu legalizācijas novēršanas jomā bija izvirzīta likuma subjektu atbildīgajiem darbiniekiem, taču tagad šis loks ir ievērojami paplašināts, attieci- not prasību uz teju visiem darbiniekiem. Protams, tie nebūtu tehniska rakstura darbinieki (apkopēji, sanitehniski u.tml.), taču darbiniekiem, kuri pēc bū- tības veic likuma subjekta funkcijas, šim zināša- nām jābūt, un darba devējam ir pienākums par to gādāt,” uzsvēra **VIOLETA ZEPPE-PRIEDĪTE**, SORAINEN Latvijas biroja korporatīvo noziegu- mu izmeklēšanas un atbilstības prakses vadītāja.

Juridiskais ietvars

Juristu diskusijās nonākts pie secinājuma, ka NILLTPFN likuma jeb, kā juristu vidē saīsināti mēdz dēvēt, AML (*Anti-money laundering – no angļu val.*) likuma kā speciāla normatīvā akta pie- mērošana nedaudz prevalē pār datu aizsardzības kā vispārējā normatīvā akta prasībām. „Ja specifika ir AML prasība, tad priekšroka dodama AML,” pauða V. Zeppa-Priedīte. Tomēr tas nenozīmē, ka, piemērojot vienu regulējumu, no otra var atteikties. Vispārīgā datu aizsardzības regula¹ noteic lielos pamatprincipus, uz kuriem balstās fizisko personu datu aizsardzība Eiropas Savienībā, un tas ir tieši piemērojams normatīvais akts, kuru neatceļ neviens cits dalībvalstu izdotais likums. Ikvienam no tiem ir jāatbilst minētās regulas prasībām. Tie mijiedarbojas – regula sniedz darbības vadlīnijas vispārīgām situācijām, savukārt AML jomu regulējošais dalībvalsts izdotais likums sniedz rīcības plānu īpa- šiem gadījumiem. Līdz ar to, ja NILLTPN likumā

kaut kas nav noregulēts, tad jāskatās, kas minēts Vispārīgajā datu aizsardzības regulā. Tieši tādēl cil- vēkiem, kas strādā AML jomā, jāzina arī regulas prasības, seminārā skaidroja **JŪLIJA TERJUHANA**, ZAB SORAINEN juriste, sertificēta datu aizsar- dzības speciāliste.

NILLTPFN likuma kontekstā tiek apstrādāti šādi personas dati:

- personas identifikācijas dati (personu aplieci- noši dokumenti, kopijas);
- saimniecisko darbību raksturojošie dati;
- personiskās darbības veidu raksturojošie dati (personiskie līdzekļi, konti, ipašumi, radniecība vai cita veida saistība ar politiski nozīmīgām personām utt.);
- finanšu dati;
- sankcijas;
- padziļinātās izpētes dati.

Strādājot ar personas datiem, būtu ieteicams redzeslokā allaž paturēt Vispārīgās datu aizsardzī- bas regulas 5. pantā noteiktos datu aizsardzības principus. Cilvēkam, kurš nav ar pamatīgām zinā- šanām datu aizsardzības jomā, ieteicams izmantot šo kā kontroles sarakstu gadījumos, kad ir kāds lemjams jautājums saistībā ar personu datiem, – pārliecinosies, vai visi principi tiek izpildīti vien- laikus, rekomendē J. Terjuhana. Principos noteiktā datu apstrāde likumīgā, godprātīgā un datu sub- jektam pārredzamā veidā nozīmē, ka **katrai datu apstrādes darbībai vienmēr jābūt tiesiski pamatotai**.

Tāpat vienmēr jābūt definētam skaidram, kon- krētam un tiesiskam mērķim, kam datu apstrāde nepieciešama. Šie mērķi jādefinē jau pirms datu ievākšanas, uzsvēr eksperte. Datu apstrādē jāievēro caurskatāmības princips – tur, kur likums to lauj, datu subjektam jāsniedz informācija par to, kur un kādiem mērķiem viņa dati tiek izmantoti.

