IETEIKUMI

Vispārīgās datu aizsardzības regulas piemērošanai

Konsolidētā redakcijā ar grozījumiem, kas izdarīti 08.01.2021.

Janvāris, 2021

SATURS

IZMANTOTIE JĒDZIENI

Zemāk ir norādīti saīsinājumi un jēdzieni, kas lietoti Ieteikumos. Ja šeit nav skaidrots kāds jēdziens, tad tas tiek lietots Vispārīgās datu aizsardzības regulā noteiktajā izpratnē:

29. panta darba grupa	Eiropas Parlamenta un Padomes Direktīvas Nr.95/46/EK "Par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti" 29. pantā noteiktā kārtībā izveidota darba grupa
Apstrādātājs	kredītiestādes sadarbības partneris (gan fiziska, gan juridiska persona), kura kredītiestādes vārdā un interesēs apstrādā kredītiestādes rīcībā esošus personas datus
Dati	jebkura informācija, kas attiecas uz identificētu vai identificējamu datu subjektu. Ar datiem saprot jebkuru informāciju, kas sniedz kādas ziņas par identificējamu datu subjektu, tai skaitā objektīvi fiksējamā informācija (piemēram, personas vārds, uzvārds, personas kods, adrese, tālruņa numurs, konta numurs un konta informācija, piemēram, maksājumi, apgrozījums) un arī subjektīva informācija par datu subjektu (piemēram, personas psiholoģiskais raksturojums, personas atrašanās riska grupā, personas kredītreitings). Tāpat ar datiem ir saprotama jebkādā formā fiksēta informācija, t.i., gan rakstiski papīra formātā, gan elektroniskā formātā, gan audio un video ierakstos fiksēti dati, gan foto, gan fiksēti kā biometriskie dati
Datu aizsardzības speciālists	speciālists, kurš saskaņā ar piemērojamiem normatīvajiem aktiem ir tiesīgs veikt datu aizsardzības speciālista pienākumus
Datu subjekts	▪ kredītiestāžu klients (t.sk. saimnieciskās darbības veicēji, potenciālais klients, patiesā labuma guvējs, saistītās personas, galvinieks, sadarbības partneri – fiziskās personas, pilnvarotās personas un jebkura cita identificēta vai identificējama persona, kura ir fiziska persona un kuras datus kredītiestāde apstrādā); ▪ darbinieks, pretendents, kuru datus kredītiestāde apstrādā
Direktīva	1995. gada 24. oktobra Eiropas Parlamenta un Padomes Direktīva Nr.95/46/EK "Par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti"
DVI	Datu valsts inspekcija
EDAK	Eiropas Datu aizsardzības kolēģija – Eiropas Savienības struktūra, kas ir izveidota saskaņā ar Regulas VII nodaļas 3. iedaļu un ir 29. panta darba grupas tiesību un saistību pārņēmēja
EEZ	Eiropas Ekonomiskā Zona
ES	Eiropas Savienība
FKTK	Finanšu un kapitāla tirgus komisija
Ieteikumi	šie Ieteikumi atbilstības Vispārīgās datu aizsardzības regulas prasībām nodrošināšanai
Īpašu kategoriju dati	dati, kas sniedz informāciju par datu subjekta rasi, etnisko piederību, politiskiem uzskatiem, reliģisko vai filozofisko pārliecību vai dalību arod biedrībā, kā arī ģenētiskie dati, biometriskie dati (ja tie tiek izmantoti ar nolūku veikt fiziskās personas unikālu identifikāciju), veselības dati vai dati par fiziskās personas dzimumdzīvi vai seksuālo orientāciju
Kredītiestāde	Latvijas Finanšu nozares asociācijas biedrs
Latvija	Latvijas Republika
NILLTPFNL	Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas likums
Pārzinis	kredītiestāde, kuras vārdā un interesēs datu subjekta dati tiek apstrādāti un kura atbild par datu apstrādi
Regula	Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regula (ES) 2016/679 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)
Trešā persona	jebkura persona, kura nav pārzinis, pārziņa darbinieks, pārziņa tieši pilnvarota persona un nav apstrādātājs un kurai ir savi neatkarīgi nolūki datu apstrādei
Trešā valsts	jebkura valsts, kura nav ES vai EEZ dalībvalsts
Uzraudzības iestāde	Datu valsts inspekcija vai cita attiecīgā uzraudzības iestāde atbilstoši Regulā noteiktajam

(Ar grozījumiem, kas izdarīti 08.01.2021.)

1. IEVADS

Šis skaidrojošais praktiskais palīgmateriāls jeb Ieteikumi ir izstrādāti, lai kredītiestādēm skaidrotu Regulas normatīvo regulējumu un atvieglotu Regulas piemērošanu, tādējādi arī nodrošinot atbilstošu personas datu apstrādi kredītiestādes ikdienas darbībā.

Regula tika pieņemta 2016. gada 27. aprīlī, un saskaņā ar Regulas 99. pantu tā stājās spēkā divdesmitajā dienā pēc publicēšanas Eiropas Savienības Oficiālajā Vēstnesī, t.i., 2016. gada 24. maijā, bet Regulu jāpiemēro no 2018. gada 25. maija. Atkāpes no šiem termiņiem netiek paredzētas, tāpēc Regula no 2018. gada 25. maija ir tieši piemērojama un pilnībā saistoša datu apstrādei ES un arī ārpus ES, ja tiek piedāvāti pakalpojumi un/vai preces datu subjektiem ES vai tiek veikta datu subjektu uzvedības novērošana, ciktāl viņu uzvedība notiek ES.

Datu aizsardzības uzraudzības iestādēm no 2018. gada 25. maija ir tiesības izmantot ar Regulu piešķirtās pilnvaras arī attiecībā uz jaunajiem nosacījumiem un prasībām, *piemēram, veikt izmeklēšanu, pieprasīt informāciju no datu pārziņa un apstrādātāja, piemērot brīdinājumus, veikt pārbaudes, piemērot pagaidu vai pastāvīgu datu apstrādes aizliegumu un uzlikt administratīvo naudas sodu*.

1.1. Ieteikumu mērķi

Ieteikumu mērķis ir veicināt vienotu pieeju personas datu aizsardzības prasību izpildē kredītiestāžu sektorā, lai veicinātu un uzlabotu sadarbību ar uzraudzības iestādi un citām iestādēm, veidotu vienotu izpratni par Regulā iekļautiem pienākumiem un tiesībām, kā arī lai uzlabotu komercdarbības un finanšu pakalpojumu vidi Latvijā.

Ieteikumi paredzēti, lai veicinātu izpratni par datu aizsardzības regulējumu un to ietekmi uz kredītiestāžu sektoru. Ieteikumiem nav absolūts raksturs un Ieteikumi nav tiesiski saistošs dokuments, bet atbalsta materiāls, proti, Ieteikumu ievērošana veicinātu Regulas prasību ieviešanu un ievērošanu katra adresāta individuālajos procesos. Regulas ieviestās izmaiņas dod iespēju pārskatīt un uzlabot esošos personas datu apstrādes procesus. Datu apstrādes procesu pārskatīšana jau pirms Regulas piemērošanas uzsākšanas brīža var veicināt iekšējo procesu optimizāciju un atbilstības risku vadības nodrošināšanu.

Jauns regulējums var radīt neskaidrības normu iztulkošanā vai piemērošanā, tādējādi ar šo Ieteikumu palīdzību iespējams veidot vienotu un ar uzraudzības institūcijām saskaņotu izpratni par atsevišķiem ar datu aizsardzību saistītiem jautājumiem kredītiestāžu sektorā.

Regula paredz ne tikai noteiktu prasību pasīvu ievērošanu, bet arī prasību organizācijām pierādīt attiecībā uz uzraugošajām iestādēm, ka Regulas nosacījumi tiek konsekventi ievēroti, t.i., tiek nodrošināta pārskatatbildības principa ievērošana. Tādējādi šajos Ieteikumos ir iekļauti atsevišķi ieteikumi, kas palīdzēs kredītiestādēm nodrošināt pārskatatbildības principa ievērošanu.

Regula nosaka, ka pārzinim un apstrādātājam ir pienākums sadarboties ar uzraudzības iestādi dažādās situācijās, tāpēc Ieteikumos tiks paredzēti arī ieteikumi sadarbībai ar uzraudzības iestādi, lai veidotu vienotu pieeju un vienuviet pieejamu informāciju par rīcību, kas nodrošinātu veiksmīgu abpusēju sadarbību.

Regulā īpaši ir izcelts pārredzamības princips, saskaņā ar kuru kredītiestādes nodrošina datu subjektu informēšanu par ar šīs personas datiem veiktām datu apstrādes darbībām un padara šīs datu apstrādes darbības pēc iespējas pārskatāmas. Lai pārredzamības principu ieviestu un uzturētu, ir nepieciešams apzināties kāda informācija ir sniedzama datu subjektiem, izvērtēt informācijas sniegšanas veidu, lai informēšana notiktu vienkārši un skaidri, tādā veidā veicinot klienta un citu personu, kuru datus apstrādā kredītiestāde, uzticēšanos kredītiestādei kā pārzinim. Īstenojot šo principu, kredītiestādei ir iespējams parādīt kredītiestādes klientiem un sabiedrībai atbildīgu pieeju datu aizsardzībai, kas var sniegt arī kredītiestādei konkurētspējas priekšrocību attiecībā pret citiem finanšu pakalpojumu tirgus dalībniekiem, kuri neizvirza savu klientu datu aizsardzību kā prioritāti.

Kā tas noteikts Regulas 39. apsvērumā, Regulā ietvertā pārredzamības principa pamatā ir prasība, ka visa informācija un saziņa, kas saistīta ar personas datu apstrādi, ir viegli pieejama un viegli saprotama un ka ir jāizmanto skaidra un vienkārša valoda. Ieteikumi sniedz iespēju kredītiestādēm vienādot pieeju saziņai ar datu subjektiem datu aizsardzības jautājumos un ieteikumus kā uzskatāmi parādīt datu subjektiem kredītiestādes veikto datu apstrādes darbību atbilstību Regulai.

1.2. Regulas rašanās nepieciešamība un tiesiskais pamatojums

Latvijā personas datu apstrāde līdz 2018. gada 25. maijam notiek saskaņā ar Fizisko personu datu aizsardzības likumu, kas ieviesa Direktīvas prasības. Direktīva tika pieņemta 1995. gada 24. oktobrī un uz Regulas pieņemšanas brīdi jau bija pagājuši vairāk nekā divdesmit gadi, kas, salīdzinot tehnoloģiju attīstību tempu, ir ļoti ilgs laiks. Šajā periodā digitālās tehnoloģijas ir būtiski attīstījušās un pilnībā pārveidojušas arī komercdarbības vidi. Ātrā tehnoloģiju attīstība ir atnesusi sev līdz arī jaunus izaicinājumus personas datu aizsardzības jomā[1].

Šobrīd tehnoloģijas ļauj izmantot, uzglabāt un apstrādāt personas datus gan kredītiestādēm, gan privātiem uzņēmumiem, gan valsts iestādēm u.c., lai varētu pildīt savas funkcijas līdz šim nepieredzētos apjomos un ātrumos. Turklāt arī patērētāju viedokļu pētījumi atklāja, ka patērētāji ir norūpējušies par savu datu drošību un vēlas lielāku kontroli par saviem datiem un to izmantošanu.

Personas datu aizsardzībai ir centrālā loma Eiropas digitālajā programmā un Eiropas 2020 stratēģijā. Regulāras digitālo tehnoloģiju un elektronisko pakalpojumu izmantošanas rezultātā tiek apstrādāti milzīgi datu apjomi, kā rezultātā tiek pieņemti lēmumi un radīti fizisku personu profili, kas var atstāt gan pozitīvas, gan arī negatīvas sekas attiecīgiem datu subjektiem, tāpēc palielinājusies vajadzība pēc jauniem personas datu aizsardzības mehānismiem.

Ņemot vērā situāciju, kas veidojās no Direktīvas pārņemšanas un dažādām ES dalībvalstu praksēm, kuras, izmantojot Direktīvā pieļaujamās atkāpes, savos nacionālajos regulējumos nostiprināja atšķirīgas prasības datu apstrādei, kas savukārt apgrūtināja komersantiem pakalpojumu sniegšanas brīvības principa pilnvērtīgu nodrošināšanu ES tirgū un atšķirīgu interpretāciju vispārīgiem principiem, tika akcentēta jauna regulējuma nepieciešamība. Tādējādi, lai nodrošinātu vienādu prasību esamību visās ES dalībvalstīs, par jaunā ES pieņemamā tiesību akta formu tika izvēlēts regulas formāts.

Regula atšķirībā no Direktīvas ir tieši piemērojama visās ES dalībvalstīs un uzliek saistības tieši pārziņiem, kuri apstrādā personas datus. Saskaņā ar Regulu katrā dalībvalstī tiks izveidota (vai pārveidota esošā) uzraudzības iestāde vai vairākas uzraudzības iestādes, kas darbosies vienotā uzraudzības iestāžu tīklā, savstarpēji sadarbojoties, ar mērķi vienoti uzraudzīt datu apstrādes procesus un nodrošināt datu aizsardzību to apstrādes procesā ES. Tāpat Regula ievieš vairākas izmaiņas salīdzinot ar iepriekšējo regulējumu. Piemēram, pārzinim bija nepieciešams reģistrēt paaugstināta riska datu apstrādes nacionālajā uzraudzības iestādē, bet, sākot ar Regulas piemērošanu no 2018. gada 25. maija, vairs nav nepieciešams reģistrēt uzraudzības iestādēs datu apstrādes, bet pārzinim pašam jāuztur apstrādes darbību reģistrs un jāidentificē paaugstināta riska personas datu apstrādes. Savukārt, ja riskus nav iespējams minimizēt, par to jākonsultējas ar uzraudzības iestādi.

Regula ievieš arī citus jaunus datu subjektu tiesību aizsargājošus pasākumus, piemēram, datu pārnesamības, datu subjekta iebilšanas tiesību, personas datu aizsardzības pārkāpumu uzskaiti un ziņošanas pienākumu.

[1] Sk. arī Eiropas datu aizsardzības uzrauga viedokli: https://edps.europa.eu/sites/edp/files/publication/17-01-13_big_data_ex_summ_en.pdf

Tomēr kopumā Regula nav veikusi *revolūciju* datu aizsardzības jomā, bet gan Regula ir datu aizsardzības vides un tehnoloģisko risinājumu attīstības rezultāts. Tādējādi Regula saglabā jau Direktīvā nostiprinātos datu apstrādes pamatprincipus un galvenos tiesību institūtus, tomēr, ņemot vērā mūsdienu digitālās vides radītos riskus, arī papildina Direktīvā izvirzītos mērķus un risinājumus, pielāgojot tos mūsdienu situācijai un tehnoloģiju attīstībai.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

1.3. Regulas vieta tiesību sistēmā

Tiesības uz privāto dzīvi ir universāli atzītas cilvēka pamattiesības, kuras ir nostiprinātas gan Eiropas Padomes Cilvēktiesību Konvencijas 8. pantā, gan Eiropas Pamattiesību Hartas 7. pantā (saskaņā ar Lisabonas līgumu Eiropas Pamattiesību Hartai ir saistošs raksturs). Tiesības uz datu aizsardzību ir cēlušās no tiesībām uz privāto dzīvi, bet datu aizsardzība ir arī būtisks elements citu tiesību realizēšanai, piemēram, tiesībām uz vārda brīvību. Tomēr tiesības uz savu personas datu aizsardzību nav absolūtas tiesības un tās var tikt ierobežotas, ja tas ir nepieciešams, lai ievērotu būtiskas sabiedrības intereses un citu personu pamatoto tiesību aizsardzību.

Tiesības uz datu aizsardzību ir nostiprinātas ne tikai Eiropas Pamattiesību Hartā, bet arī Līguma par Eiropas Savienības darbību 16. pantā. Turklāt Līgums par Eiropas Savienības darbību ir viens no dokumentiem, kurā personas tiesības uz savu personas datu aizsardzību ir nostiprinātas, kā patstāvīgi ES atzīstams cilvēktiesību elements, nevis tikai kā tiesību uz privātumu sastāvdaļa.

1.4. Regulas piemērojamība

Regula ir tiesību akts, kas ir tieši piemērojams visās ES dalībvalstīs, tādējādi nosakot vienādas juridiskās prasības visās ES dalībvalstīs. Lai gan Regula ir vispārpiemērojama, tajā pašā laikā Regula paredz arī iespēju dalībvalstīm pieņemt vairākas atkāpes no tās. Līdz ar to pastāv iespēja, ka starp ES dalībvalstīm pilnībā netiks novērsta datu aizsardzības regulējuma sadrumstalotība. Kredītiestādēm Regula ir jāpiemēro tiešā veidā, taču, ja Latvijas normatīvie akti nosaka kādas papildu tiesības vai pienākumus attiecībā uz datu apstrādi, kredītiestādei savā darbībā jāievēro arī Latvijā spēkā esošie normatīvie akti.

Tikšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR Darba grupu 2018. gada 21. maijā Datu valsts inspekcija pauda viedokli, ka juridisko personu dati atrodas ārpus Regulas tvēruma. Par izņēmumu var uzskatīt pašnodarbināto personu datus, jo tie nav iekļauti publiskajos reģistros. Taču katrā konkrētā situācijā jāizvērtē sadarbības konteksts un, ja tas ir saistīts ar komercdarbību, pašnodarbinātās personas datus var uzskatīt par juridiskās personas datiem. Vienlaicīgi DVI aicina izvērtēt, vai juridisko personu pārstāvju (fizisko personu) dati ir attiecināmi uz šīm juridiskajām personām un tiek izmantoti tikai šo juridisko personu vajadzībām. Piemēram, turīgo personu saraksta sagatavošana būtu uzskatāma par fizisko personu datu apstrādi.

Savukārt tikšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR Darba grupu 2019. gada 7. martā Datu valsts inspekcija pauda viedokli, ka attiecībā uz bankomātu tukšošanai Regula nebūtu piemērojama, jo šajā gadījumā trūkst automātiskās apstrādes elements. Taču līgumā ar sadarbību partneri jābūt atrunātām prasībām attiecībā uz pakalpojumu nodrošināšanu un konfidencialitātes ievērošanu.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

1.5. Ieteikumos apskatāmo jautājumu izvēle

Kredītiestāžu sektora specifika ir saistīta ar liela skaita privātpersonu datu apstrādes nepieciešamību, lai nodrošinātu finanšu pakalpojumu sniegšanu, tādējādi vairumā gadījumu kredītiestādes būs uzskatāmas par pārziņiem, kas veic liela apjoma datu apstrādes dar-

bības. Turklāt saistībā ar kredītiestāžu sniegtajiem pakalpojumiem personas dati var tikt nodoti ārpus ES un EEZ. Šo iemeslu dēļ kredītiestādēm nepieciešams saglabāt augstās prasības apstrādāto datu drošības, tiesiskuma un adekvātuma nodrošināšanai un indivīdu aizsardzībai.
Kredītiestāžu pakalpojumu nodrošināšanā ir iesaistīts liels skaits sadarbības partneru, piemēram, korespondentbankas, starptautiskas uzraudzības iestādes, maksājumu pakalpojumu sniegšanas nodrošinātāji, kredītspēju raksturojošas informācijas turētāji, tādējādi īpaša uzmanība jāveltī sadarbības jautājumiem ar datu apstrādātājiem, kuriem kredītiestādes uztic datu apstrādi, kā arī datu nodošanai citām trešajām personām.

Kredītiestādēm var būt dažādas vajadzības datu apstrādes jomā atkarībā no to darbības lieluma, proti, gan lielas pilna pakalpojumu klāsta reģionālas kredītiestāžu grupas, gan mazāki tirgus dalībnieki ar šaurāku klientu loku, gan arī atkarībā no to piedāvāto pakalpojumu un produktu loka.

Kredītiestādēm ir raksturīga arī plaša informācijas tehnoloģiju (IT) sistēmu izmantošana pakalpojumu un biznesa vajadzību nodrošināšanai, kas bieži vien ietver sarežģītas vai savstarpēji atšķirīgas sistēmas uzbūves un prasa paaugstinātu drošības uzraudzību, kā arī dažādu pasākumu veikšanu, lai kredītiestādes turpinātu nodrošināt savu datu apstrādes darbību atbilstību spēka esošiem tiesību aktiem, tai skaitā Regulai.

Vērtējot Regulas ieviešanu kredītiestāžu sektorā, ir jāņem vērā, ka jau šobrīd uz kredītiestāžu darbības nodrošināšanu attiecas liels skaits gan Latvijas spēkā esošie tiesību akti (likumi, Ministru kabineta noteikumi, FKTK izdoti tiesību akti), gan arī ES pieņemtie tiesību akti, kuri kredītiestādēm to darbību nodrošināšanā jāievēro un saprātīgi jāpiemēro kopā ar Regulas prasību īstenošanu.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

1.6. Ieteikumu adresāti

Ieteikumi ir izstrādāti ar mērķi sniegt Latvijas Finanšu nozares asociācijas biedriem atbalstu Regulas piemērošanā. Latvijas Finanšu nozares asociācija ir biedrība, kas uz brīvprātības principa pamata apvieno Latvijā reģistrētās bankas un ārzemju banku filiāles, kā arī citas finanšu institūcijas (asociētie biedri[2]).

Attiecīgi Ieteikumu adresātiem šie Ieteikumi kalpos kā līdzeklis labas prakses veidošanā attiecībā uz kredītiestādes darbību vai citu finanšu pakalpojumu sniegšanu, kas tiek veikta Latvijā. Latvijas Finanšu nozares asociācijas asociētie biedri Ieteikumus piemēro tāda apmērā, kas attiecināmas uz to darbības specifiku.

[2] https://www.financelatvia.eu/asociacija/par-asociaciju/

2. DATU APSTRĀDES PRINCIPI

Šajā nodaļā tiek sniegts vispārējs Regulā nostiprināto personas datu apstrādes principu uzskaitījums un īss skaidrojums, bet detalizēti minētie principi ir skaidroti turpmākajās Ieteikumu nodaļās, ņemot vērā to, ka turpmāk uzskaitītās prasības izriet no šiem principiem.

2.1. Likumīgums, godprātība un pārredzamība

Lai īstenotu šos principus kredītiestāžu ikdienas darbībā, kredītiestāde nodrošina pret datu subjektu godprātīgu attieksmi attiecībā uz viņa datu apstrādi jeb veic datu subjektu datu apstrādi labā ticībā. Godprātības princips pēc būtības ietver arī visus pārējos principus, jo visi principi pamatā ir vērsti, lai realizētu kredītiestādes kā pārziņa godīgu attieksmi pret datu subjektu, tai skaitā, bet ne tikai informējot viņu par datu apstrādi, neizmantojot datus citiem nolūkiem kādiem tie tikuši ievākti.

Godprātīga attieksme izpaužas kredītiestādes rīcībā, respektējot datu subjekta intereses aizsargāt savu privātumu, kā arī veicinot un atvieglojot datu subjektam tā tiesību realizēšanu, piemēram, nodrošinot vienkāršotu datu subjekta piekļuvi informācijai par tā datu apstrādi, droši glabājot datu subjekta datus, ļaujot labot neprecīzus datu subjekta datus un citu tiesību īstenošanu.

Kredītiestādes, veicot datu apstrādi, ņem vērā datu subjektu briedumu, vecumu un citus personības aspektus un neizmanto personas trūkumus un nezināšanu, lai sasniegtu savus nolūkus.

Viena no godprātības principa izpausmēm ir datu pārredzamības principa nodrošināšana, ar to saprotot, ka kredītiestāde nodrošina pilnīgu, precīzu un pārliecinošu datu subjektu informēšanu par sagaidāmo datu apstrādi un tās sekām, ja nav ierobežojumu šādas informācijas izpaušanai. Turklāt, lai šo principu īstenotu, datu subjektam informācija ir jānodrošina kodolīgā, saprotamā (ņemot vērā datu subjekta briedumu un citas īpašības, *piemēram, bērni, seniori u.c.*), viegli pārskatāmā un viegli pieejamā veidā. Tādējādi datu subjekts tiks pienācīgi informēts, apzinoties savu datu apstrādes būtību un iespējamās sekas, un šāda datu apstrāde neradīs būtisku ietekmi uz datu subjekta privātumu.

Likumīga datu apstrāde paredz, ka kredītiestāde atbildīgi izvēlas nolūkus, kādiem tā datus plāno apstrādāt, nepieļaujot tādu nolūku rašanos un īstenošanu, kuri var nepamatoti ietekmēt datu subjekta privātumu. Par likumīgiem nolūkiem viennozīmīgi atzīstami tādi nolūki, kas sabiedrībā un normatīvajos aktos ir atzīti par samērīgiem un pieļaujamiem.

Otrs būtisks likumības principa aspekts ir datu apstrādes uzsākšana tikai atbilstoša tiesiskā pamata esamības gadījumā. Pirms jebkuru datu ievākšanas, izpaušanas trešajām personām, kā arī pirms ievākto datu apstrādes nolūka maiņas ir jāizvērtē, vai šādai datu apstrādei ir piemērojams kāds no Regulā minētajiem tiesiskiem pamatiem. Savukārt gadījumā, ja tiek apstrādāti Īpašu kategoriju dati (*piemēram, dati par veselību, tautību, reliģisko pārliecību, biometriskie dati*) vai dati, kas saistīti ar datu subjekta sodāmībām, ir jānodrošina, ka attiecīgai datu apstrādei ir piemērojami īpašie Regulā noteiktie gadījumi šādu datu apstrādei.

Par šī principa piemērošanu vairāk lasiet Ieteikumu 3.2. nodaļā.

2.2. Nolūka ierobežojums

Lai ievērotu nolūka ierobežojuma principu, kredītiestādēm ir kritiski jāizvērtē katras plānotās un esošās datu apstrādes nepieciešamība. Šī principa realizācija nepieļauj datu ievākšanu un apstrādi bezmērķīgi (bez konkrēta nolūka) jeb neesot acīmredzamai un pastāvošai nepieciešamībai šādu datu apstrādei. Kredītiestādes neveic datu apstrādi, nezinot

kādiem nolūkiem un kad ievāktie dati tiktu izmantoti, kā arī neievāc datus un neuzglabā tos nekonkrētiem nākotnes nolūkiem, kuru vajadzība nav izvērtēta un realizācijas uzsākšana nav apstiprināta ar normatīvajiem aktiem, attiecīgiem kredītiestādes pārvaldes institūciju lēmumiem vai iekšējiem normatīviem dokumentiem (*piemēram, procedūrām, instrukcijām*).

Šis princips arī nosaka, ka svarīgi ir konstatēt datu ievākšanas sākotnējo nolūku, un, ja datu izmantošanas nolūks tiek mainīts un nav saderīgs ar šo sākotnējo nolūku, tad šādai datu apstrādei ir jāpārvērtē tiesiskais pamats.

Par šī principa piemērošanu vairāk lasiet Ieteikumu 3.1.nodaļā.

2.3. Datu minimizēšana

Datu minimizēšanas principu mēdz dēvēt arī par *proporcionalitātes principu, adekvātuma principu vai samērīguma principu*, bet to nozīme ir vienāda, proti, iepriekš noteiktos leģitīmos nolūkus īstenot ar minimāli nepieciešamo datu apjomu šo nolūku sasniegšanai. Šī principa īstenošanas būtība ir apstrādāt tikai attiecīgā nolūka sasniegšanai nepieciešamos datus, tādējādi samazinot apstrādāto datu apjomu. Datu minimizēšanas principa ieviešana kredītiestādes ikdienas procesos, *piemēram, pārskatot esošos risinājumus un procesus, organizējot piekļuvi datiem tikai attiecīgām struktūrvienībām, kurām tas nepieciešams pienākumu izpildei*, ļauj kredītiestādei identificēt datus, kuru apstrādes nepieciešamība attiecīgu kredītiestādes produktu un pakalpojumu nodrošināšanai ir pārvērtējama, un novērst datu pārmērīgu apstrādi, nodrošinot arī papildu iespēju demonstrēt atbilstību Regulai.

Piemērojot šo principu, kredītiestādēm ir jāapzinās, ka datu minimizēšana nav vienreizēji veicams pasākums, bet šī principa īstenošana datu apstrādes ciklā būtu jāveic regulāri, jo darījumu vide, normatīvo aktu prasības un apkārtējie apstākļi ir mainīgi.

Datu minimizācijas princips vienādi ir piemērojams gan tām datu apstrādēm, ko kredītiestādes veic iekšienē, gan arī gadījumos, ja datus ir nepieciešams nodot datu apstrādātājiem (*piemēram, samazinot nododamo datu apmēru un/vai pseidonimizējot datus*) vai izpaužot datus trešajām personām.

Par šī principa piemērošanu vairāk lasiet Ieteikumu 4.nodaļā.

2.4. Precizitāte

Precīzi dati ir viena no Regulas pamatvērtībām, jo tikai precīzi dati var nodrošināt godprātīgu un taisnīgu lēmumu pieņemšanu attiecībā uz datu subjektu. Turklāt jāņem vērā, ka neprecīzi dati atsevišķās situācijās var radīt būtiskas negatīvās sekas attiecībā uz datu subjektu, kuras nebūs taisnīgas, *piemēram, ja kredītiestāde būs ziņojusi Latvijas Bankas Kredītu reģistram vai kredītinformācijas birojiem kļūdainu informāciju par klienta aizdevuma atmaksas kavējumu, klientam var tikt liegta piekļuve citiem ar kredītrisku saistītiem produktiem ne tikai attiecīgā kredītiestādē, bet arī citās kredītiestādēs*.

Šī principa godprātīga īstenošana ir ne tikai kredītiestādes pienākums, bet ir nepieciešama veiksmīgas pamatdarbības nodrošināšanai, līdz ar to kredītiestāde izstrādā mehānismus (*piemēram, iekļaujot līgumos vai vispārējos darījumu noteikumos datu subjektam pienākumu informēt kredītiestādi par izmaiņām datos, veicot datu salīdzināšanu ar datiem citās datu bāzēs, lūdzot klientam internetbankā pārskatīt savu datu precizitāti*) kā tiks nodrošināta datu precizitāte tos pirmreizēji ievācot, kā arī turpmāk datus apstrādājot konkrētu nolūku sasniegšanai, ja dati mainās (*piemēram, klienta kontakttālruņa numura, uzvārda, adreses, personas koda maiņa*).

Regula paredz, ka iesaistīties savu datu precizitātes nodrošināšanā var arī pats datu subjekts, gan iniciējot kredītiestādei precizēt savus datus, kas atrodas kredītiestādes rīcībā,

gan arī iegūstot no kredītiestādes tajā apstrādātos datus un tādā veidā pārliecinoties, vai kredītiestādes rīcībā esošā informācija ir precīza un likumīgi apstrādāta, pieprasot kredītiestādi šo informāciju labot, ja dati ir neprecīzi.

Izstrādājot iekšējos procesus un mehānismus datu precizitātes nodrošināšanai, kredītiestādei ir jāņem vērā arī datu subjekta Regulā noteiktās tiesības un to realizācija.

Par šī principa piemērošanu vairāk lasiet Ieteikumu 5.3. un 6.nodaļā.

2.5. Glabāšanas ierobežojums

Glabāšanas ierobežojuma principa būtība ir datus glabāt tikai tik ilgi, cik tas ir nepieciešams nolūka sasniegšanai, un tiklīdz nolūks ir sasniegts dati ir jāizdzēš vai informācijas nesēji, kuros dati ir fiksēti, jāiznīcina.

Tomēr šis princips nebūtu jāapskata virspusēji, jo, beidzoties vienam nolūkam, var rasties jauni leģitīmi nolūki, kas var pamatot nepieciešamību datus glabāt ilgāk – arī pēc pamatnolūka izbeigšanās, *piemēram, ja pakalpojuma līgums ar klientu tiek izbeigts, pamatnolūks – sniegt pakalpojumu klientam – ir sasniegts un dati šim nolūkam vairs nebūtu nepieciešami un apstrādājami, tomēr ir pieļaujams, ka dati tiek apstrādāti papildus nepieciešamiem nolūkiem – izpildīt normatīvo aktu prasības par attaisnojamu grāmatvedības dokumentu glabāšanu vai lai aizsargātu kredītiestādes leģitīmās intereses, ja bijušais klients vēlētos apstrīdēt darījumus vai sniegtos pakalpojumus*. Gadījumos, kad mainās datu apstrādes nolūks, ir nepieciešams pārvērtēt datu apstrādes apjomu, kuru nepieciešams apstrādāt, lai sasniegtu jaunos nolūkus, *piemēram, ieviešot mehānismus un procedūras, kas noteiktu kārtību, kādā pārskatāms veiktās datu apstrādes apjoms nolūku maiņas gadījumā*.

Par šī principa piemērošanu vairāk lasiet Ieteikumu 4.3. nodaļā.

2.6. Integritāte un konfidencialitāte

Ievērojot to, ka mūsdienās datu apstrāde galvenokārt notiek ar elektroniskiem datu apstrādes līdzekļiem, šo līdzekļu izmantošana var radīt gan priekšrocības efektīvā datu apstrādes nodrošināšanā, gan arī trūkumus jeb riskus datu subjektu datu apstrādei. Līdz ar to jāpievērš uzmanību tehnisko un organizatorisko risinājumu ieviešanai kredītiestādē, lai pēc iespējas samazinātu riskus datiem, kurus rada tehnoloģiju izmantošana (*piemēram, datu nokļūšana trešo personu rīcībā, datu nepamatota iznīcināšana*).

Regula nosaka, ka datu apstrāde ir organizējama, izmantojot atbilstošus tehniskos vai organizatoriskos līdzekļus, lai nodrošinātu datu drošību, novēršot neatļautu piekļuvi un mainīšanu, kā arī lai izvairītos no nejaušiem datu zudumiem vai bojājumiem.

Regula nenosaka konkrētus kredītiestādei veicamos tehniskos un organizatoriskos pasākumus, lai nodrošinātu atbilstību Regulai un nodrošinātu datu drošību, bet tā ir kredītiestādes atbildība izvērtēt iespējamos apdraudējumus un to ietekmi uz datu subjektiem, tādējādi izvēloties atbilstošus tehniskus un organizatoriskus līdzekļus un pasākumus iespējamam apdraudējumam un citiem riskiem, lai tos novērstu vai minimizētu.

Par šī principa piemērošanu vairāk lasiet Ieteikumu 6. nodaļā.

2.7. Pārskatatbildība

Regula paredz, ka datu subjektam ne vienmēr ir efektīvi līdzekļi (*piemēram, nav zināšanu vai informācijas*), lai kontrolētu savus datus un pamatotu savus apsvērumus par pārziņa rīcībā esošu datu nedrošu un/vai nelikumīgu apstrādi. Līdz ar to Regula pārceļ pierādīšanas pienākumu par Regulas prasību pilnvērtīgu izpildi no datu subjekta uz pārzini.

Lai šo principu īstenotu, kredītiestādei jau pirms datu apstrādes uzsākšanas un Regulas piemērošanas ir jāapsver risinājumi, kā kredītiestāde uzskatāmi demonstrēs Regulas ievērošanu, *piemēram, datu drošības nodrošināšanā, datu subjekta tiesību realizācijas nodrošināšanā, risku novērtēšanā un novēršanā*. Atbilstību demonstrēt var veicot, piemēram, šādas darbības:

1) atbilstošu tehnisko un organizatorisko līdzekļu un pasākumu ieviešana (t.sk. iekšējo normatīvo aktu izstrāde, iekšējo datu apstrādes procesu auditu veikšana, darbinieku apmācība);
2) aktuālu procedūru/instrukciju attiecībā uz apstrādes darbībām uzturēšana;
3) ietekmes novērtējuma veikšana;
4) datu apstrādes reģistra ieviešana un uzturēšana;
5) datu aizsardzības speciālista norīkošana;
6) datu aizsardzības "pēc noklusējuma" un integrētas datu aizsardzības īstenošana, nodrošinot datu minimizēšanu, pseidonimizāciju, pārredzamību, ļaujot datu subjektam kontrolēt un pārraudzīt savu datu apstrādi, kā arī ieviešot atbilstošus drošības pasākumus;
7) pievienošanās rīcības kodeksiem vai veiktās datu apstrādes sertificēšana;
8) sadarbības ar uzraudzības iestādi tās uzdevumu izpildē nodrošināšana.

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 39., 40., 58., 60. un 85. apsvērumā un Regulas 5., 6., 15. un 25. pantā.

3. LIKUMĪGAS DATU APSTRĀDES NODROŠINĀŠANA

3.1. Nolūku noteikšana

Nolūku nepieciešamība

Netiek pieļauta datu apstrāde bez iepriekš noteiktiem datu apstrādes nolūkiem, līdz ar to pirms datu apstrādes uzsākšanas ir nepieciešams izvērtēt un noteikt datu apstrādes nolūkus. Nolūki kredītiestādē var būt vairāki, *piemēram, darbinieku nodarbināšana, pakalpojumu sniegšana klientiem vai kredītiestādes drošības nodrošināšana*. Turklāt nolūkiem var būt apakšnolūki, *piemēram, lai nodrošinātu pamatnolūka – pakalpojumu sniegšanu klientiem – izpildi, būtu nepieciešama šādu apakšnolūku realizēšana: sniegto pakalpojumu administrēšana, samaksas par pakalpojumiem administrēšana, NILLTPFNL prasību izpilde, kavētu maksājumu piedziņa*.