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 aprīti un ar ko atceļ direktīvu 95/46/EK.

Jāatceras, ka dati jāvāc pietiekamā apjomā, lai izpildītu mērķi, bet ne vairāk. „Nedrīkst turēties pie principa – vākt visu pēc iespējas vairāk, gan jau reiz noderēs. Tas tiktu uzskatīts par pārmērīgu datu apstrādi,” piebilst J. Terjuhana.

Svarīgi arī atcerēties, ka datiem jābūt precīziem un, ja vajadzīgs, atjauninātiem (jānosaka iekšējā kārtība procedūrai, kā tas notiek, – tā jaieraksta uzņēmuma politikā, jāparedz IT sistēmās, jāinformē darbinieki). Katram datu veidam jābūt arī noteiktam glabāšanas laikam, kam jāseko līdzi, un, noteiktajam periodam beidzoties, dati jādzēš. Normatīvie akti šo periodu lielākoties nenosaka, tomēr dažiem datu veidiem (piemēram, grāmatvedībā vai NILLTPFN izpētes jomā) tie var būt definēti.

Uzmanība jāpievērš arī datu drošībai – lai dati netiek pazaudēti, lai tiem nevar piekļūt nesankcionētas personas; trešajām personām (t.sk. uz trešājām valstīm) datus nedrīkst nodot bez pienācīgiem piesardzības pasākumiem (kā arī tiesiskā pamata).

No Vispārīgajā datu regulā paredzētajiem sešiem datu apstrādes tiesiskajiem pamatiem NILLTPFN jomā varētu būt iespējams pielietot četras:

- līguma noslēgšana un izpilde,
- juridisks pienākums – normatīvo aktu noteikts pienākums ievākt konkrētus datus,
- sabiedrības intereses – normatīvo aktu noteiktas tiesības ievākt datus,
- pārziņa leģitīmās intereses.

Datu subjektu tiesības noteiktos gadījumos (sabiedribai nozīmīgu mērķu sasniegšanai) var tikt ierobežotas, un NILLTPFN pieder pie šiem gadījumiem. Piemēram, var tikt ierobežotas datu subjektu tiesības saņemt informāciju par to, ka par viņiem tiek veikta izpēte.

Nododot personas datus uz trešajām valstīm (ārpus ES un EEZ), jāņem vērā, vai konkrētā valsts ietilpst Eiropas Komisijas apstiprinātajā sarakstā kā droša valsts datu aizsardzības jomā. Uz šīm valstīm var nodot datus bez papildu garantijām. Taču, nododot datus uz citām trešajām valstīm, jāizmanto Vispārīgās datu regulas 46. pantā minētie līdzekļi – standartklauzulas, rīcības kodeksi, sertifikācijas mehānismi, līgumi starp iestādēm. Jāņem vērā, ka arī datu nodošanai uz ASV vairs nevienā gadījumā nav piemērojami vienkāršotie noteikumi, jo „privātuma vairoga” programma vairs nav spēkā. Ātsevišķos gadījumos datu nodošanai uz trešajām valstīm var noderēt arī datu subjekta piekrīšana, līguma noslēgšana, likumīgo prasību ištenošana vai svarīgi iemesli sabiedrības interesēs, apliecinā J. Terjuhana.

Kam pievērst uzmanību ikdienas praksē

EDVĪNS DRABA, ZAB SORAINEN vecākais jurists, seminārā sniedza ieteikumus, kā ievērot datu aizsardzības prasības, praktiski veicot NILLTPFN procedūras.

Veicot klienta izpēti, svarīgi pārliecināties, ka, iegūstot no klienta jebkādu pamatojošo informāciju, tā ir saistīta ar konkrēto klienta izpētes mērķi (piemēram, pamato konkrētu darījumu, sniedz priekšstatu par klienta izglītību un pieredzi, pamato līdzekļu izcelsmi u.tml.), rekomendē Finanšu un kapitāla tirgus komisijas 2021. gada 21. decembrī izdotie ieteikumi Nr. 169 „Ieteikumi noziedzīgi

Datu apstrādē jāievēro caurskatāmības princips – tur, kur likums to īauj, datu subjektam jāsniedz informācija par to, kur un kādiem mērķiem viņa dati tiek izmantoti.

iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas un sankciju riska pārvaldišanas iekšējās kontroles sistēmas izveidei un klientu izpētei”. E. Draba norāda, ka pārmērīga datu vākšana var pārkāpt datu aizsardzības regulejumu.

Likuma subjekts klienta izpētes procesā drīkst pieprasīt informāciju arī no trešajām personām (piemēram, klienta sadarbības partneriem), nosaka NILLTPFN likuma 28. pants. Tāpat likuma subjektam ir arī pienākums iegūt personu identificējošā dokumenta kopiju, kuru var uzglabāt gan papīra, gan elektroniskā (skēnētā) formātā.

Iegūstot datus klienta izpētes ietvaros, jāpatur prātā datu iegūšanas nolūks, un tas jānošķir no ciem datu iegūšanas nolūkiem, kas nav saistīti ar NILLTPFN likuma izpildi. Protī, NILLTPFN likuma nolūkos iegūtus datus nedrīkst izmantomēt ciem, piemēram, komerciāliem mērķiem, brīdina E. Draba.

Apstrādājot politiski nozīmīgu personu datus, jāatceras, ka tie saistīti ar politisko pārliecību, kas Vispārējās datu regulas izpratnē ir īpašas kategorijas personas dati (regulas 9. pants). Šo datu apstrāde pieļaujama būtisku sabiedrības interešu dēļ, kas nostiprinātas dalībvalsts normatīvajos aktošos. Vienlaikus jāatceras, ka pastāv vairāki izaicinājumi. Pirmkārt – kā noteikt šo personu loku? „Neraugoties uz to, ka NILLTPFN likums uzskaita diezgan daudz dažādu amatu, kas iekļaujami zem politiski nozīmīgas personas termina, tomēr likumā tiek lietota frāze „tai skaitā”, kas nozīmē, ka „politiski nozīmīga persona” aizvien ir atvērta definīcija, un likuma subjektam pašam ir jāspēj noteikt, vai persona ir tāda vai nav. Turklat ir vēl divas apakškategorijas – politiski nozīmīgo personu ģimenes locekļi un ar politiski nozīmīgām personām cieši saistītas personas, kas atkal ir potenciāli ļoti plaša kategorija,” uzsver E. Draba.



JŪLIJA TERJUHANA

Zvērinātu advokātu biroja Sorainen juriste, sertificēta datu aizsardzības speciāliste

EDVĪNS DRABA

Zvērinātu
advokātu
biroja
Sorainen
vecākais
jurists



► Saskaņā ar NILLTPFN likuma 10.¹ pantu likuma subjektam ir pienākums pārbaudīt, ka par augstākās vadības locekli vai šā likuma prasību ievērošanu atbildīgo darbinieku var būt persona, kas atbilst likumā izvirzītajām prasībām (t.sk. nav sodita). Līdz ar to likuma subjektam jāpieprasī dati no Sodu reģistra, un jāatceras, ka arī tie ir sensitīvi dati, kuru apstrādē un uzglabāšanā jāievēro īpaša piesardzība. „Pieķluvei šādiem datiem jābūt ierobežotai arī uzņēmuma iekšienē,” atgādina eksperts.

Likuma subjektiem ir pienākums arī ziņot par aizdomīgiem darījumiem. Šai gadījumā jāpievērš uzmanība tam, ka NILLTPFN likumā ieviests jauns pants (3.¹), kas paredz, ka faktiski jebkurai personai ir pienākums ziņot Finanšu izlūkošanas dienestam par aizdomīgiem darījumiem. Arī uz šo personu attiecas likuma 38. pants, kas paredz aizliegumu informēt klientu, patieso labuma guvēju, kā arī citas personas par to, ka ziņas par klientu vai tā darījumu ir sniegtas Finanšu izlūkošanas dienestam.