Turklāt ar noteiktu periodiskumu nolūku nepieciešamību ir jāpārvērtē, lai konstatētu gadījumus, kad nolūks ir sasniegts, un lai izvairītos no gadījumiem, kad dažādu apstākļu izmaiņu rezultātā nolūkam ir zudusi nepieciešamība (*piemēram, mainījušies normatīvie akti, mainījušies klienta paradumi, mainījušies ārējie apstākļi, kas noteica nepieciešamību pēc attiecīga nolūka*).

Zemāk tiek norādīts ilustratīvs iespējamo nolūku uzskaitījuma piemērs kredītiestādē. Tomēr jāņem vērā, ka katrai kredītiestādei tas var tikt organizēts atšķirīgi, ņemot vērā kredītiestādes struktūru, piedāvātos pakalpojumus un citus apstākļus, kā arī šis nolūku uzskaitījums nav izsmeļošs (īpaši 2. un 3. līmeņa nolūki) un ir papildināms, un pielāgojams, ņemot vērā konkrētās kredītiestādes vajadzības un specifiku.

Tabula Nr. 1

Dažādu līmeņu nolūku piemēri

1. līmeņa nolūks	2. līmeņa nolūki	3. līmeņa nolūki
1. Personāla vadības nolūki		
	1.1. Personāla atlase;	
	1.2. Darba līguma noslēgšana un izpilde;	
	1.3. Darba laika uzskaite;	
	1.4. Darba samaksas aprēķina un darba samaksas veikšanas nodrošināšana;	
	1.5. Grāmatvedības prasību izpilde (attiecīgu attaisnojumu dokumentu noformēšana, komandējuma noformēšana);	
	1.6. Likumā noteikto pienākumu veikšana (ziņošana Valsts ieņēmumu dienestam, Valsts sociālās apdrošināšanas aģentūrai, darbinieka piederības arodbiedrībai noskaidrošana darba līguma uzteikuma gadījumā);	
	1.7. "Labumu groza" nodrošināšana (veselības apdrošināšanas organizēšana, sadarbības partneru iesaiste, lai darbinieki saņemtu atlaides);	
	1.8. Darba pienākumu izpildes fiksēšana un kontrole;	

1. līmeņa nolūks	2. līmeņa nolūki	3. līmeņa nolūki
2. Kredītiestādes pakalpojumu sniegšana klientiem	2.1. Klienta identifikācija;	
	2.2. Konta apkalpošanas/ maksājumu pakalpojumu sniegšanas nodrošināšana:	2.2.1. Maksājumu nodrošināšana;
		2.2.2. Maksājumu karšu/ kredītkaršu izdošana un apkalpošana;
	2.3. Attālināto kredītiestādes pakalpojumu nodrošināšana:	2.3.1. Internetbankas pakalpojumu nodrošināšana;
		2.3.2. Telefonbankas pakalpojumu nodrošināšana;
		2.3.3. Mobilo aplikāciju pakalpojumu nodrošināšana;
		2.3.4. Sīkdatņu izmantošana;
	2.4. Kreditēšanas pakalpojumu sniegšana:	2.4.1. Klienta kredītspējas izvērtēšana;
		2.4.2. Galvinieka kredītspējas izvērtēšana un galvojuma līguma noslēgšana;
		2.4.3. Ķīlas līguma noslēgšana un ķīlas priekšmeta novērtēšana;
		2.4.4. Līguma izpildes uzraudzības un kredīta atmaksas nodrošināšana;
	2.5. Tiesību aktos noteikto pienākumu izpilde:	2.5.1. Klienta izpēte, t.sk. klienta identifikācija, patiesā labuma guvēja noskaidrošana un politiski nozīmīgas personas noskaidrošana;
		2.5.2. Ziņošana Latvijas Bankas Kredītu reģistram;
		2.5.3. Valsts iestāžu/izmeklēšanas u.c. tiesībsargājošo iestāžu pieprasījumu izpilde;
		2.5.4. NILLTPFNL likuma prasību izpilde, piemēram, aizdomīgu un neparastu darījumu konstatēšanas sistēmas uzturēšana un ziņošana;
3. Mārketinga vajadzībām	3.1. Klientu grupu izvērtēšana un izpēte;	
	3.2. Komerciālu paziņojumu sūtīšana un citu saziņas formu izmantošana;	
	3.3. Klientu lojalitātes pasākumu organizēšana;	
	3.4. Potenciālo klientu uzrunāšana;	
	3.5. Sīkdatņu izmantošana;	
4. Risku novērtēšana un novēršana darījumos ar klientiem:	4.1. Kredītiestādes risku pārvaldība;	
	4.2. Klientu un citu personu kredītspējas izvērtēšana;	
	4.3. Krāpšanas gadījumu novēršana un atklāšana;	
5. Saimniecisko un administratīvo aktivitāšu veikšana:	5.1. Drošības nodrošināšana kredītiestāžu telpās (piemēram, pieejas kontroles sistēmu uzturēšana);	
	5.2. Īpašuma aizsardzība (piemēram, videonovērošanas sistēmu uzturēšana);	
	5.3. Tiesību aktos noteikto pienākumu izpilde (piemēram, dažādu kredītiestādes maksātspējas kritēriju izpilde, revīziju veikšana);	
	5.4. Sadarbības nodrošināšana ar sadarbības partneriem, t.sk. sadarbības nodrošināšanai nepieciešamās informācijas nodošana/saņemšana;	
	5.5. Parādu atgūšanas un piedziņas darbību veikšana.	

Nolūku fiksēšana

Nolūkam jābūt noteiktam pirms datu apstrādes uzsākšanas un ieteicams to apstiprināt ar kredītiestādes pārvaldes institūcijas lēmumu vai rīkojumu, vai norādīt citos kredītiestādes iekšējos tiesību aktos (*piemēram, procedūrās vai instrukcijās*), vai arī apstiprināt citā kredītiestādes noteiktā kārtībā, lai nodrošinātu jaunu nolūka nozīmību. Nolūkam būtu jābūt reģistrētam kredītiestādes uzturētajā datu apstrādes darbību reģistrā.

Tāpat būtu nepieciešams pirms jebkura jauna nolūka datu apstrādes uzsākšanas vai nolūka izmaiņām pieprasīt un saņemt datu aizsardzības speciālista viedokli. Ja datu aizsardzības speciālista viedoklis atšķiras un turpmākā apstrāde notiek pretēji datu aizsardzības speciālista norādēm, kredītiestāde dokumentē pamatojumu šādai datu apstrādes īstenošanai. Turklāt būtu jāizvērtē, vai pirms jaunu nolūku apstiprināšanas attiecīgam nolūkam nebūtu jāveic datu aizsardzības ietekmes novērtējums, taču, ja tiek pieņemts lēmums neveikt datu aizsardzības ietekmes novērtējumu, argumenti ir dokumentējami[3].

Nolūku ietekme uz datu subjektu

Tikai precīzi definēts nolūks varēs palīdzēt kredītiestādei nodrošināt adekvātu datu apstrādi izvirzītam nolūkam (piemēram, ievērot datu minimizēšanas principu), kā arī nodrošināt likumīgu datu apstrādi, izvēloties atbilstošus tiesiskos pamatus un nodrošinot godprātīgu attieksmi pret datu subjektu, to atbilstoši informējot.

Datu subjektu informēšana par nolūkiem

Izvērtējot jautājumu par datu subjektu informēšanu par apstrādes nolūkiem, būtu jāņem vērā šādi aspekti:

1. pārāk detalizēta nolūku uzskaite datu subjektam sniedzamajā informācijā var neļaut sasniegt Regulā noteikto mērķi – nodrošināt datu subjekta informēšanu kodolīgā, pārredzamā un saprotamā veidā, izmantojot skaidru un vienkāršu valodu. Līdz ar to ieteicams apsvērt dažādu detalizēto (augstāk norādītā paraugā – 3. līmeņa nolūki) nolūku apvienošanu (piemēram, informēt datu subjektu par 1. vai 2. līmeņa nolūkiem atkarībā no datu apstrādes rakstura) informēšanas vajadzībām un nodrošināt izvērstāku nolūku skaidrojumu pēc datu subjekta pieprasījuma vai iekļaut to kādā no datu subjektam pieejamiem dokumentiem (piemēram, kredītiestādes privātuma politikā),

2. ja dati ir ievākti no trešajām personām (piemēram, klienta kredītspējas pārbaudei, klienta izpētes informācija iegūta no publiskām un trešo personu turējumā esošām datu bāzēm) un šāda informācijas iegūšana un/vai izpaušana ir paredzēta ES vai Latvijas normatīvajos aktos, tad saskaņā ar Regulas 14. panta 5. punktu, par šādu datu apstrādi kredītiestādei nav pienākums informēt datu subjektu.

Nolūka nozīmīgums jeb būtiskums

Nolūkam attiecībā uz kredītiestādi ir jābūt nepieciešamam kredītiestādes komerciālo nolūku sasniegšanai, turklāt nepieciešamībai izvēlēto nolūku īstenot ir jābūt pašreizējai, nevis pamatotai ar nekonkrētiem nākotnes plāniem. Nolūku maznozīmīgums var atklāties arī datu apstrādes laikā, tādēļ ir nepieciešams ar noteiktu regularitāti pārvērtēt nolūku nozīmīgumu, pievēršot uzmanību nolūku īstenošanai un kredītiestādes attieksmei (to būtiskuma vērtēšanā) attiecībā uz nolūkiem.

Lai sekotu līdzi nolūku izpildei un nolūku sasniegšanai, nepieciešamo datu apstrādei būtu rekomendējams noteikt atbildīgās personas vai struktūrvienības katra nolūka pārraudzībai, t.sk. periodiskai nolūku nepieciešamības pārvērtēšanai un nolūka sasniegšanai apstrādāto datu pārvērtēšanai.

[3] Sk. arī: Ieteikumu 6.3. nodaļu "Novērtējums par ietekmi uz datu aizsardzību".

Nolūku maiņa jeb datu apstrāde sākotnēji neparedzētiem nolūkiem

Kredītiestāde jebkurus datus sākotnēji ir ievākusi ar kādu konkrētu nolūku, kuru ietvaros veikto datu apstrādi kredītiestādei ir jāspēj kontrolēt un nodrošināt datu apstrādi atbilstoši šiem sākotnējiem nolūkiem, saskaņā ar kuriem dati tika ievākti. Ja kredītiestādei rodas nepieciešamība šos datus izmantot citiem nolūkiem, ir jāveic jaunā nolūka saderības pārbaude ar sākotnējo nolūku un jānodrošina datu subjektu informēšana par nolūku maiņu, tiesiskā pamata pārvērtēšanu, ja nolūks nav saderīgs ar sākotnējiem nolūkiem un datu subjekta tiesībām šajā sakarā (*piemēram, datu subjekta tiesībām iebilst*). Ja kredītiestāde vēlas datus izmantot jauna pakalpojuma nodrošināšanai datu subjektam, jāizvērtē vai nav iespējams noslēgt ar datu subjektu jaunu pakalpojuma līgumu, tādā veidā tiktu izpildītas datu subjekta informēšanas prasības un nodrošināts atbilstošs tiesiskais pamats datu apstrādei.

Informācija, kas tikusi ievākta NILLTPFNL prasību izpildei, ir jāizmanto atbilstoši nolūkam, ja tiek mainīts nolūks (*piemēram, informācija izmantota kredītspējas vērtēšanai*), ir jāvērtē, vai ir jauns tiesisks pamats (*piemēram, nepieciešamība līguma noslēgšanai vai leģitīmās intereses*). Tomēr svarīgi ir apzināties, ka ne visos gadījumos būs iespējams nolūku mainīt, kas varētu būt atkarīgs no datu iegūšanas avotiem. *Piemēram, ja dati ir iegūti no publiskiem avotiem vai no paša datu subjekta, veicot atbilstošu risku izvērtējumu un nolūku saderības pārbaudi, būtu iespējams datus izmantot arī kredītspējas vērtēšanai, bet, ja dati tieši NILLTPFNL prasību izpildei ir iegūti no Valsts ieņēmuma dienesta, bez atsevišķas datu subjekta piekrišanas un/vai Valsts ieņēmumu dienesta piekrišanas datus citiem nolūkiem nevarētu izmantot*.

Ja nolūks, kādam datus plānots turpmāk izmantot, ir saderīgs ar nolūku, kādam dati tika sākotnēji ievākti, tad šāda apstrāde ir pieļaujama, pamatojoties uz sākotnējo tiesisko pamatu. Šādi sākotnējiem nolūkiem saderīgi nolūki varētu būt ar datu subjekta piekrišanu mainīti nolūki vai ES un Latvijas tiesību aktos noteiktie nolūki (*piemēram, likuma "Par grāmatvedību", NILLTPFNL, Kredītiestāžu likuma, Patērētāju tiesību aizsardzības likuma izpilde*), kā arī nolūki, kurus par tādiem, veicot zemāk noteikto izvērtējumu, ir atzinusi kredītiestāde. Nolūku saderības pārbaude ietver sevī vismaz šādu aspektu izvērtējumus:

1. saikne starp nolūku, kādos dati tika sākotnēji vākti, un nolūkiem, kādiem turpmāk paredzēts datus izmantot;

2. kontekstu, kādā dati ir vākti, īpašu uzmanību pievēršot datu subjekta un kredītiestādes kā pārziņa attiecībām, *piemēram, seniori, kuriem varētu būt citādāka izpratne par pieprasītās informācijas raksturu un iespējām to izmantot; aizdevumu pieprasītāji, kuriem varētu būt kritiska ekonomiskā situācija, vai darba attiecības, kurās darbinieks visticamāk nespēja kritiski izvērtēt datu sniegšanas nepieciešamību vai iebilst pret atsevišķu datu apstrādi, vai šāda datu sniegšana bija obligāta*;

3. datu raksturs, jo īpaši tas, vai tiek apstrādātas Īpašu kategoriju dati vai apstrādāti dati, kas attiecas uz sodāmību un pārkāpumiem;

4. turpmākās apstrādes iespējamās sekas datu subjektam, *piemēram, vai datu subjektam, apstrādājot datus saskaņā ar mainīto nolūku, var tikt radītas negatīvas sekas (piemēram, negatīva lēmuma formā)*;

5. apstrādājamo datu apjoma palielināšana;

6. kādas papildu garantijas datu subjekta tiesību līdzsvarošanai tiks nodrošinātas (*piemēram, datu šifrēšana un pseidonimizācija, datu subjektam tiks nodrošināta tiesība atteikties no turpmākas datu apstrādes*).

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 50. apsvērumā un Regulas 6. pantā.

3.2. Vispārīgie datu apstrādes tiesiskie pamati

Tiesiskā pamata esamība ir viens no priekšnoteikumiem likumīgas datu apstrādes nodrošināšanai, tādēļ ir būtiski kontrolēt kredītiestādes datu plūsmas, identificējot šādas plūsmas pamatojošos tiesiskos pamatus. Kredītiestādei kā pārzinim attiecīgos datus apstrādājot, ir jāidentificē konkrēts tiesiskais pamats. Tāpat vērā ņemams ir Regulas noteikums, ka par attiecīga tiesiskā pamata esamību ir jāinformē arī datu subjekts. Zemāk izklāstīti skaidrojumi, sadalīti pa tiesisko pamatu kategorijām, kas atvieglo atbilstošu tiesiskā pamata izvēli. Gadījumos, kad kredītiestāde datus apstrādā kā apstrādātājs kāda cita pārziņa uzdevumā, kredītiestādei nav nepieciešams tiesiskais pamats datu apstrādei, ciktāl datu apstrāde notiek dotā uzdevuma ietvaros. Šādā gadījumā kredītiestādei kā apstrādātājam ir jāuztur šādu apstrādes darbību reģistrs.

3.2.1. Piekrišana

"(..) datu subjekts ir devis piekrišanu savu personas datu apstrādei vienam vai vairākiem konkrētiem nolūkiem (..)" [4]

Piekrišanas būtība un forma

Ar piekrišanu datu subjekts apstiprina datu apstrādes uzsākšanu, tādā veidā apliecinot, ka datu apstrāde ir samērīga un atbilst datu subjekta interesēm un vajadzībām. Tomēr piekrišanas izmantošana ir rūpīgi jāvērtē, piemēram, ja datus ir nepieciešams apstrādāt līgumsaistību izpildei, tad piekrišana nebūs atbilstošākais tiesiskais pamats šādai datu apstrādei un atbilstošāk būtu izvēlēties citu tiesisko pamatu. Piekrišanai ir jāatbilst zemāk norādītām pazīmēm, kas padara piekrišanas izmantošanu par piemērotu atsevišķās datu apstrādēs, *piemēram, komerciālu paziņojumu sūtīšanai, internetbankas identifikatoru izmantošanai trešo pušu pakalpojumos*.

Tāpat ir jānošķir piekrišana personas datu apstrādes kontekstā no piekrišanas, kas izriet no Kredītiestāžu likuma 62. panta ceturtās daļas un ir attiecināma uz "bankas noslēpuma" izpaušanu, lai izpildītu ar klientu noslēgtu līgumu.

Piekrišanas izteikšana netiek aprobežota ar kādu konkrētu formu piekrišanas iegūšanai, līdz ar to tā var tikt iegūta:

1. rakstiski (*piemēram, parakstot piekrišanas dokumentu*),
2. elektroniskā formātā (*piemēram, ar attiecīgas atzīmes izdarīšanu kredītiestādes internetbankā*),
3. mutiski (*piemēram, datu subjektam piekrītot telefonsarunas laikā, nodrošinot attiecīgus pierādījumus piekrišanas izteikšanas faktam*),
4. ar aktīvu darbību (*piemēram, klientam atstājot savu vizītkarti, tas piekrīt, ka viņa datus, kas norādīti vizītkartē, apstrādās persona, kurai vizītkarte ir nodota*).

Kredītiestādei ir pienākums pierādīt, ka tā ir ieguvusi nepārprotamu datu subjekta piekrišanu datu apstrādei, un saglabāt šādus pierādījumus pārskatatbildības principa nodrošināšanas ietvaros.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

[4] Regulas 6. panta 1. punkta "a" apakšpunkts.

Derīgas piekrišanas pazīmes

Lai piekrišana būtu likumīga un spēkā esoša, tai ir jāatbilst vairākām obligātām piekrišanas pazīmēm:

1. **"aktīvi sniegta"** – piekrišana ir jāsniedz ar aktīvu darbību jeb paziņojuma vai skaidri apstiprinošas darbības veidā, *piemēram, aktīvi atzīmējot izvēli noteiktā laukā (piemēram, ieliekot atzīmi jeb "ķeksi"), parakstot atsevišķu piekrišanas dokumentu, iesniedzot dzīvesgājuma aprakstu (CV) darba devējam*;

2. **"informēta"** un **"apzināta"** – lai piekrišana būtu apzināta, datu subjektam ir jāapzinās, kādiem nolūkiem viņa dati tiks apstrādāti. Lai datu subjekts spētu pienācīgi izvērtēt, vai piedāvātā datu apstrāde atbilst tā vajadzībām, datu subjektam pirms piekrišanas izteikšanas ir jābūt informētam vismaz par pārziņa identitāti un apstrādes nolūkiem, kā arī par to, kur iepazīties ar pārējo Regulā noteikto informāciju par tā datu apstrādi.