Klienta izpētes gaitā iegūto informāciju, kā arī informāciju par klienta veiktajiem maksājumiem un saraksti ar klientu ir pienākums glabāt vēl piecus gadus pēc darījuma attiecību izbeigšanas vai gadījuma rakstura darījuma veikšanas. „Tātad ir pamats glabāt visus klienta personas datus, kas ietilpst šo trīs punktu tvērumā, taču ne citu informāciju, uz kuru var attiekties citi glabāšanas termiņi,” infor-

mē jurists. **Pēc glabāšanas termina beigām likuma subjektam ir pienākums (nevis tiesības) iznīcināt tā rīcībā esošos dokumentus un informāciju par personu**, un šī procedūra ir skaidri jāparedz iekšējās kontroles sistēmas dokumentācijā. „Ja šāda kārtība iekšējās kontroles sistēmā nav paredzēta, Valsts ieņēmumu dienesta prakse, kas apstiprināta arī tiesu praksē, ir klasificēt to kā pārkāpumu,” brīdina E. Draba.

„Pašlaik ES līmenī nav vienotas un harmonizētas izpratnes par to, kā ir nošķiramas prasības, kas attiecas uz AML, no prasībām, kas attiecas uz personas datu aizsardzību. Tomēr paredzams, ka turpmāk likuma subjektiem aizvien vairāk vajadzēs piedomāt par to, kādus personas datus un kā apstrādāt AML kontekstā. Iespējams, nākotnē būs aizvien grūtāk pamatot neierobežotu personas datu apjomu apstrādi, balstoties tikai uz AML regulējuma izpildi,” secina eksperts.

Vai pakalpojumi uzņēmumu grupas ietvaros arī pakļaujami NILLTPFNL prasībām?

ALISA LEŠKOVIČA, ZAB SORAINEN zvērināta advokāte, semināra noslēgumā atbildot uz jautājumiem, aplūkoja interesantu un bieži neskaidrības radošu aspektu – vai NILLTPFN likuma prasības attiecas arī uz uzņēmumiem, kas sniedz finanšu pakalpojumus saistītajiem uzņēmumiem?

PERSONAS DATU APSTRĀDE,

Datu valsts inspekcija (DVI) sniegusi atbildi uz jautājumu par to, vai bankai ir obligāti nepieciešams nodot maksājuma veicēja personas kodu, personas konta numuru un citus personas datus maksājuma saņēmējam.

Sniedzot atbildi, DVI skaidro, ka banku tiesības, funkcijas un darbību nosaka banku sektora tiesiskais regulējums. Tiesību akti stingri nosaka kārtību, kādā veidā un kāda informācija tiek apstrādāta, veicot elektronisku maksājumu.

Banku darbību regulējošie tiesību akti uzliek pienākumu bankai:

- identificēt maksātāju un maksājuma saņēmēju¹;
- nodrošināt, ka maksājumā ir norādīts maksātāja vārds

un uzvārds vai nosaukums, maksātāja maksājuma korts, maksātāja adrese, klienta identifikācijas numurs (personas kods) vai dzimšanas datums un vieta².

Tāpat ņemams vērā, ka no nozares vadlīnijām izriet banku pienākums, saņemot jebkādu maksājumam pievienoto informāciju, neatkarīgi no tā, vai tā ir obligāti norādāma, šo informāciju nodot maksājuma saņēmējam³. Tas nozīmē, ka visu informāciju, kas tiek ievadīta

maksājuma uzdevumā, saņems arī maksājuma saņēmējs, un bankai nav tiesību patvaišīgi kādu no šīs informācijas dzēst.