   Pamatinformācijai ir jābūt datu subjektam viegli pieejamai piekrišanas izteikšanas laikā, līdz ar to, par nepietiekami informētu datu subjekts var tikt atzīts, ja piekrišanā nav sniegta nekāda informācija par datu apstrādes nolūkiem un pārzini, bet ir tikai norādītas atsauces uz likuma vai Regulas normām vai citiem dokumentiem, kuri datu subjektam nav pieejami un pārskatāmi piekrišanas izteikšanas laikā. Šajā gadījumā būtu nepieciešams piekrišanas izteikšanas laikā sniegt vismaz iepriekš minēto pamatinformāciju, taču papildu detalizētāka informācija varētu tikt izvietota citā dokumentā (t.sk. vispārējos darījumu noteikumos, privātuma politikā), uz kuru ir norāde piekrišanas izteikšanas dokumentā vai citā viegli pieejamā vietā, kā arī datu subjektam tiek nodrošināts vienkāršs, pieejams veids, kā ar attiecīgo dokumentu iepazīties (*piemēram, tas ir izdrukāts un tiek datu subjektam izsniegts, tas ir pieejams kredītiestādes interneta vietnē*);

3. **"konkrēta"** – piekrišanai ir jāattiecas uz konkrētu datu apstrādes nolūku, par kuru datu subjekts tiek informēts pirms piekrišanas došanas. Ja ir nepieciešams iegūt piekrišanu vairākiem nolūkiem, kredītiestādei jāiegūst atsevišķa piekrišana katram nolūkam. Taču tajos gadījumos, kad vairāki datu apstrādes mērķi ir nesaraujami saistīti un īstenojami tikai kopā (*piemēram, mārketinga mērķis tiek īstenots kopā ar profilēšanu*), var tikt iegūta viena piekrišana visiem datu apstrādes mērķiem. Ja piekrišana ir iekļauta kādā dokumentā kopā ar citiem jautājumiem, piekrišana ir jāizdala no cita satura un datu subjektam ir jāspēj to izteikt neatkarīgi no, *piemēram, līguma parakstīšanas*;

4. **"brīva"** – datu subjektam ir jābūt īstai un brīvai izvēlei un piekrišanas iegūšanas procesam nevar piemist piespiedu vai maldinošs raksturs. Līdz ar to jāizvērtē, vai datu subjektam ir izvēles brīvība dot piekrišanu un vai, nesaņemot piekrišanu, datu subjektam netiks radītas nelabvēlīgas sekas, *piemēram, ar datu subjektu netiks noslēgs līgums*. Tāpat būtu rūpīgi izvērtējami gadījumi, kurās konstatējama datu subjekta un pārziņa iespējamā nevienlīdzība tiesiskajās attiecībās, *piemēram, darba devēja un darbinieka attiecības, kurās darbinieks var sniegt piekrišanu, baidoties no iespējamām negatīvajām sekām, kas savukārt var padarīt piekrišanu par apstrīdamu*. Tomēr piekrišana būs atzīstama par brīvu un labprātīgi sniegtu, ja datu subjektam tiek piedāvāti kādi ieguvumi, *piemēram, atlaižu, bonusu vai papildus pakalpojumu formā, no kuriem kā atsevišķu piemēru var minēt gadījumu, kad persona piekrīt dzimšanas datuma apstrādei, lai dzimšanas dienā saņemtu iespēju ar atlaidi izmantot sadarbības partneru pakalpojumus*;

5. **"atsaucama"** – datu subjektam jebkurā laikā ir tiesības atsaukt piekrišanu un nav iespējams vienoties ar datu subjektu par to, ka viņš savu piekrišanu nedrīkst atsaukt. Līdz ar to rūpīgi ir jāizvērtē piekrišanas atbilstība datu apstrādes būtībai. Turklāt par iespēju atsaukt piekrišanu datu subjekts ir jāinformē pirms viņš savu piekrišanu ir devis. Tikšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR Darba grupu 2019. gada 7. martā Datu valsts inspekcija pauda viedokli, ka ja informācija par piekrišanas atsaukšanu jau ir ietverta, piemēram, privātuma politikā, klientu var papildus neinformēt par piekrišanas došanas specifiku un iespējām to atsaukt.

   Piekrišanas atsaukšanas process ir jānodrošina tikpat vienkāršs, kā piekrišanas saņemšana, *piemēram, ja digitālajā vidē piekrišana tika saņemta, tad arī jānodrošina šādā veidā iespēja atsaukt piekrišanu*. Piekrišanas atsaukšanas rezultātā kredītiestāde turpmāk neapstrādā datus nolūkiem, kādiem piekrišana tika atsaukta, bet kredītiestādei ir tiesības datus apstrādāt citiem nolūkiem un attiecīgi citiem tiesiskiem pamatiem, piemēram, saglabāt pierādījumus par piekrišanas esamību;

6. **"pierādāma"** – ja kredītiestāde savu datu apstrādi pamato ar datu subjekta piekrišanu, tai jāspēj uzskatāmi pierādīt, ka datu subjekts ir piekritis datu apstrādei, *piemēram, ar papīra dokumentā fiksētu piekrišanu, ar telefona sarunu ierakstiem, *.log failiem*. Pierādījumi par piekrišanas saņemšanu ir jāuzglabā tik ilgi, kamēr uz piekrišanas pamata tiek veikta datu apstrāde, kā arī pēc tās iespējamo prasījumu noilguma periodu, lai nodrošinātu kredītiestādes leģitīmo interešu aizsardzību strīda par tiesiskā pamata esamību rašanās gadījumā.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Atbildības pārnešana ar piekrišanu

Piekrišanas saņemšana neatbrīvo kredītiestādi no pienākuma ievērot citas datu aizsardzības tiesību normas un principus, t.sk. samērīguma izvērtēšanu, datu drošības nodrošināšanu, kam turklāt ir jābūt veiktam jau pirms piekrišanas saņemšanas un datu apstrādes uzsākšanas.

Tāpat piekrišana nevar padarīt par likumīgu tādu datu apstrādi, kura ir aizliegta ar likumu vai Regulu, piemēram, datu, kas attiecas uz sodiem, apstrāde ir atļauta tikai atsevišķos izņēmuma gadījumos, ja to paredz ES vai Latvijas tiesību akti vai tā tiek veikta oficiālas iestādes kontrolē un datu subjekta piekrišana šo aizliegumu atcelt nevar.

Piekrišanas termiņš

Piekrišana ir jāsaņem pirms datu apstrādes uzsākšanas. Piekrišanas spēkā esamībai nav termiņa ierobežojuma, izņemot gadījumus, kad piekrišanas tekstā datu subjekts pats ir ierobežojis piekrišanas darbības ilgumu. Līdz ar to, ja piekrišanā nav norādīts termiņš, tad ir pamatoti uzskatīt, ka piekrišana ir spēkā nenoteiktu laiku, t.i., līdz nolūka sasniegšanai vai līdz piekrišanas atsaukšanai.

Tomēr ieteicamā prakse būtu ar noteiktu regularitāti pārskatīt jau izteiktas piekrišanas spēkā esamības termiņus, jo, iespējams, uz piekrišanu veiktās darbības vairs nav datu subjektam aktuālas vai klients ir aizmirsis par piekrišanas izteikšanu, *piemēram, klients – students – ir piekritis saņemt jaunumus par studentiem noderīgiem kredītiestādes un tās sadarbības partneru piedāvājumiem. Lai arī piekrišana ir dota bez termiņa ierobežojuma, tomēr klientam pārtraucot studijas var vairs nebūt aktuāli studentiem adresēti sūtījumi. Līdz ar to pamatoti būtu periodiski pārskatīt piekrišanā norādītās datu apstrādes atbilstību klienta vajadzībām, un iespējams datu apstrādi šim nolūkam pārtraukt vai saņemt jaunu piekrišanu vai piemērot citu tiesisko pamatu, ja plānots mainīt apstrādes nolūku*.

Piekrišana citas personas vietā

Piekrišanu datu subjekts var sniegt tikai pats par sevi (izņemot vecāku un bērnu attiecībās vai citos gadījumos, ja personai ir rīcības spējas ierobežojumi). Atsevišķi izvērtējama būtu arī piekrišanas izteikšana uz pilnvaras pamata, ņemot vērā pilnvarojuma apjomu.

Tabula Nr. 2

Derīgas un neatbilstošas piekrišanas piemēri:

Derīga piekrišana	Neatbilstoša piekrišana
Digitālajā vidē pieņemama piekrišana būtu ar atzīmes izdarīšanu ("OPT-IN" princips) izvēles laukā ("Check box").	Digitālajā vidē neatbilstoša piekrišana būtu, ja piekrišanas izvēles laukā ("Check box") atzīme ir jau ievietota pēc noklusējuma un datu subjektam ir tiesības to izņemt laukā ("OPT-OUT" princips).
Izsūtot klientam paziņojumu internetbankā, kurā būtu norādīts, ja klients piekrīt jauna pakalpojuma izmantošanai, tad lai nosūta kredītiestādei apstiprinājumu šādai piekrišanai.	Izsūtot klientam e-pasta vēstuli un/vai paziņojumu internetbankā, kurā būtu norādīts, ja klients 10 dienu laikā neizteiks iebildumus, tad kredītiestāde uzskatīs to par piekrišanu datu apstrādei.
Datu subjekts piekrīt informācijas par papildus pakalpojumu saņemšanas iespējām uz savu e-pastu.	Datu subjekts piekrīt jebkādai savu datu apstrādei, kuru veiks kredītiestāde.
Datu subjekts piekrīt sava tālruņa numura izmantošanai komerciālu paziņojumu saņemšanai, turklāt nepiekrišanas gadījumā nodrošinātais pakalpojums negatīvi ietekmēts netiks.	Piekrišana tiek iegūta, norādot klientam, ka piekrišanas nesniegšanas gadījumā pakalpojuma līgums netiks noslēgts.
Līguma 3. lpp. 15. punktā tiek norādīts, ka klients parakstot līgumu ir piekritis savu datu nodošanai trešajai personai komerciālu paziņojumu sūtīšanai, un pie attiecīgā līguma punkta ir izvietoti divi atzīmējami izvēles lauki **"[ ] piekrītu/ [ ] nepiekrītu**".	Līguma 3. lpp. 15. punktā tiek norādīts, ka klients parakstot līgumu ir piekritis savu datu nodošanai trešajai personai komerciālu paziņojumu sūtīšanai, bez atsevišķiem piekrišanas atzīmes izdarīšanas laukiem.

Ja datu apstrāde tiek pamatota ar datu subjekta piekrišanu, kredītiestādei jāspēj uzskatāmi parādīt, ka piekrišana ir iegūta, nodrošinot atbilstību visām iepriekš norādītajām un Regulā minētajām datu subjekta piekrišanas pazīmēm.

Piekrišanu izmantot būtu ieteicams gadījumos, kad tās iegūšana nav kritiska biznesa procesu nodrošināšanai un/vai pakalpojuma sniegšanai, *piemēram, komerciālu paziņojumu sūtīšanas nodrošināšanai*.

Piekrišanas atsaukšanas gadījumā kredītiestādei būtu nepieciešams pārtraukt datu apstrādi, kas tiek veikta uz piekrišanas pamata.[5] Šajā gadījumā attiecīgie dati vairs nav apstrādājami nolūkiem, attiecībā uz kuriem piekrišana ir tikusi atsaukta, tomēr ir jāizvērtē, vai nav nepieciešams turpināt attiecīgo datu apstrādi citiem nolūkiem un attiecīgi uz citiem tiesiskiem pamatiem (*piemēram, datu uzglabāšana kredītiestādē, lai pierādītu datu apstrādes likumību vai piekrišanas esamību pārbaužu gadījumos*).

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 32., 42. un 43. apsvērumā un Regulas 6., 7. un 8. pantā, kā arī EDAK 2020. gada 4. maija "Pamatnostādnēs 05/2020 par piekrišanu atbilstoši Regulai 2016/679"[6] un 29. panta darba grupas 2011. gada 13. jūlija "Atzinumā 15/2011 par jēdziena "piekrišana" definīciju"[7].

(Ar grozījumiem, kas izdarīti 08.01.2021.)

[5] Sk. arī: Ieteikumu 5.5. nodaļu.
[6] EDAK 2020. gada 4. maija "Pamatnostādnes 05/2020 par piekrišanu atbilstoši Regulai 2016/679": https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf (angļu val.)
[7] 29. panta darba grupas 2011. gada 13. jūlija "Atzinums 15/2011 par jēdziena "piekrišana" definīciju": https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_lv.pdf

3.2.2. Līgumisku attiecību nodibināšana un izpilde

"(..) apstrāde ir vajadzīga līguma, kura līgumslēdzēja puse ir datu subjekts, izpildei vai pasākumu veikšanai pēc datu subjekta pieprasījuma pirms līguma noslēgšanas (..)"[8]

Nepieciešamība

Šis tiesiskais pamats dod iespēju apstrādāt datus pirms līguma noslēgšanas, lai sagatavotu līgumu un apstrādāt tikmēr, kamēr ir spēkā līgums ar datu subjektu. Līdz to datus, kuri ir nepieciešami līguma noslēgšanai, būtu ieteicams apstrādāt tieši uz šī tiesiskā pamata, nevis, *piemēram, balstīt uz piekrišanu, kuru datu subjekts var jebkurā brīdī atsaukt*. Attiecībā uz datu apstrādi, kas pamatota ar līguma izpildi, datu subjektam nav tiesību aizliegt savu datu izmantošanu līguma izpildei, kamēr līgums ir spēkā.

Šis tiesiskais pamats būtu piemērots datu nosūtīšanai starptautiskām maksājumu karšu organizācijām (MasterCard, VISA u.c.), lai izpildītu starp klientu un kredītiestādi noslēgto maksājumu karšu (kredītkaršu) līgumu, kā arī informācijas nodošana korespondentbankām, lai nodrošinātu no starp klientu un kredītiestādi noslēgtā konta līguma izrietošo maksājumu veikšanu.

Šī tiesiskā pamata izmantošana neatceļ kredītiestādes pienākumu sniegt vispārīgo informāciju datu subjektam par tā datu apstrādi. Skatīt arī Ieteikumu 5.1. nodaļu.

Nolūka ierobežojums

Šis tiesiskais pamats pieļauj apstrādāt tikai tos datus, kas nepieciešami līguma izpildei, *piemēram, konta apkalpošanas līguma izpildei ir nepieciešams apstrādāt datus par klienta identitāti, klientam piešķirto konta numuru, informāciju par kontā esošo finanšu līdzekļu plūsmu un pamatojumu, e-pasta adresi un tālruņa numuru, lai sazinātos ar klientu saistībā ar sniegto pakalpojumu un citu tādu informāciju, bez kuras pakalpojuma sniegšana nebūtu iespējama*.

Savukārt, ja datu apstrāde ir nepieciešama citiem (papildu) nolūkiem, *piemēram, e-pasta adreses izmantošanai trešo personu komerciālu paziņojumu sūtīšanai, datu apstrāde parāda piedziņas darbību veikšanai vai klienta izpētei*, šo tiesisko pamatu izmantot nebūs pamatoti un būtu jāvērtē, vai var tikt piemērots kāds cits tiesiskais pamats, piemēram, piekrišana, cita līguma izpilde, juridiska pienākuma izpilde, kredītiestādes vai trešo personu leģitīmās intereses.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Pasākumu veikšana pirms līguma noslēgšanas

Ja ir nepieciešama datu apstrāde, sagatavojot līgumu (līgumprojektu), to ir iespējams veikt uz šī paša tiesiskā pamata bez cita tiesiskā pamata meklēšanas, tomēr apstrādājamo datu apjomam nevajadzētu pārsniegt līguma sagatavošanai nepieciešamos datus. Šiem pasākumiem un attiecīgai datu apstrādei pirms līguma noslēgšanas ir jābūt cieši saistītai ar noslēdzamo līgumu, nevis pamatotai ar kredītiestādes leģitīmām interesēm.

Par atbilstošu apstrādi šim tiesiskam pamatam līguma sagatavošanas posmā būtu atzīstama *informācijas ievākšana, kuru nepieciešams norādīt līgumā vai izvērtēt līguma noslēgšanas procesā; līgumslēdzēju pušu identifikācijai nepieciešamā informācija (t.sk. informācija par personas identitāti apliecinošiem dokumentiem, pilnvarojumiem); datu nodošana (līgumprojekta ietvaros) citiem plānotā līguma līgumslēdzējiem vai to pārstāvjiem*.

[8] Regulas 6. panta 1. punkta "b" apakšpunkts.

Par neatbilstošu šim tiesiskam pamatam varētu tikt atzīta datu apstrāde, kas nepieciešama kavēto maksājumu piedziņai; kredītiestādes interešu aizsardzība, vēršoties tiesā; līguma satura izpaušana tiesībaizsardzības iestādēm. Šajos gadījumos atbilstošāks varētu būt kredītiestādes leģitīmo interešu pamatojums vai juridiska pienākuma izpilde.

Lai veiktu pasākumus pirms līguma noslēgšanas un uz tā pamata apstrādātu datus, ir nepieciešama datu subjekta izrādīta iniciatīva līguma noslēgšanai vai datu subjekta dots apstiprinājums līguma sagatavošanai. *Līdz ar to par neatbilstošu šim tiesiskam pamatam būtu atzīstama situācija, ja tiktu veikta esoša klienta kredītspējas pārbaude, lai pēc savas iniciatīvas piedāvātu klientam ar kredīta risku saistītus produktus. Tomēr šajā gadījumā būtu izvērtējama kredītiestādes leģitīmo interešu kā tiesiskā pamata piemērošana.*

Ja līgums pēc līguma projekta sagatavošanas netiek noslēgts, līguma sagatavošanai veiktā datu apstrāde joprojām ir uzskatāma par likumīgu un var tikt pamatota uz šo tiesisko pamatu. Tomēr, tiklīdz ir saņemta informācija par datu subjekta lēmumu līgumu neslēgt, tad dati, kas tika izmantoti līguma sagatavošanai, ir dzēšami, izņemot gadījumus, ja ir nepieciešams saglabāt pierādījumus tam, ka iepriekšējā apstrāde bija likumīga, *piemēram, pierādījumu tam, ka klienta izpēte ir tikusi veikta pamatoti un ievērojot NILLTPFNL prasības*, kas savukārt būtu pamatojams ar pārziņa leģitīmām interesēm vai juridiska pienākuma izpildi.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Trešo personu datu apstrāde

Ņemot vērā to, ka šis tiesiskais pamats pieļauj apstrādāt tikai tāda datu subjekta datus, kurš ir līgumslēdzēja puse un izrādījusi iniciatīvu līgumu noslēgt, uz šī tiesiskā pamata nebūs pamatoti apstrādāt trešo personu datus, kuri ir saistīti ar noslēdzamo līgumu (*piemēram, pieteikumā norādītie radinieku dati – vērtējot klienta kredītspēju, pieteikumā / līgumā norādītie (iespējamo) galvinieku vai ķīlas devēju dati, darījuma konta otru pusi*), bet nav līgumslēdzējas puses vai izrādījuši iniciatīvu noslēgt līgumu. Šādu trešo personu datu apstrādei ir piemērojams kredītiestādes vai trešās personas (klienta) leģitīmo interešu īstenošanas tiesiskais pamats.

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 44. apsvērumā un Regulas 6. pantā, kā arī EDAK 2019. gada 8. oktobra "Pamatnostādnēs par personas datu apstrādi saskaņā ar VDAR 6. panta 1. punkta "b" apakšpunktu datu subjektiem sniegto tiešsaistes pakalpojumu kontekstā"[9] un 29. panta darba grupas 2014. gada 9. aprīļa "Atzinumā 06/2014 par personas datu apstrādātāja likumīgo interešu jēdzienu saskaņā ar Direktīvas 95/46/EK 7. pantu"[10].

(Ar grozījumiem, kas izdarīti 08.01.2021.)

[9] EDAK 2019. gada 8. oktobra "Pamatnostādnes par personas datu apstrādi saskaņā ar VDAR 6. panta 1. punkta "b" apakšpunktu datu subjektiem sniegto tiešsaistes pakalpojumu kontekstā": https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf (angļu val.)

[10] 29. panta darba grupas 2014. gada 9. aprīļa "Atzinums 06/2014 par personas datu apstrādātāja likumīgo interešu jēdzienu saskaņā ar Direktīvas 95/46/EK 7. pantu": https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_lv.pdf

3.2.3. Juridiska pienākuma izpilde

"(..) apstrāde ir vajadzīga, lai izpildītu uz pārzini attiecināmu juridisku pienākumu (..)" [11]

"Juridiska pienākuma" jēdziena būtība

Piemērojot šo tiesisko pamatu, kredītiestādei nav rīcības brīvība vai arī ir ierobežota izvēles brīvība uz tai noteiktajiem pienākumiem, līdz ar to par šim tiesiskam pamatam atbilstošu datu apstrādi būs atzīstami tādi tiesību aktos noteiktie pienākumi, kas nepieļauj kredītiestādei lemt par datu apstrādes nodrošināšanu, *piemēram, Kredītiestāžu likuma 63. pantā uzskaitītie informācijas sniegšanas gadījumi vai Patērētāju tiesību aizsardzības likuma 8. panta 4.1 daļā noteiktais pienākums pirms patērētāja kreditēšanas līguma noslēgšanas izvērtēt informāciju par patērētāja ienākumiem un izdevumiem, NILLTPFNL noteiktais pienākums veikt klienta izpēti*.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Juridisku pienākumu avoti

Juridisks pienākums var tikt noteikts ar jebkāda veida ES vai Latvijas spēkā esošu tiesību aktu, t.sk. likumiem, Ministru kabineta noteikumiem, valsts iestāžu (FKTK, Latvijas Bankas, tiesībaizsardzības iestāžu, Valsts darba inspekcijas un citu iestāžu) rīkojumiem vai noteikumiem.

Latvijas Finanšu nozares asociācija ņem vērā FKTK viedokli par to, ka daudzas tiesību normas nāk no vecām direktīvām, kuras tik aktīvi neregulēja datu aizsardzības jautājumus. Līdz ar to tās situācijas, kad normatīvais akts nosaka tiesību, kas pēc būtības nozīmē tiesisko pienākumu, ir izveidojies juridiskās tehnikas dēļ (viedoklis pausts tiekšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR Darba grupu 2019. gada 7. martā).

29. panta darba grupas ieskatā juridiska pienākuma avots nav uzraudzības iestāžu ieteikumi un vadlīnijas vai vispārīgās politikas pamatnostādnes un nosacījumi. Tāpēc šajā gadījumā datu apstrādes aktivitātes jānovērtē saskaņā ar Regulas 6. panta 1. punkta "f" apakšpunktu.

Tikšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR Darba grupu 2019. gada 7. martā Datu valsts inspekcija aicināja skatīties pēc juridiskā pienākuma jēgas. Ja datu pārzinim ir izvēles brīvība attiecībā uz mērķa sasniegšanu un vēlamā rezultāta panākšanu, tad šāda datu apstrāde būtu jāpamato ar leģitīmajām interesēm. Piemēram, ar leģitīmajām interesēm būtu jāpamato tāda datu apstrāde, kuru katra kredītiestāde veic saskaņā ar sevis noteiktajām metodēm, pasākumiem, pat ja normatīvais akts uzliek ģenerālpienākumu. Taču tajos gadījumos, kad kredītiestādes izvēles iespējas ir ierobežotas un pēc būtības tām veicamā datu apstrāde ir noteikta kādā saistošā dokumentā, kā arī tās izmanto vienādus resursus un vienveidīgu metodiku, datu apstrādi varētu pamatot ar juridisko pienākumu.

DVI ieskatā, cits iespējamais risinājums ir vērtēt valsts iestāžu vadlīniju un ieteikumu saistošo raksturu. Ja tāds ir konstatējams, tiek uzskatīts, ka normatīvais akts uzliek pienākumu. Saistošais raksturs nav konstatējams tajos gadījumos, kad par vadlīniju vai ieteikumu neievērošanu nav paredzēta soda sankcija. Latvijas Finanšu nozares asociācija vērš uzmanību, ka valsts iestādes izdod vadlīnijas un ieteikumus, lai skaidrotu noteikto normatīvo tiesību aktu vai tiesību normu. Līdz ar ko lēmumi tiek pieņemti, pamatojoties uz augstāka juridiskā spēka tiesību aktu vai normu, taču argumentācijai izmanto skaidrojošās vadlīnijas un ieteikumus. Kā piemēru var minēt Patērētāju tiesību aizsardzības centra izdotās "Vadlīnijas patērētāju spējas atmaksāt kredītu novērtēšanai"[12], kuras pēc FKTK viedokļa vairāk norāda uz juridisko pienākumu (viedoklis pausts tiekšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR Darba grupu 2019. gada 7. martā).

[11] Regulas 6. panta 1. punkta "c" apakšpunkts.
[12] Patērētāju tiesību aizsardzības centra Vadlīnijas patērētāju spējas atmaksāt kredītu novērtēšanai kredītu devējiem, kas sniedz kreditēšanas pakalpojumus patērētājiem (apstiprinātas 27.04.2018.). Pieejams: http://www.ptac.gov.lv/sites/default/files/vadlinijas_pateretaju_spejas_atmaksat_kreditu_novertesanai_kreditu_devejiem_kas_sniedz_kreditesanas_pakalpojumus_pateretajiem.pdf

Juridiska pienākuma avots nav ārpus ES un EEZ esošu valstu normatīvajos aktos vai šo valstu iestāžu lēmumos noteiktie pienākumi. Šajā gadījumā šo pienākumu izpilde būtu jāvērtē, izmantojot kredītiestādes vai trešo personu, kurai dati tiek nodoti, leģitīmo interešu vērtēšanas un līdzsvarošanas ar datu subjekta interesēm metodika.

Tomēr, ņemot vērā to, ka finanšu pakalpojumu sniegšana ir viena no visplašāk tiesību aktos regulētām nozarēm, juridiska pienākuma izpildes tiesiskais pamats viennozīmīgi būtu jāuztver par visvairāk izmantojamo tiesisko pamatu, *piemēram, kredītiestādēm ir jāizpilda dažādi tiesību aktos kredītiestādēm saistoši pienākumi dažādās jomās*:

1. nodokļu administrēšanas jomā;
2. noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanas jomā;
3. darba attiecību nodrošināšanā;
4. koorporatīvās pārvaldības atbilstošā nodrošināšanā;
5. kredītiestādes iekšējās kontroles sistēmas izveidošanā un nodrošināšanā;
6. finanšu instrumentu atbilstošā apkalpošanā;
7. patērētāju un citu subjektu kreditēšanas jomā, piemēram, lai pārbaudītu klientu maksātspēju un kredītspēju;
8. kiberdrošības nodrošināšanā;
9. kontu uzturēšanā;
10. maksājumu pakalpojumu nodrošināšanā;
11. grāmatvedības un audita atbilstošā veikšanā un uzturēšanā;
12. kredītiestāžu darbību uzraudzības īstenošanas ietvaros.

Kā minēts zemāk 5.1.punktā un saskaņā ar Regulas 14.panta 5.punkta "c" apakšpunktu, gadījumos, kad personas datu apstrāde ir skaidri paredzēta ES vai Latvijas tiesību aktos, datu pārzinim nerodas pienākums sniegt informāciju datu subjektam par viņa datu apstrādi.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 10., 19., 41. un 45. apsvērumā un Regulas 6. pantā, kā arī 29. panta darba grupas 2014. gada 9. aprīļa "Atzinumā 06/2014 par personas datu apstrādātāja likumīgo interešu jēdzienu saskaņā ar Direktīvas 95/46/EK 7. pantu"[13].

(Ar grozījumiem, kas izdarīti 08.01.2021.)

3.2.4. Datu subjekta vai trešo personu vitāli svarīgu interešu aizsardzība

"(..) apstrāde ir vajadzīga, lai aizsargātu datu subjekta vai citas personas vitāli svarīgas intereses (..)"[14]

Vitāli svarīgas intereses

Šis tiesiskais pamats ir izņēmuma tiesiskais pamats un tas būtu jāattiecina tikai uz personu īpaši svarīgu interešu, tādu kā dzīvības un veselības, aizsardzību. Kredītiestāžu gadījumā šis tiesiskais pamats nebūtu plaši izmantojams, bet varētu tikt piemērots atsevišķos gadījumos darbinieku datu apstrādē (piemēram, ievācot informāciju par darbinieka veselības stāvokli, lai veselības stāvokļa pasliktināšanās gadījumā spētu sniegt tam palīdzību), kā arī krīzes situācijās (piemēram, ja kredītiestāžu telpās personai rodas veselības problēmas un nepieciešams veselības stāvokli apspriest ar neatliekamās medicīnas palīdzības darbiniekiem).

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 46. apsvērumā un Regulas 6. pantā.

[13] 29. panta darba grupas 2014. gada 9. aprīļa "Atzinums 06/2014 par personas datu apstrādātāja likumīgo interešu jēdzienu saskaņā ar Direktīvas 95/46/EK 7. pantu": https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_lv.pdf
[14] Regulas 6. panta 1. punkta "d" apakšpunkts.

3.2.5. Sabiedrības interešu ievērošana vai oficiālo pilnvaru realizācija

"(..) apstrāde ir vajadzīga, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot pārzinim likumīgi piešķirtās oficiālās pilnvaras (..)"[15]

Sabiedrības intereses

Sabiedrības interesēm vajadzētu būtu nostiprinātām tiesību aktos, līdz ar to šī pamata piemērošana pēc būtības ir līdzīga juridiska pienākuma izpildes pamatojumam ar atšķirību tajā, ka šie uzdevumi sabiedrības interesēs varētu nebūt tik precīzi noformulēti un pieļautu arī daļēju rīcības brīvību lēmumu pieņemšanā atšķirībā no juridiska pienākuma, kā tiesiskā pamata piemērošanas. Kredītiestāžu darbībā uz šī tiesiskā pamata varētu notikt ziņošana izmeklēšanas iestādēm pēc kredītiestādes iniciatīvas par iespējamiem noziedzīgiem nodarījumiem, *piemēram, par naudas izkrāpšanas mēģinājumiem*.

Apstrādājot datus uz šī tiesiskā pamata, kredītiestādei ir jāpārliecinās, vai attiecīgā sabiedrības interese ir pilnībā nostiprināta tiesību aktos vai arī atstāta kredītiestādei rīcības brīvība izvēlēties līdzekļus un datu apjomu nolūku sasniegšanai. Tādējādi ir jāizvērtē, vai ir iespējams datu subjektu informēt par paredzamo datu apstrādi. Tomēr būtu jāņem vērā gadījumi, kuros tiesību akts aizliedz datu subjekta informēšanu par paredzēto vai jau veikto datu apstrādi.

Pārzinim likumīgi piešķirtās oficiālās pilnvaras

Oficiālām pilnvarām jābūt nostiprinātām tiesību aktos, kas pieļauj daļēju rīcības brīvību lēmumu pieņemšanā attiecībā uz datu apstrādes apjomu un nolūkiem. Finanšu pakalpojumu sektorā pastāv tikai atsevišķi izņēmumu gadījumi, kad šī sektora dalībniekiem tiek piešķirtas no valsts oficiālas pilnvaras, kas tiek veiktas sabiedrības interesēs, *piemēram, valsts attīstības finanšu institūcija ALTUM*, kura tad attiecīgi var atsevišķām datu apstrādes darbībām izmantot šo pamatojumu.

Datu subjekta tiesības iebilst

Izmantojot šo pamatu, jārespektē datu subjekta tiesības iebilst apstrādei, un, saņemot šādus iebildumus, kredītiestādei, ņemot vērā datu subjekta norādītos iemeslus saistībā ar datu subjekta īpašo situāciju, ir jāpārvērtē datu apstrādes nepieciešamība un samērīgums attiecībā uz konkrēto datu subjektu un jāpieņem lēmums par datu apstrādes pārtraukšanu, ja datu subjekta iesniegtie fakti maina samērīguma līmeni attiecībā uz datu subjekta datu apstrādi, vai jāpieņem lēmums turpināt apstrādāt datus, ja kredītiestāde uzskatāmi spēj parādīt, ka sabiedrības intereses ir svarīgākas par datu subjekta interesēm.

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 45. apsvērumā un Regulas 6. pantā, kā arī 29. panta darba grupas 2014. gada 9. aprīļa "Atzinumā 06/2014 par personas datu apstrādātāja likumīgo interešu jēdzienu saskaņā ar Direktīvas 95/46/EK 7. pantu"[16].

3.2.6. Pārziņa vai trešās personas leģitīmās intereses

"(..) apstrāde ir vajadzīga pārziņa vai trešās personas leģitīmo interešu ievērošanai, izņemot, ja datu subjekta intereses vai pamattiesības un pamatbrīvības, kurām nepieciešama personas datu aizsardzība, ir svarīgākas par šādām interesēm (..)"[17]

[15] Regulas 6. panta 1. punkta "e" apakšpunkts.
[16] 29. panta darba grupas 2014. gada 9. aprīļa "Atzinums 06/2014 par personas datu apstrādātāja likumīgo interešu jēdzienu saskaņā ar Direktīvas 95/46/EK 7. pantu": https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_lv.pdf
[17] Regulas 6. panta 1. punkta "f" apakšpunkts.

Līdzsvarošanas pienākums

Lai šo tiesisko pamatu piemērotu, kredītiestāde attiecībā uz plānoto datu apstrādi veic līdzsvarošanas pārbaudi jeb interešu līdzsvarošanas testu, lai kredītiestāde varētu pieņemt izsvērtu, dokumentētu un pamatotu lēmumu par šī tiesiskā pamata atbilstošu piemērošanu. Prognozējams, ka šī tiesiskā pamata piemērošana kļūs arvien plašāka, līdz ar to kredītiestādēm ir ieteicams izstrādāt iekšējo kārtību, kā veikt šo interešu līdzsvarošanas pārbaudi un kontroli.

Līdzsvarošanas pārbaude ietver vismaz šādas darbības:

1. kredītiestādes vai trešās personas, kurai dati tiks nodoti, leģitīmo interešu būtiskuma izvērtēšana;
2. ietekmes uz datu subjektu izvērtēšana;
3. pasākumu paredzēšana datu subjekta tiesību aizsardzībai.

Kā veikt interešu līdzsvarošanu?

29. panta darba grupas atzinumos[18] ir doti mehānismi un ieteikumi, kā veikt šo interešu līdzsvarošanas pārbaudi, un apstākļi, kuri būtu ņemami vērā, veicot to. Tādējādi līdzsvarošanas pārbaudes procesā būtu jāizvērtē vairāki aspekti.

Kredītiestādes vai trešās personas leģitīmo interešu novērtēšana

Leģitīmām interesēm (ieinteresētība apstrādē) ir jābūt skaidri definētām un pieņemamām saskaņā ar spēkā esošiem tiesību aktiem, kā arī reālām un pašreizējām. Leģitīmas intereses var izrietēt gan no spēkā esošiem tiesību aktiem vai uzraudzības iestāžu vadlīnijām, gan no dažādu kredītiestāžu vai trešās personas pamattiesību īstenošanas (*piemēram, tiesībām uz īpašumu, tiesībām uz efektīvu tiesību aizsardzību un uz taisnīgu tiesu, komercdarbības brīvību, vārda un informācijas brīvību*), gan no sabiedrībā svarīgām interesēm (*piemēram, kredītiestāžu un sabiedrības kopējas intereses nodrošināt, lai pakalpojumus nevar saņemt krāpjoties, vai nepieļaut noziedzīgu nodarījumu izdarīšanu, nodrošināt noguldītāju aizsardzību un to noguldījumos izvietoto līdzekļu drošību*), gan arī no pašas kredītiestādes vai trešās personas individuālām interesēm (*piemēram, nodrošināt savu pakalpojumu kvalitatīvu sniegšanu, risku novēršanu*). Kredītiestādes vai trešo personu intereses bauda lielāku atbalstu sabiedrībā, jo šī interese ir nozīmīgāka. Uz intereses nozīmīgumu var norādīt arī tiesību aktos iekļautās pārziņa vai trešo personu tiesības veikt kādu datu apstrādi vai sasniegt noteiktus nolūkus (*piemēram, Kredītiestāžu biroju likuma 106.panta ceturtajā daļā noteiktas kredītiestāžu, kredītiestāžu meitas sabiedrību, kuras sniedz ar kredītrisku saistītus pakalpojumus, krājaizdevumu sabiedrību un apdrošinātāju tiesības savstarpēji apmainīties ar ziņām par parādniekiem un viņu saistību izpildes gaitu*).

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Ietekmes uz datu subjektu novērtēšana

Kad ir identificētas kredītiestādes vai trešās personas leģitīmās intereses un to būtiskums, ir jāizvērtē otras līdzsvarošanas puses – datu subjektu – intereses. Datu subjektu interešu izvērtēšanā būtu ieteicams izvērtēt šādus apsvērumus:

1. **kādas pozitīvās vai negatīvās sekas plānotā datu apstrāde atstās uz datu subjektu?** Atšķirīgu iespaidu uz datu subjektu atstās datu apstrāde, kura radīs datu subjektam pozitīvas sekas (*piemēram, klienta profilēšanas rezultātā datu subjektam būs iespēja saņemt pakalpojumu ar ievērojamu atlaidi*), un apstrāde, kura radīs datu subjektam negatīvas sekas. Līdz ar to pirmajā gadījumā būs salīdzinoši vieglāk rast līdzsvaru starp pušu interesēm, tomēr otrajā gadījumā kredītiestādes interesei ir jābūt daudz nozīmīgākai. Vērtējot jāņem vērā arī fakts, ka viena datu apstrāde var radīt gan pozitīvas, gan negatīvas sekas vienlaicīgi, šajā situācijā ir jāvērtē visas iespējamās sekas kopsakarā;

[18] Sk.: 29. panta darba grupas 2014. gada 9. aprīļa "Atzinums 06/2014 par personas datu apstrādātāja likumīgo interešu jēdzienu saskaņā ar Direktīvas 95/46/EK 7. pantu": https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_lv.pdf, 7. panta 3.1. punkts.