Bankai noteiktais pienākums identificēt gan maksātāju, gan maksājuma saņēmēju ir noteikts, lai novērstu noziedzīgi iegūtu līdzekļu legalizēšanu. Starptautiskās organizācijas Financial Action Task Force (FATF) rekomendācijās noteikts, kādai informācijai jābūt norādītai pārrobežu transakcijās (pārvedumos) par maksājuma veicēju, tostarp maksātāja vārds (uzvārds), maksātāja konta numurs, kur tāds tiek lietots, lai apstrādātu, maksātāja adrese, vai personas kods, vai klienta identifikācijas numurs, vai dzimšanas datums un vieta. Līdzīgi informācijai jābūt norādītai arī

¹ Maksājumu pakalpojumu un elektroniskās naudas likuma 70. panta pirmās daļas 1. punkts.

² Eiropas Parlamenta un Padomes regulas (ES) 2015/847 par līdzekļu pārvedumiem pievienoto informāciju un ar ko atcel regulu (EK) Nr. 1781/2006 4. panta 1. punkts.

³ Eiropas Maksājumu Padomes izdotie SEPA kredīta pārvedumu shēmas noteikumi.

„Vispirms jāpievērš uzmanība finanšu iestādes definīcijai, kas paredz, ka finanšu iestāde ir jebkurs komersants, kas nav kreditiestāde, bet sniedz vienu vai vairākus finanšu pakalpojumus, piemēram, izsniedz kreditus, aizdevumus, galvojumus,” norāda A. Leškoviča. VID uzkata, ka nav būtiski, vai finanšu pakalpojumi tiek sniegti ārējiem klientiem vai saistītajiem uzņēmumiem, tāpat nav būtiski, vai tas ir komersanta pamatdarbības veids. „VID ieskatā pietiek pat ar vienu aizdevumu citam uzņēmumam, lai aizdevēju uzskatītu par finanšu iestādi. Neesmu gan pārliecināta, ka šāds pienēmums ir pareizs, drīzāk teiktu, ka var pastrīdēties. Taču šāds VID uzkats ir pasts vairākās lietās, kas tika skatītas tiesā. Tīklidz sniedzat kādam aizdevumu, jūs kļūstat par NILLTPFN likuma subjektu un jums ir jāsniedz VID informācija, ka jums ir arī šāds darbības veids,” atklāj advokāte. Tiesa šo jautājumu gan vairāk skatot no saimnieciskās darbības perspektīvas – uzņēmuma atbilstība finanšu iestādes statusam tiek vērtēta atkarībā no tā, cik bieži un sistemātiski tas sniedz finanšu pakalpojumus un kāds ir šo darījumu apjoms. Bijusi lieta, kurā uzņēmums izsniedzis sešus aizdevumus saistītam uzņēmumam, un šie aizdevumi tiesas skatījumā atzīti par pietiekami biežiem finanšu pakalpojumiem, lai aizdevēju uzskatītu par finanšu iestādi. Tiesas vērtējumā nav nozīmes, ka daļa no aizdevumiem tika izsniegti saistītiem uzņēmumiem, tāpēc jāņem vērā, ka AML prasības noteiktī jāievēro arī šādās situācijās, secina A. Leškoviča.

Taču no 2022. gada likumā stājušies spēkā grozījumi, kas paredz, ka situācijā, ja finanšu iestāde tikai grupas ietvaros vai kooperatīvās sabiedrības biedriem sniedz kreditēšanu, finanšu lizingu vai galvojumu to pamatdarbības nodrošināšanai (un izpildās vairāki citi likumā minētie nosacījumi par uzņēmumu grupas sastāvu, patiesajiem labuma guvējiem u.c.), tad iespējams piemērot izņēmumu un neattiecināt NILLTPFN likuma prasības, informē eksperte.

Tāpat uzņēmumiem bieži neesot skaidrs, vai uz tiem attiecas NILLTPFN likuma prasības, ja grāmatvedības pakalpojumi netiek sniegti ārējiem klientiem, bet tikai meitas kompānijām. „Pēc būtības uzņēmums veic tādu kā iekšējā grāmatvedības departamenta funkciju. VID atbilde gan ir viennozīmīga – arī tad, ja uzņēmumi sniedz grāmatvedības pakalpojumus tikai savas grupas ietvaros, tikai saistītiem uzņēmumiem, uz tiem attiecas visas NILLTPFN likuma prasības. Šajā gadījumā gan varētu runāt par to, ka riska līmenis ir zemāks, to mēr risku novērtējums un saistīto uzņēmumu izpēte tāpat ir jāveic. Bieži uzņēmumi aizbildinās, ka šāda izpēte nav jāveic, jo patiesais labuma guvējs ir viens un tas pats, lai arī ir trešās valsts pilsonis, izaugs Latvijā u.tml. Tiesas ieskatā tam nav nozīmes, klients ir jāvērtē, un tāpat ir jāziņo par aizdomīgiem darījumiem,” norāda A. Leškoviča.

B JP

Semināra atzinās apkopoja
IKARS KUBLIŅŠ

ALJSA LEŠKOVIČA

Zvērinātu
advokātu
biroja
Sorainen
zvērināta
advokāte



veicot bankas maksājumus

iekšzemes transakcijās, ja vien to nevar padarīt pieejamu saņēmējbankai un attiecīgajām uzraudzības iestādēm citos veidos. Šajā gadījumā maksājuma uzdevums ietver tikai konta numuru vai unikālo transakcijas (pārveduma) numuru, nodrošinot minēto identifikatoru sasaisti ar transakciju (pārvedumu) un maksātāju vai saņēmēju.

Nemot vērā minēto, banku veiktā personas datu apstrāde – informācijas par maksātāju (vārdu, uzvārdu, personas kodu, konta numuru u.c.) nodošana maksājuma saņēmējam pamatojama ar uz pārzini attiecināmu juridisku pienākumu vai pārziņa vai trešās personas leģitīmām interesēm. Maksātāja bankas konta un personas koda nodošanas tiesiskais pamats at-

karībā no maksājuma veikšanas mērķa, maksātāja un maksājuma saņēmēja statusa un maksājuma veikšanas apstākļiem var būt Vispārējā datu aizsardzības regulas 6. panta 1. punkta b, c vai f apakšpunkts, kā arī konkrētās situācijās var būt piemērojami vairāki minētie tiesiskie pamati vienlaikus.

DVI arī norāda, ka personas vārds un uzvārds ir vispārpriņemti identifikatori salīdzinoši vienkāršās sadzīviskās situācijās un vairumā gadījumu spēj nodrošināt unikālu personas identifikāciju, taču, veicot komercdarbību, personas vārds un uzvārds nevar kalpot kā unikāls identifikators. Latvijā unikālais personas identifikators ir personas kods. Tāpēc bankām, lai identificētu maksātāju, ir jāizmanto gan

personas vārds, uzvārds, gan arī personas kods.

Pastāv situācijas, kurās konkrētu personu grupu maksājuma saņēmējiem ir nepieciešams zināt personas koda, lai spētu identificēt konkrēto maksātāju. Šādas personas var būt, piemēram, juridiskās personas, kas sniedz elektroenerģijas, komūnālos u.c. pakalpojumus, parādu atguvēji, nebanku aizdevēji⁴, grāmatvedības uzskaites dokumentu saņēmēji⁵ u.c. Personas koda nenorādišana var būtiski apgrūtināt šo personu darbu un iespēju identificēt konkrēto klientu, kas veic maksājumu, atbilstoši normatīvo aktu prasībām.

Detalizēta atbilde uz jautājumu lasāma DVI tīmekļvietnē publicētajā atbildes uz jautājumu izrakstā⁶.

B JP

⁴ MK 2018. gada 3. jūlija noteikumu Nr. 392 „Kārtība, kādā Noziedzīgi legūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanas likuma subjekts veic klienta neklāties identifikāciju” 7.3. punkts.

⁵ Grāmatvedības likuma 11. panta piektā daļa.

⁶ Skatīt:
<https://www.dvi.gov.lv/lv/skaidrojumi-un-viedokli#par-personas-datu-apstradi-veicot-elektroniskos-maksajumus>