Ievērojamu risku datu subjekta tiesībām var radīt datu apstrāde, kas var izraisīt fizisku, materiālu vai nemateriālu kaitējumu, īpaši, ja datu apstrāde var izraisīt diskrimināciju, identitātes zādzību vai dokumentu viltošanu, finansiālu zaudējumu, kaitējumu reputācijai, ar dienesta noslēpumu aizsargātu datu konfidencialitātes zaudējumu, neatļautu pseidonimizācijas atcelšanu vai jebkādu citu īpaši nelabvēlīgu ekonomisko vai sociālo situāciju, ja datu subjektiem var tikt atņemtas viņu tiesības un brīvības, vai atņemta iespēja kontrolēt savus datus, ja tiek veikta profilēšana, vai ja apstrāde aptver lielu datu daudzumu un ietekmē lielu skaitu datu subjektu. Līdz ar to, ja ir konstatējams, ka apstrāde varētu radīt kādu no šiem vai vairākus no šiem riskiem, nepieciešams rūpīgi izvērtēt vai kredītiestādes leģitīmā interese ir pietiekoši būtiska.

Tāpat svarīgi ir pēc iespējas ņemt vērā arī datu subjektu individuālo attieksmi pret atsevišķām datu apstrādes situācijām, *piemēram, viens datu subjekts var neitrāli vai pozitīvi attiekties pret telefonisku apsveikumu dzimšanas dienā, tomēr citai personai tas var radīt negatīvas emocijas*;

2. **kādu emocionālo ietekmi var atstāt plānotā datu apstrāde uz datu subjektu?** *Piemēram, kredītiestāde organizē labdarības pasākumu ar mērķi sniegt atbalstu trūcīgajām personām. Pasākuma ietvaros plānota attēlu publicēšana. Ne visi atbalsta saņēmēji varētu būt apmierināti ar viņu attēlu publicēšanu, jo tādējādi tiks atklāta informācija par viņu finansiālajām grūtībām. Šādos gadījumos ieteicama apmeklētāju fotografēšana, piemēram, pie foto sienas, tādējādi nodrošinot tikai tādu viesu attēlu publicēšanu, kas ar savu aktīvu rīcību ir faktiski piekrituši publicēšanai*.

3. **risku iestāšanās iespējamības izvērtējums.** Risku iestāšanās varbūtību var apskatīt no diviem aspektiem:

   a) ja datu apstrāde ir vērsta uz kādu risku novēršanu un/vai mazināšanu (*piemēram, krāpšanas novēršanu, drošību, zādzību novēršanu*), tad kritiski jāizvērtē, cik liela ir riska iestāšanās iespējamība, proti, jo mazāka iespējamība, ka risks īstenosies, jo attiecīgi mazāk būtiska ir kredītiestādes leģitīmā interese, un otrādi. Ja risks pats par sevi ir būtisks, *piemēram, visu klientu datu bāzes pazaudēšana*, tad arī maza riska iestāšanās iespējamība nespētu mazināt kredītiestādes leģitīmās intereses būtiskumu,

   b) jāizvērtē uzglabāto datu nozīmība un līdz ar to arī drošība, respektīvi, jo lielāks risks, ka trešajām personām varētu būt paaugstināta interese par kredītiestādes rīcībā esošiem datiem un paaugstināta vēlme tos iegūt, jo būtiskāki drošības pasākumi kredītiestādei ir jāveic, lai datus aizsargātu. Ja riskus datu drošībai nav iespējams pilnībā novērst vai samazināt risku līdz minimumam, tad būtu jāizvērtē, vai šāda datu apstrāde vispār ir veicama;

4. **datu veidi un iespējamo seku būtiskums nelikumīgas datu apstrādes (piemēram, datu noplūdes vai datu izdzēšanas) gadījumā**. Jo sensitīvāki dati (ar to saprotot gan Īpašu kategoriju datus un datus par sodāmībām, gan arī datu subjekta uzskatus par tam svarīgiem datiem, *piemēram, informācija par klientu un viņa darījumiem, par finanšu resursu pieejamību norēķinu kontā*) tiek uzglabāti un apstrādāti, jo būtiskākai ir jābūt kredītiestādes vai trešās personas leģitīmai interesei, lai pamatotu šādu datu apstrādi. Tāpat atkarībā no datu sensitivitātes ir veicami atšķirīgi pasākumi ievācamās informācijas aizsardzībai;

5. **datu subjekta pamatotās gaidas**. Jāizvērtē datu subjekta attieksme pret kredītiestādi un apstākļiem, kādos dati tika ievākti, un vai datu subjekts datu nodošanas brīdī varēja saprātīgi paredzēt vai pieņemt, ka viņa datu apstrāde varētu notikt attiecīgajā veidā. *Piemēram, klientu izpētes vajadzībām atbilstoši NILLTPFNL prasībām iegūto informāciju nedrīkst izmantot mārketinga nolūkiem, t.i., lai izpētītu klienta dzīves stilu un prognozētu klienta rīcību, tādējādi piedāvājot viņam atbilstošus pakalpojumus*;

6. datu subjekta statuss. Daudz rūpīgāk ir jāizvērtē ietekme uz speciālām sabiedrības grupām, kurām ir atšķirīgas spējas atbilstoši novērtēt situāciju un reaģēt uz to (*piemēram, bērni, seniori, personas ar invaliditāti*), kā arī jāvērtē, vai datu subjekts nav pakļautības attiecībās, kas varētu neļaut viņam pilnībā realizēt savas tiesības, izvairoties no iespējamas negatīvas attieksmes (*piemēram, darbinieki*).

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Kredītiestādes īstenoti papildu drošības pasākumi, lai novērstu nepamatotu ietekmi uz datu subjektiem

Iepriekšējos divos punktos veikto līdzsvarošanas rezultātu vēl var ietekmēt kredītiestādes veiktie papildu pasākumi datu subjekta tiesību aizsardzībai. Jo vairāk šādi pasākumi tiek veikti, jo uzskatāms, ka datu subjekta tiesības ir vairāk aizsargātas, kas var tikt ņemts vērā līdzsvarošanas pārbaudes rezultātā izdarītajos secinājumos, lai konstatētu, vai kredītiestādes vai trešās personas leģitīmās intereses ir pietiekami būtiskas, lai varētu veikt datu apstrādi. Šādiem papildus pasākumiem ir pieskaitāmi, piemēram, šādi pasākumi:

1. **pārvērtēšana**. Būtu nepieciešams nodrošināt periodisku kredītiestādes leģitīmo interešu pārvērtēšanu, tai skaitā pārvērtējot arī ietekmi uz datu subjektu. Pārvērtēšanas biežums būtu atkarīgs no datu apstrādes veida un nolūkiem. Jo mainīgāka vide, jo biežāk būtu jāveic pārvērtēšana. Papildus interešu pārvērtēšana būtu jāveic arī pēc datu subjekta pieprasījuma, ja tas izmanto tiesības iebilst savu datu apstrādei;

2. **drošības pasākumi**. Jo būtiskāka ir iespējamā ietekme uz datu subjektu, jo lielāka uzmanība jāpievērš drošības pasākumiem, tai skaitā pēc iespējas pseidonimizējot vai šifrējot datus;

3. **datu minimizēšana**. Kredītiestādei ir jāizvērtē visas iespējamās alternatīvas savu leģitīmo interešu sasniegšanai un jāizvēlas tāda veida datu apstrāde, kas vismazāk skar datu subjektu un tā datus;

4. **datu subjektu vai to pārstāvju iesaistīšana**. Ja ir iespējams, ieteicams līdzsvarošanas procesā iesaistīt datu subjektus un/vai to pārstāvjus (*piemēram, darbinieku arodbiedrību*), noskaidrojot to viedokļus par izvērtēšanā iesaistītiem aspektiem;

5. **tiesību iebilst datu apstrādei nodrošināšana**. Ja ir iespējams, tad ir ieteicams nodrošināt datu subjektam tiesības iebilst datu apstrādei, kas līdzsvarošanas procesā ir būtisks instruments kredītiestāžu interešu pamatošanā.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Interešu līdzsvarošanas rezultāts

Līdzsvarošanas mērķis nav novērst jebkāda veida negatīvo ietekmi uz datu subjektu (lai gan uz to ir jātiecas), bet gan novērst nesamērīgu ietekmi uz datu subjektu. Līdz ar to kredītiestādes leģitīmā interese var tikt uzskatīta par pamatotu arī gadījumos, ja tā atstāj samērīgu iespaidu uz datu subjektu.

Interešu līdzsvarošanas izvērtējuma dokumentēšana

Ņemot vērā pārskatatbildības principu, interešu līdzsvarošanas izvērtējumu ir ieteicams dokumentēt. Tas palīdzēs arī pie interešu pārvērtēšanas, jo būs fiksēts iepriekšējā vērtēšanā izmantotais pamatojums. Nav nepieciešams katru veikto izvērtējumu noteiktā formā iekšēji saskaņot (*piemēram, saņemt valdes apstiprinājumu*), tomēr ir jābūt iekšējai procedūrai, kas paredzētu vismaz izvērtējuma rezultāta fiksēšanu. Tas arī nodrošinātu iespēju pierādīt, ka interešu līdzsvarošanas izvērtējums ir noticis, kā arī konstatēt izvērtējumā izmantotos apsvērumus. Šāda izvērtējuma veikšana var noritēt arī kā daļa no biznesa projekta izvērtēšanas procedūras (tajā skaitā piesaistot datu aizsardzības speciālistu).

Tabula Nr. 3

Piemērs interešu līdzsvarošanas procesam

Izvērtējamie faktori	Plānotā datu apstrāde: Telefonu sarunu ieraksti pierādījumu (telefonbankas pakalpojuma ietvaros) nodrošināšanas nolūkā
Solis Nr. 1 Iespējamā tiesiskā pamata izvēle	1) Regulas 6. panta 1. punkta "a" apakšpunkta (piekrišana) piemērošana – nebūs iespējama, jo personai nav izvēles iespēja piekrist vai nepiekrist sarunu ierakstam;
	2) Regulas 6. panta 1. punkta "b" apakšpunkta (līgumsaistību izpildei) piemērošana – nebūs atbilstoša, jo pierādījumu nodrošināšana nav nepieciešama tieši pakalpojuma sniegšanai, bet nepieciešamība ir, lai kredītiestāde spētu pierādīt līguma izpildi, ja rastos strīds;
	3) Regulas 6. panta 1. punkta "c" apakšpunkta (juridiska pienākuma izpilde) piemērošana – nav konstatēts, ka kāds tiesību akts, izņemot Finanšu instrumentu tirgus likumu (šajā gadījumā kā pamatojumu var izmantot šo tiesisko pamatu, neveicot līdzsvarošanas pārbaudi), noteiktu pienākumu kredītiestādei veikt šādu sarunu ierakstus;
	4) Regulas 6. panta 1. punkta "d" apakšpunkta (vitāli svarīgas intereses) p5iemērošana – netiek konstatēta vitāli svarīgu interešu aizsardzība konkrētajā apstrādē;
	5) Regulas 6. panta 1. punkta "e" apakšpunkta (sabiedrības intereses vai pārvaldes uzdevumu veikšana) piemērošana – netiek konstatēta būtisku sabiedrības interešu esamība vai pārvaldes uzdevumu izpilde konkrētajā apstrādē;
	6) Regulas 6. panta 1. punkta "f" apakšpunkta (pārziņa leģitīmās intereses) piemērošana – līguma pienācīga neizpilde var radīt kredītiestādei zaudējumu risku, ja klients vērsīsies pret to ar pretenzijām. Īpaši ņemams vērā, ka pakalpojums tiek saistīts ar klientam piederošām materiālām vērtībām, kas ir īpaši sensitīvs jautājums attiecībā uz klientu. Tāpat pierādīšanas pienākumu kredītiestādēm paredz arī maksājumu pakalpojumu un elektroniskās naudas apstrādi reglamentējošie normatīvie akti. Tādējādi kredītiestādei ir nepieciešamība nodrošināties pret iespējamām nepamatotām pretenzijām, saglabājot attiecīgus pierādījumus par rīkojumu došanas faktu un personu, kas rīkojumus devusi.
Solis Nr. 2 Kredītiestādes intereses likumības un būtiskuma izvērtējums	1) Pierādījumu saglabāšana par līgumisku saistību izpildi nav aizliegta tiesību aktos un civilprocesuālajos normatīvajos aktos ir atzīta par nepieciešamu, kā arī to paredz maksājumu pakalpojumu un elektroniskās naudas apstrādi reglamentējošie normatīvie akti, tādējādi tā ir uzskatāma par likumīgu interesi;
	2) interese ir definēta pietiekami konkrēti un nav šaubu par tās saturu;
	3) interese ir pašreizēja un reāla, jo kredītiestāde ir noslēgusi līgumus ar klientiem par attiecīga pakalpojuma sniegšanu.
Solis Nr. 3 Datu apstrādes nepieciešamības (iespējamo alternatīvu) pārbaude	Tiek konstatēts, ka mutiski, izmantojot telefonsakarus, sniegtus rīkojumus nav iespējams pierādīt citādā veidā, kā tikai ierakstot attiecīgu telefonsarunu.

Solis Nr. 4 Datu subjekta interešu novērtēšana	1) Datu subjekta intereses ir ietekmētas, jo tiek ierakstītas datu subjekta sarunas ar kredītiestādes darbiniekiem;
	2) dati nav uzskatāmi par Īpašu kategoriju datiem līdz ar to tie nepakļaujas paaugstinātai aizsardzībai, tomēr tiek ņemts vērā, ka dati par klienta personību un finanšu darījumiem ir paaugstināti aizsargājami saskaņā ar Kredītiestāžu likumu;
	3) datu apstrāde nav vērsta uz neaizsargātām sabiedrības grupām (piemēram, bērni, darbinieki, seniori), tomēr šīs personas var iekļūt to datu subjektu lokā, kuru dati tiek apstrādāti;
	4) dati tiks apstrādāti plašā mērogā – jo ir liels klientu skaits, kuri izmanto minēto pakalpojumu;
	5) datus netiek plānots atklāt publiski, tikai pašiem klientiem, uzraudzības iestādēm, tiesībaizsardzības iestādēm un tiesām, ja nepieciešams;
	6) dati netiks izmantoti profilēšanai;
	7) datu subjekta pamatotās gaidas: datu subjektam vajadzētu apzināties, ka rīkojumu sniegšana par naudas līdzekļu pārskaitījumiem ir paaugstināta riska darījumi, un kredītiestādei jāpierāda rīkojuma sniegšana;
	8) ja datu apstrāde netiktu veikta, tiktu radīta nenoteiktība komerctiesiskajā un civiltiesiskajā vidē, jo klientiem būtu iespēja apstrīdēt veiktos darījumus, kas varētu arī ietekmēt kredītiestādes un līdz ar to arī visa finanšu sektora stabilitāti (ja darījumu apstrīdēšana notiktu plašā mērogā un kredītiestādei nebūtu pierādījumi par atbilstošu rīkojumu saņemšanu un izpildi);
	9) ja sarunas netiktu ierakstītas, riski kredītiestādei būtu tik būtiski, ka šāds pakalpojums netiktu piedāvāts, līdz ar to, tikai pamatojoties uz šāda veida apstrādi ir iespējams datu subjektam sniegt šo pakalpojumu, kas ir ērts veids datu subjektam piekļūt saviem finanšu līdzekļiem;
	10) papildus ir ņemams vērā fakts, ka datu subjektam ir izvēles iespēja izmantot telefonbankas pakalpojumus, kur tiek veikts balss ieraksts, vai citus rīkojumu iesniegšanas veidus, piemēram, internetbankas pakalpojumus vai iesniegt rīkojumus klātienē;
	11) pārmērīgas datu apstrādes risks, proti, nevar izslēgt, ka uz noteikto tālruņa numuru piezvana klients, kurš nedod rīkojumu par maksājuma veikšanu, bet izmanto uzziņām, kur nebūtu nepieciešams veikt sarunas ierakstu, vai arī papildus dotam rīkojumam sniedz cita veida informāciju kredītiestādes darbiniekam, kurai nebūtu nepieciešams ierakstu veikt. Tomēr kredītiestāde ņem vērā, ka jebkuri papildu ierobežojumi (piemēram, nepieļaut klientam sniegt papildu informāciju, kamēr tas nav pārslēdzies uz citu tālruņa līniju, kurā ieraksts netiek veikts) ir apgrūtinoši gan klientam, gan kredītiestādei un var apdraudēt šāda pakalpojuma pastāvēšanu.

Solis Nr. 5 Papildu pasākumi interešu līdzsvarošanai	1) **datu minimizācija** – ņemot vērā to, ka uz kredītiestādes tālruni var zvanīt arī personas, ar kurām nav noslēgts attiecīgs pakalpojuma līgums, vai potenciālie klienti, kā arī esoši klienti, bet par citiem jautājumiem, ir nepieciešams ieviest tehniskus un organizatoriskus pasākumus, kas ļautu datu subjektam izvēlēties sarunas tēmu un, ja sarunas tēma ir tāda, kuru pilnībā vai daļēji nav nepieciešams ierakstīt, nodrošināt iespēju datu subjektam veikt sarunu bez tās ierakstīšanas vai bez sevis identificēšanas;
	2) **funkcionālais nošķirums** – ja sarunas tiek ierakstītas arī citiem nolūkiem (piemēram, kvalitātes nodrošināšanai), būtu jāievieš tehniski un organizatoriski pasākumi, kas nodalītu sarunu ierakstus dažādiem nolūkiem un nepieļautu nolūku sajaukšanos;
	3) **pseidonimizācijas izmantošanas iespējamība** – izvērtējams, vai rīkojumu došanu varētu organizēt, pamatojoties uz klientu/lietotāju numuriem, sarunā nefiksējot citus datus (vārdu, uzvārdu, personas kodu), tādējādi, ja gadījumā telefonsarunu ieraksts kļūtu pieejams personām, kurām nav tiesiska pamata piekļūt attiecīgiem datiem, attiecībā uz tām šie dati būtu anonīmi un netiktu nodarīts kaitējums datu subjekta interesēm;
	4) **datu subjekta informēšana** – ir nepieciešams datu subjektu informēt par šādu datu apstrādi gan līgumā, gan arī pirms ieraksta uzsākšanas, lai datu subjekts apzinātos, ka dati tiek ierakstīti, un atbilstoši rīkotos;
	5) papildus ir izvērtējams, vai nav nepieciešams veikt novērtējumu par ietekmi uz datu aizsardzību;
	6) **glabāšanas termiņi** – klienti var apstrīdēt darījumus 3 gadu laikā (komercdarījuma noilgums) vai atsevišķos gadījumos 10 gadu laikā (vispārējais noilgums), bet saskaņā ar likumu "Par grāmatvedību" attaisnojuma dokumenti glabājami – 5 gadus.
Solis Nr. 6 Atbilstības demonstrēšana un pārredzamības nodrošināšana	1) Datu subjektam ir jābūt pieejamai informācijai par iemesliem, kādēļ kredītiestāžu interese būtiskāka par datu subjekta tiesību ierobežojumu, iekļaujot attiecīgas norādes pakalpojuma līgumā, vispārējos darījumu noteikumos, interneta vietnē un/vai citā datu subjektam pieejamā veidā;
	2) šo novērtējumu dokumentētā veidā saglabāt un nepieciešamības gadījumā darīt pieejamu uzraudzības iestādei;
	3) regulāri pārskatīt šo datu apstrādes procesa izvērtējumu, ņemot vērā attiecīgās apstrādes raksturu un riska līmeni, paredzot attiecīgo pārskatīšanas biežumu jau sākotnējā izvērtējuma laikā.
Solis Nr. 7 Rīcība datu subjekta iebildumu gadījumā	1) Šajā gadījumā nebūtu pamatoti noteikt datu subjektiem beznosacījumu atteikšanās tiesības, ņemot vērā to, ka kredītiestādes interese ir būtiska;
	2) ja datu subjekts iebilst šādai datu apstrādei (piemēram, uzglabāšanai), procesa īpašnieks izvērtē datu subjekta argumentus, un vai tie maina līdzsvarošanas rezultātu un, ja maina, tad veic attiecīgas darbības, lai apstrādi koriģētu.
Solis Nr. 8 Gala lēmums	Atzīt, ka līdzsvarošanas rezultātā kredītiestādes leģitīmās intereses ir nozīmīgākas par datu subjekta aizskārumu, kas pieļauj datu apstrādes veikšanu pamatojoties uz Regulas 6. panta 1. punkta "f" apakšpunktu (pārziņa leģitīmās intereses).

Datu subjekta tiesības iebilst

Izmantojot šo pamatu, ir jārespektē datu subjekta tiesības iebilst apstrādei. Saņemot šādus iebildumus, kredītiestādei, ņemot vērā datu subjekta norādītos iemeslus saistībā ar datu subjekta īpašo situāciju, ir jāpārvērtē datu apstrādes nepieciešamība un samērīgums attiecībā uz konkrēto datu subjektu un jāpieņem lēmums par datu apstrādes pārtraukšanu, ja datu subjekta iesniegtie fakti maina abu pušu interešu līdzsvara līmeni attiecībā uz datu subjekta datu apstrādi, vai datu apstrādes turpināšanu, ja kredītiestāde uzskatāmi spēj parādīt, ka tās vai trešās personas leģitīmās intereses ir svarīgākas par datu subjekta interesēm.

Kādos gadījumos, pirms tam veicot individuālu interešu izvērtējumu jeb interešu līdzsvarošanu, būtu izmantojams šis tiesiskais pamats?

Šo tiesisko pamatu, veicot atsevišķu interešu līdzsvarošanas izvērtēšanu, būtu apsverams izmantot šādos gadījumos:

1. ja apstrāde ir saistīta ar līguma izpildi, tomēr pastāv risks, ka tā nav būtiska līguma pamatfunkciju nodrošināšanai;
2. ja datu apstrādi pieprasa trešo valstu (ārpus ES un EEZ) normatīvie akti vai trešo valstu, ar kurām nav savstarpējās tiesiskās palīdzības līguma, tiesas spriedumi;
3. ja datu apstrāde pamatota ar valsts iestāžu vadlīnijām un rekomendācijām (vairāk skatīties augstāk 3.2.3.punktā);
4. ja normatīvais akts paredz kredītiestādei tiesības (rīcības brīvību) veikt kādu datu apstrādi (vairāk skatīties augstāk 3.2.3.punktā);
5. ja nepieciešama datu apstrāde tiesvedībās;
6. kredītiestādei piesaistot ārējos konsultantus (*piemēram, zvērināti advokāti, revidenti, auditori*), ja šādu konsultantu piesaiste nav noteikta, kā juridisks pienākums;
7. krāpšanas novēršanai;
8. īpašuma aizsardzībai;
9. lai pierādītu savu pienākumu izpildi (piemēram, ierakstot telefonsarunas pakalpojumu kvalitātes kontrolei);
10. datu nosūtīšana citiem grupas uzņēmumiem (ES un EEZ ietvaros) iekšējos administratīvos nolūkos, t.sk. klientu vai darbinieku datu apstrādei;
11. darbinieka interešu konflikta pārbaudes nepieciešamībai, īpaši, ja šādas pārbaudes nepieciešamību nenosaka normatīvie akti.

Kā vēl vienu piemēru datu apstrādei, kas var tikt veikta, pamatojoties uz datu pārziņa leģitīmajām interesēm, var minēt klientu aptaujas, kuras tiek veiktas ar mērķi noskaidrot klienta viedokli par saņemtajiem pakalpojumiem un šo informāciju ņemt vērā, lai

1) uzlabotu pakalpojuma sniegšanu tieši šim klientam, un/vai
2) uzlabotu pakalpojuma sniegšanu kopumā.

Tikšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR Darba grupu 2019. gada 7. martā Datu valsts inspekcija pauda viedokli, ka būtu jāvērtē klientu aptaujas nolūks un saturs. Ja aptauja tiek veikta ar nolūku noskaidrot klienta viedokli par saņemto pakalpojumu un šo viedokli ņemt vērā, lai uzlabotu pakalpojuma kvalitāti šim klientam vai arī klientiem kopumā, šādu datu apstrādi var pamatot ar pakalpojuma sniedzēja leģitīmajām interesēm.

Taču, ja aptauja tiek veikta, lai reizē reklamētu pakalpojuma sniedzēja tēlu un pakalpojumus, šādai datu apstrādei būtu jāsaņem datu subjekta piekrišana. Līdzīgi būtu jāvērtē klientiem sūtītie apsveikumi, piemēram, dzimšanas dienā. Ja reizē ar apsveikumu pakalpojuma sniedzējs reklamē savu tēlu un pakalpojumus, datu apstrāde būtu jāpamato ar klienta piekrišanu. DVI ieskatā, varētu pastāvēt pakalpojuma sniedzēja leģitīmā interese veikt klientu aptaujas vai sveikt klientus ar svētkiem. DVI neidentificēja iespējamo kaitējumu klientiem apstrādājot klientu datus apsveikumu vai aptauju sūtīšanas nolūkā. DVI ieskatā fakts, ka nepastāv, vai pastāv neliels kaitējuma klientam risks ir būtisks apstāklis, kas ņemams vērā veicot līdzsvarošanas testu.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 37., 41., 47., 48. un 49. apsvērumā un Regulas 6. pantā, kā arī 29. panta darba grupas 2014. gada 9. aprīļa "Atzinumā 06/2014 par personas datu apstrādātāja likumīgo interešu jēdzienu saskaņā ar Direktīvas 95/46/EK 7. pantu"[19].

(Ar grozījumiem, kas izdarīti 08.01.2021.)

3.3. Īpašu kategoriju datu apstrāde

Īpašu kategoriju datu nozīmīgums

Īpašu kategoriju dati ir jāapstrādā ar augstākām drošības prasībām, jo nelikumīga Īpašu kategoriju datu apstrāde var nodarīt būtiskāku kaitējumu datu subjekta interesēm. Līdz ar to kredītiestādei būtu jānodala Īpašu kategoriju dati no citiem datiem un jāierobežo piekļuve tiem, kā arī jānosaka paaugstinātas drošības prasības darbībām ar tiem.

Īpašu kategoriju dati var būt sastopami dažādos dokumentos un informācijas vienībās (*piemēram, video ierakstos un fotogrāfijās*), tomēr ir kritiski jāizvērtē, vai šo informāciju ir plānots izmantot kā Īpašu kategoriju datus. Ja šāda nolūka nav, tad attiecīgās informācijas apstrāde nebūtu jāuzskata par Īpašu kategoriju datu apstrādi. Piemēram, ja videonovērošanas ierakstā tiek fiksēta persona, kura ir apģērbta apģērbā, kurš var atklāt tās piederību kādai reliģiskai kustībai, bet nav nolūka šo video ierakstu analizēt tieši šādas informācijas izmantošanai, tad šādu datu apstrāde nebūtu jāvērtē kā Īpašu kategoriju datu apstrāde.

Apstrādes ierobežojumi

Saskaņā ar Regulas 9. panta pirmo daļu Īpašo kategoriju datu apstrāde ir aizliegta, ja vien nav konstatējams kāds no panta otrajā daļā minētajiem izņēmumiem vai arī attiecīgā ES dalībvalsts ir ieviesusi papildu nosacījumus, tostarp ierobežojumus, attiecībā uz ģenētisko datu, biometrisko datu vai veselības datu apstrādi.

Tikšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR Darba grupu 2019. gada 7. martā Datu valsts inspekcija pauda viedokli, ka gadījumos, kad datu subjekts pēc savas iniciatīvas iesniedz datu pārzinim īpašu kategoriju datus, varētu uzskatīt, ka dati iegūti ar datu subjekta nepārprotamu piekrišanu. Ja informācija par piekrišanas atsaukšanu jau ir ietverta datu pārziņa privātuma politikā, klientu var papildus neinformēt par piekrišanas došanas specifiku un iespējām to atsaukt. Turklāt DVI uzskata, ka risks klienta privātuma aizskārumam ir neliels, ja klienta iedotie dati tiek izmantoti, lai pieņemtu klientam labvēlīgu lēmumu.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

[19] 29. panta darba grupas 2014. gada 9. aprīļa "Atzinums 06/2014 par personas datu apstrādātāja likumīgo interešu jēdzienu saskaņā ar Direktīvas 95/46/EK 7. pantu": https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_lv.pdf

Darbinieku veselības datu un informācijas par darbinieka piederību arodbiedrībai apstrāde

Apstrādāt šos datus ir iespējams pamatojoties uz Regulas 9. panta otrā punkta "b" un "h" apakšpunktu, kas pieļauj Īpašu kategoriju datu apstrādi, ja tā ir vajadzīga, lai realizētu pienākumus un tiesības nodarbinātības jomā un darbinieka darbaspējas novērtēšanā, ciktāl to pieļauj dalībvalstu tiesību akti. Tādējādi ir jāievēro arī speciālajās normās noteiktos ierobežojumus šādu datu apstrādei jeb datu minimizāciju, *piemēram, saskaņā ar Darba likuma 101. panta sesto daļu darba devējam ir pienākums noskaidrot, vai darbinieks ir arodbiedrības biedrs tikai pirms darba līguma uzteikšanas, bet attiecībā uz veselības datiem Darba likuma 33. panta ceturtā daļa nosaka darba devējam tiesības iegūt informāciju par darbinieka veselības stāvokli tikai tik daudz, ciktāl tam ir būtiska nozīme darba līguma noslēgšanā un paredzētā darba veikšanā*. Ja, piemēram, saskaņā ar Darba likuma 36. panta otro daļu, darbinieks tiek nosūtīts uz veselības pārbaudi, ārsts norāda tikai to, vai pretendents ir piemērots paredzētā darba veikšanai.

Politiski nozīmīgu personu datu apstrāde

Šo datu apstrāde būtu jāpamato ar Regulas 9. panta 2. punkta "g" apakšpunktu, kas pieļauj politiskās pārliecības datu apstrādi būtisku sabiedrības interešu dēļ, kas nostiprinātas dalībvalsts normatīvajos aktos. Šajā gadījumā papildus ir jāizmanto atsauce uz NILLTPFNL 25. pantā noteikto pienākumu noskaidrot klienta vai tā patiesā labuma guvēja statusu, respektīvi, vai persona ir politiski nozīmīga persona.

Biometrisko datu apstrāde

Ņemot vērā to, ka biometrisko datu apstrāde kļūst arvien populārāka personu identifikācijas procesos, kā arī piekļuves telpām kontroles sistēmās, ir nepieciešams norādīt, ka biometriskie dati ietilpst Īpašu kategoriju datu tvērumā. Līdz ar to šos datus nav iespējams apstrādāt, pamatojoties tikai uz kredītiestādes leģitīmajām interesēm. Biometriskos datus identifikācijai ir iespējams izmantot, saņemot brīvu un nepārprotamu datu subjekta piekrišanu vai, ja biometrisko datu apstrāde ir nepieciešama būtisku sabiedrības interešu dēļ, t.i., ja Latvijas normatīvajos aktos šī interese ir nostiprināta un tādēļ paredzēta biometrisko datu apstrāde.

Pases kopiju ievākšana

Pasēs atsevišķos gadījumos (*piemēram, vecā parauga pases vai ārvalstnieku pases*) tiek atspoguļotas arī ziņas, kas var saturēt Īpašu kategoriju datus, piemēram, ziņas par datu subjekta tautību. Kredītiestādēm varētu būt nepieciešamība apstrādāt pases vai cita identificējoša dokumenta datus – klientu un darbinieku identifikācijai. Attiecībā uz klienta identifikāciju saskaņā ar NILLTPFNL 14. panta pirmo daļu, kredītiestādei ir pienākums izgatavot to personu apliecinošu dokumentu kopijas, uz kura pamata ir veikta klienta identifikācija, tajā skaitā arī pases kopija. Šī juridiskā pienākuma izpilde ir pietiekams pamats, lai apstrādātu arī visu informāciju, kas atrodas personu apliecinoša dokumenta kopijā (t.sk. personas augums un atsevišķos gadījumos personas tautība, ja ir norādīts).

Jāņem vērā, ka saskaņā ar datu minimizācijas principu, lai sasniegtu NILLTPFNL noteikto mērķi, pietiekama būtu pases pirmā atvēruma (kurā ir atspoguļoti personas pamatdati) un atsevišķos gadījumos arī atvēruma, kurā ir dati par uzturēšanās atļauju, kopija un pārmērīgi ir kopēt turpmākos pases atvērumus, kuros var būt norādīta papildu informācija. Turklāt jāņem vērā, ka saskaņā ar Ministru kabineta 2012. gada 21. februāra noteikumiem Nr. 134 "Personu apliecinošu dokumentu noteikumi" personas tautība tiek norādīta pases 3. lappusē (proti, turpmākajos pases atvērumos), tādējādi kredītiestādei, ievācot personu apliecinoša dokumenta pamata atvēruma kopiju, nemaz nav nepieciešams apstrādāt Īpašu kategoriju datus.

Tomēr jāņem vērā izņēmumi, ja citu valstu personu apliecinošu dokumentu vai vecāka izlaiduma Latvijas personu apliecinošu dokumentu pamata atvērumā ir norādīti Īpašu kategoriju dati, tad šāda apstrāde būs pamatota un leģitīma.

Attiecībā uz personu apliecinošu dokumentu kopiju izdarīšanu saistībā ar darba tiesiskām attiecībām, jānorāda, ka šāda prakse varētu tikt uzskatīta par pārmērīgu, jo likumdevējs jau Darba likuma 35. panta pirmās daļas 1. punktā ir norādījis, ka, lai personu identificētu, ir pietiekami ar personu apliecinoša dokumenta uzrādīšanu. Savukārt nepieciešamo informāciju, kas vajadzīga, lai pierādītu personas identifikāciju, ir iespējams fiksēt, *piemēram, personas kartiņā*.

Kredītiestāde kā apdrošināšanas starpnieks

Ja kredītiestāde nodarbojas ar apdrošināšanas starpniecību saskaņā ar Apdrošināšanas un pārapdrošināšanas starpnieku darbības likuma normām un šīs apdrošināšanas starpniecības ietvaros tai nepieciešams apstrādāt Īpašu kategoriju datus, tad šajās attiecībās kredītiestāde, visticamāk, būtu uzskatāma kā apstrādātājs apdrošināšanas sabiedrības (pārziņa) interesēs. Līdz ar to kredītiestādei būtu jāpakļaujas apdrošināšanas sabiedrības norādījumiem attiecībā uz apstrādātajiem datiem, nošķirot apdrošināšanas starpnieka apstrādājamos datus no pārējiem kredītiestādes apstrādājamiem datiem, kā arī būtu jāuztur datu apstrādātāja darbību reģistrs.

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 35., 51., 52., 53. un 54. apsvērumā un Regulas 9. pantā.

3.4. Datu par sodāmību un pārkāpumiem apstrāde

Apstrādes ierobežojumi

Datu apstrādi par sodāmību un pārkāpumiem vai ar tiem saistītiem drošības pasākumiem var veikt tikai oficiālas iestādes kontrolē vai tad, ja apstrādi atļauj ES vai dalībvalstu nacionālie tiesību akti. Līdz ar to datus par sodāmību un pārkāpumiem (t.sk. krimināls odiem un administratīvo pārkāpumu sodiem) kredītiestāde drīkst apstrādāt tikai likumā noteiktajos gadījumos un norādītajā apmērā.

Tikšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR Darba grupu 2019. gada 7. martā Datu valsts inspekcija pauda viedokli, ka gadījumos, kad datu subjekts pēc savas iniciatīvas iesniedz datu pārzinim datus par sodāmību un pārkāpumiem, varētu uzskatīt, ka dati iegūti ar datu subjekta piekrišanu. Ja informācija par piekrišanas atsaukšanu jau ir ietverta datu pārziņa privātuma politikā, klientu var papildus neinformēt par piekrišanas došanas specifiku un iespējām to atsaukt. Turklāt DVI uzskata, ka risks klienta privātuma aizskārumam ir neliels, ja klienta iedotie dati tiek izmantoti, lai pieņemtu klientam labvēlīgu lēmumu.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Dati par sodāmību un pārkāpumiem darba attiecībās

Lai izpildītu pienākumu pārbaudīt personas sodāmību, kredītiestāde pieprasa informāciju par personas sodāmību (no pašas personas vai attiecīgiem reģistriem), ja personu plānots iecelt kā atbildīgo par NILLTPFNL prasību ievērošanu, jo NILLTPFNL 10. panta ceturtā daļa nosaka, ka šādus pienākumus drīkst veikt persona, kura nav notiesāta par tīšu noziegumu izdarīšanu. Tāpat kredītiestādei saskaņā ar Kredītiestāžu likuma 25. panta pirmo daļu ir pienākums pārliecināties par valdes locekļu, iekšējā audita dienesta vadītāja, risku direktora, par atbilstības kontroli atbildīgās personas, sabiedrības kontroliera, ārvalsts kredītiestādes filiāles Latvijā un kredītiestādes filiāles ārvalstīs vadītāja, kā arī prokūrista datiem par

sodāmību, pārliecinoties, vai minētā persona nav notiesāta (vai kriminālliet a izbeigta) par tīša noziedzīga nodarījuma izdarīšanu, arī ļaunprātīgu bankrotu. Sodāmības nepieļaujamība var tikt minēta arī citos tiesību aktos un attiecībā uz citām darbinieku kategorijām, *piemēram, attiecībā uz revīzijas komitejas locekļiem*[20].

Tāpat saskaņā ar Kredītiestāžu likuma 34.[5] pantu kredītiestādei ir pienākums apstrādāt pretendentu un darbinieku datus par sodāmību, jo kredītiestāde nedrīkst nodarbināt personas, kuras ir tieši saistītas ar finanšu pakalpojumu sniegšanu vai kredītriska pārvaldību vai ietekmē kredītiestādes riska profilu, ja persona ir sodīta par tīša nozieguma izdarīšanu pret valsti, īpašumu vai pārvaldības kārtību vai par tīša nozieguma izdarīšanu tautsaimniecībā vai valsts institūciju dienestā, vai par tāda nozieguma izdarīšanu, kas saistīts ar terorismu, un sodāmība par to nav noņemta vai dzēsta.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Dati par sodāmību un pārkāpumiem klientu izpētē

Pamatojoties uz NILLTPFNL 41. panta otrās daļas 4. punktu, kredītiestādēm ir tiesības un, atsevišķos gadījumos, pat pienākums apstrādāt klienta, potenciālā klienta, klienta patiesā labuma guvēju, klienta pārstāvju datus par sodāmību, par noziedzīgiem nodarījumiem tautsaimniecībā, veicot klienta noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas riska novērtējumu, kā arī gadījumos, kad tiek vērtēta nepieciešamība ziņot Kontroles dienestam par aizdomīgu darījumu vai atturēties no aizdomīga darījuma veikšanas.

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 75. apsvērumā un Regulas 10. pantā.

3.5. Bērnu personas datu apstrādes noteikumi

Bērnu īpašā aizsardzība

Bērniem (personām līdz 18 gadu vecumam, vai līdz pilngadības sasniegšanai, ja pilngadība iestājās pirms 18 gadu vecuma sasniegšanas) pienākas īpaša datu aizsardzība, jo viņiem nav tādas pašas rīcībspējas kā pilngadīgai personai un viņi var pietiekami neapzināties attiecīgos riskus, sekas un aizsardzības pasākumus un savas tiesības saistībā ar datu apstrādi. Šāda īpaša aizsardzība ir jāpiemēro bērnu datu apstrādei, kas veikta gan ar automatizētiem līdzekļiem, gan arī manuālai, strukturētai apstrādei, ko neveic ar automatizētiem līdzekļiem. Nebūtu ieteicams uz bērniem attiecināt automatizētu lēmumu pieņemšanu.[21] Ja tomēr automatizēta lēmumu pieņemšana tiek attiecināta, tad rūpīgi jāizvērtē, vai šāda datu apstrāde nevar nodarīt kādu kaitējumu bērna interesēm. Pieļaujama automatizētu lēmumu pieņemšana attiecībā uz bērnu datu apstrādi, būtu, piemēram, lai pasargātu bērna finanšu līdzekļus no dažādiem riskiem, kurus bērns varētu pilnībā nenovērst vai pietiekami samazināt ar saviem paša spēkiem.

Bērnu informēšana

Izvēloties saziņas veidu ar bērnu, informācija tam ir jāsniedz un saziņa jāveic tik skaidrā un vienkāršā valodā, lai bērns to varētu viegli saprast. Tāpat būtiski par datu subjekta tiesībām informēt ne tikai bērna likumisko pārstāvi, bet arī bērnu, ja viņš atbilstoši kredītiestādes praksei var īstenot kādu noteiktu tiesību apjomu patstāvīgi bez likumiskā pārstāvja līdzdalības. Vienlaikus, ja bērna datus izmanto jomā, kur tam nav paredzēta pastāvība attiecībā uz lēmuma pieņemšanu, pārzinim ir jānodrošina bērna likumīgā pārstāvja informēšana par plānoto datu apstrādi.

[20] Finanšu instrumentu tirgus likuma 55.[6] panta ceturtā daļa.
[21] Regulas 71. apsvērums.

Bērnu datu izmantošana informācijas sabiedrības pakalpojumos

Ja informācijas sabiedrības pakalpojumos[22] ir paredzēts apstrādāt bērna datus, pamatojoties uz bērna sniegtu piekrišanu, ir jāņem vērā Fizisko personu datu apstrādes likuma 33. pantā paredzētais, ka bērns patstāvīgi ir tiesīgs izteikt piekrišanu sākot no 13 gadu vecuma un bērnam ir jābūt informētam par to, kādai datu apstrādei tiek sniegta piekrišana. Ja tiek radīta iespēja informācijas sabiedrības pakalpojumus lietot bērniem jaunākiem par 13 gadu vecumu, tad kredītiestādei ir jāpārliecinās, vai bērna vietā piekrišanu ir devusi vai vismaz apstiprinājusi persona, kurai ir aizgādības vai aizbildnības tiesības attiecībā pret bērnu. Kārtību kā kredītiestāde pārliecinās par bērna piekrišanas došanu ieteicams iekļaut attiecīgajā procedūrā.

Attiecībā par pārliecības līmeni par to, ka piekrišanu ir devusi vai apstiprinājusi persona, kurai ir aizgādības vai aizbildnības tiesības, kredītiestādei ir jāpieliek saprātīgas pūles, lai šo saikni pārbaudītu. To iespējams veikt, ņemot vērā pieejamās tehnoloģijas, līdz ar to akceptējams ir risinājums, ja iepriekš identificēta persona (*piemēram, vecāks*) rakstiski deklarētu (*piemēram, izmantojot internetbankas risinājumu*) saikni ar aizgādībā vai aizbildnībā esošiem bērniem un autorizētu atsevišķas savu bērnu darbības informācijas sabiedrības pakalpojumos.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Bērnu tiesības lemt par saviem datiem citās sfērās

Kopumā ir jāņem vērā, ka bērnam līdz pilngadības sasniegšanai nav pilna rīcības spēja (izņemot augstāk minēto izņēmumu attiecībā uz piekrišanu), tādējādi arī bērnu tiesību realizācijai ir jānotiek ar bērna vecāku vai aizbildņu starpniecību, tai skaitā datu kopiju pieprasīšanu, apstrādes darbību ierobežošanu, datu dzēšanu un citu tiesību realizāciju. Tomēr, ja kredītiestāde piedāvā speciālus pakalpojumus bērniem, ir ieteicams, ievērojot bērna briedumu un spēju lemt par savu tiesību realizēšanu, izvērtēt iespēju arī bērnam patstāvīgi realizēt atsevišķas tiesības, ciktāl tās nespēj radīt bērnam kaitējumu. Šādai atsevišķu tiesību realizācijas piešķiršanai bērniem nevajadzētu ierobežot bērna vecākiem vai aizbildņiem iespēju pārraudzīt ar bērnu saistītu datu apstrādi un, ja nepieciešams, realizēt visas datu subjekta tiesības attiecībā uz to.

Papildus jāpiemin, ka Regula nosaka, ka iepriekš minētie noteikumi par bērnu datu izmantošanu informācijas sabiedrības pakalpojumos neietekmē vispārējās līgumtiesības, t.sk. noteikumu attiecībā uz bērna noslēgta līguma spēkā esamību, noslēgšanu vai sekām. Līdz ar to pieļaujama ir bērna lemšana par saviem datiem, piemēram, darba attiecībās, kur saskaņā ar Darba likuma 37. pantu bērns patstāvīgi var noslēgt darba līgumu sākot ar 15 gadu vecuma sasniegšanu un bērna rīcība ar savu atsevišķo mantu kā to paredz Civillikuma normas.

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 38. un 58. apsvērumā un Regulas 8. pantā.

[22] Saskaņā ar Informācijas sabiedrības pakalpojumu likuma 1. panta 2. punkta noteikto definīciju, informācijas sabiedrības pakalpojums ir distances pakalpojums (puses vienlaicīgi nesatiekas), kuru parasti sniedz par maksu, izmantojot elektroniskus līdzekļus (elektroniskas datu apstrādes un uzglabāšanas, tajā skaitā ciparu saspiešanas, iekārtas) un pēc pakalpojuma saņēmēja individuāla pieprasījuma. Informācijas sabiedrības pakalpojumi ietver preču un pakalpojumu elektronisko tirdzniecību, komerciālu paziņojumu sūtīšanu, iespēju piedāvāšanu informācijas meklēšanai, piekļuvi pie tās un informācijas ieguvei, pakalpojumus, kas nodrošina informācijas pārraidi elektronisko sakaru tīklā vai piekļuvi elektronisko sakaru tīklam, informācijas glabāšanu.
Saskaņā ar Eiropas Parlamenta un Padomes Direktīvas (ES) 2015/1535 (2015. gada 9. septembris), ar ko nosaka informācijas sniegšanas kārtību tehnisko noteikumu un Informācijas sabiedrības pakalpojumu noteikumu jomā 1. panta 1. punkta "b" apakšpunktu Informācijas sabiedrības pakalpojums, tas ir, jebkāds pakalpojums, ko parasti sniedz par atlīdzību no attāluma (pakalpojumu sniedz bez vienlaicīgas pušu klātbūtnes), ar elektroniskiem līdzekļiem (pakalpojumu nosūta un galamērķī saņem ar elektroniskas apstrādes (ietverot digitālu kompresiju) un datu uzglabāšanas aparatūras palīdzību un ka to pilnībā pārraida, nosūta un saņem pa vadiem, pa radio ar optiskiem vai citiem elektromagnētiskiem līdzekļiem) un pēc pakalpojumu saņēmēja individuāla pieprasījuma pakalpojumu sniedz, pārraidot datus pēc individuāla pieprasījuma).

4. DATU MINIMIZĒŠANA

4.1. Mehānismi datu minimizēšanas nodrošināšanai

Principa būtība

Datu minimizēšanas būtība ir noskaidrot minimāli nepieciešamo datu apjomu un apstrādes apmēru, lai sasniegtu iepriekš noteiktos nolūkus. Lai pārliecinātos, ka dati tiek apstrādāti atbilstošā apmērā:

1. kredītiestādei ir precīzi jānodefinē nolūks, jo tikai precīzs nolūks ļauj saprast, kāds datu apjoms un apstrādes apmērs ir minimāli nepieciešams, lai sasniegtu attiecīgo nolūku. *Piemēram, pārāk vispārīgi nodefinēts nolūks – "klientu apkalpošana" –, neļautu precīzi saprast, kādu datu kategoriju apstrāde ir minimāli nepieciešama*. Ja šis nolūks tiktu sadalīts apakšnolūkos – "klienta identificēšana" (klātienē, elektroniski), "klientu attiecību uzturēšana", "konkrēta pakalpojuma sniegšana", "pierādījumu nodrošināšana rīkojumu izpildei" –, jau daudz efektīvāk būtu iespējams izvērtēt šo nolūku sasniegšanai nepieciešamo datu minimālo apjomu katrā no gadījumiem;

2. kredītiestādei būtu jāizvērtē visas alternatīvas, kā ar mazāku datu apstrādi varētu sasniegt noteikto nolūku, un jāizvēlas alternatīva ar vismazāko iejaukšanos privātumā. *Piemēram, ja kredītiestāde vēlas sūtīt klientiem īsziņas (SMS) atgādinājumus par līguma izpildi, tad šī nolūka sasniegšanai nav nepieciešams ievākt arī klienta elektroniskā pasta adreses, vai, piemēram, testējot informācijas sistēmas, tas ir jādara ar neīstiem datiem, nevis izmantojot reālu klientu datu bāzi, tādējādi apdraudot datu precizitāti, drošību un konfidencialitāti*;

3. jāizlemj, ar kādiem tehniskiem risinājumiem apstrāde tiks nodrošināta un jāizvēlas vismazāk datu subjekta interešu aizskarošs. *Piemēram, ja videonovērošanas kameras ir izvietotas drošības nolūkiem, lai konstatētu īpašumā iekļuvušas personas, nebūtu samērīgi veikt arī audio ierakstu, jo tas nav minimāli nepieciešams nolūka sasniegšanai*. Būtu jāizvērtē arī personas, kurām savu pienākumu veikšanai ir nepieciešams piekļūt attiecīgiem datiem, tādējādi veicot piekļuves un apstrādes tiesību segmentēšanu un kontroli, kā arī pēc iespējas kredītiestāde nodrošina, lai persona piekļūst tikai tādam datu apjomam, kas nepieciešams tai uzticēto pienākumu izpildei.

Pseidonimizācija

Pseidonimizācija ir metode datu apstrādei tādā veidā, lai datus nebūtu iespējams sasaistīt ar konkrētu datu subjektu bez papildu informācijas izmantošanas, ja šāda papildu informācija tiek turēta nošķirti un papildus aizsargāta, *piemēram, klienta numuru izmantošana, ja informācija par klientu (vārds, uzvārds, personas kods) tiek glabāta nošķirti*.

Šis ir viens no mehānismiem kā minimizēt datu apstrādi, jo personas, kas piekļūst šādiem datiem, nespēj šos datus sasaistīt ar konkrētu personu, līdz ar to attiecībā uz viņiem tos var uzskatīt par anonīmiem datiem. Tomēr, izvēloties pseidonimizācijas metodes, ir rūpīgi jāpārliecinās, ka visi identifikatori, pēc kuriem personu var atpazīt, tiek aizstāti, *piemēram, nepietiekami ir CV aizklāt pretendenta vārdu, uzvārdu un personas kodu, lai uzskatītu, ka CV iekļautie dati ir pseidonimizēti, jo pēc citas dokumentā esošas informācijas (darba gaitas, izglītības iestādes) šo personu var identificēt*.

Pseidonimizācija, izvērtējot katras kredītiestādes darbības specifiku, varētu tikt izmantota, piemēram, glabājot datus, nošķirot pseidonimizētos datus no datiem, kas atšifrē pseidonimizētos datus, tādējādi nodrošinot, ka, piekļūstot pamatdatiem, nav iespējams identificēt personu, uz kuru attiecīgā informācija attiecas. Būtu izvērtējams, vai atsevišķām struktūrvienībām to pienākumu veikšanai nav pietiekami apstrādāt pseidonimizētus datus (piemēram, sagatavojot dažādas kredītiestādes iekšējas darbības pārskatus), tādu pašu izvērtējumu veicot arī attiecībā uz apstrādātājam uzticētām datu apstrādēm.

4.2. Datu minimizēšana atsevišķiem nolūkiem

Datu glabāšana rezerves kopiju vajadzībām

Datu iekļaušana rezerves kopijās ir pietiekami pamatota kredītiestādes leģitīma interese apstrādāt šos rezerves kopijās glabātos datus, pat ja citi nolūki datu apstrādei ir izpildīti. Atsevišķus datus no rezerves kopijas nav iespējams izdzēst, jo tad tas var būtiski ietekmēt citu personu tiesības uz datu saglabāšanu, jo "izjaucot" rezerves kopiju, tā var nepildīt savu funkciju – atjaunot datus, ja tas būtu nepieciešams, līdz ar to arī iespaidojot datu integritāti un drošību. Tomēr kredītiestādei ir jānosaka rezerves kopiju veidošanas biežums, kā arī glabāšanai nepieciešamais rezerves kopiju skaits, nosakot, ka vecākās rezerves kopijas tiek dzēstas. Tā tiktu nodrošināta arī datu dzēšana pēc kredītiestādes leģitīmā nolūka īstenošanas.

Dokumenti, kas satur datus ar dažādiem dzēšanas termiņiem

Ja dokuments satur datus ar dažādiem dzēšanas termiņiem vai sasaistīti dokumenti satur atsevišķus dokumentus ar dažādiem glabāšanas termiņiem, *piemēram, ar elektronisko parakstu parakstīta dokumentu pakete, kurā iekļauti dažādi atsevišķi dokumenti ar atšķirīgiem glabāšanas termiņiem, vai dokuments, kurā dažādi darbinieki parakstās par iepazīšanos ar procedūru*, pamatoti ir glabāt dokumentu vai dokumentu paketi līdz brīdim, kamēr iestājas visu dokumentā minēto datu dzēšanas vai dokumentu paketē esošu atsevišķu dokumentu dzēšanas termiņš.

Rīcība ar darbinieka elektronisko pastu, darbiniekam izbeidzot darba tiesiskās attiecības
Ja darbinieks ir izbeidzis darba tiesiskās attiecības ar kredītiestādi, kredītiestādei nevajadzētu izmantot automatizētas pārsūtīšanas funkciju uz cita darbinieka elektroniskā pasta adresi, bet gan izvērtēt iespējamību nodrošināt promesošā darbinieka elektronisko pastu ar automātisku paziņojumu elektroniskā pasta vēstules sūtītājiem, informējot par to, ka darbinieks vairs nav darba tiesiskajās attiecībās ar kredītiestādi, un norādot, ka šī elektroniskā pasta adrese netiek pārlūkota un lūgt elektroniskā pasta vēstuli pārsūtīt darbiniekam, kurš aizvieto promesošu darbinieku.

Šajā gadījumā elektroniskā pasta vēstules saturā minēto datu izpaušana būtu atstāta elektroniskā pasta sūtītāja kontrolē un viņš varētu izvēlēties, zinot elektroniskā pasta sūtījuma nolūku un saturu, elektroniskā pasta vēstules pārsūtīšanu vai atturēties no tās, ja elektroniskā pasta vēstule satur personiska rakstura saraksti.

Klienta kredītspējas izvērtēšana izmantojot informāciju, kuru klients pats apzināti publiskojis

Ja kredītiestādei ir leģitīms nolūks datu ievākšanai, piemēram, klienta kredītspējas izvērtēšanai, pamatojoties uz klienta iesniegtu pieteikumu ar kredītrisku saistīta pakalpojuma nodrošināšanai, ir pieļaujama šādas informācijas ievākšana arī no publiski pieejamiem avotiem, tai skaitā no avotiem, kuros klients pats apzināti ir publicējis par sevi informāciju (t.sk. publiski pieejamos sociālajos tīklos). Tomēr, ņemot vērā apstrādes mērogu un ietekmi uz datu subjektiem, kredītiestādei būtu jāizvērtē novērtējuma par ietekmi uz datu aizsardzību veikšanas nepieciešamība šādos apstrādes gadījumos.

Dokumentu ar paplašinātu datu apjomu saņemšana

Atsevišķos gadījumos var rasties situācija, kad kredītiestāde patstāvīgi ievāc informāciju (piemēram, no publiskiem reģistriem) vai klients kredītiestādei, lai tā veiktu klienta izpēti, iesniedz dokumentus, kuri satur arī citu datu subjektu datus, *piemēram, sadarbības līgumi, komercsabiedrības dibināšanas dokumenti, kuros atrodami arī citu dibinātāju dati, dažāda veida protokoli ar citu personu datiem*. Šajā gadījumā šāda dokumenta glabāšana būtu uzskatāma par samērīgu un nepieciešamu, jo, ja dokumenta saturs tiktu rediģēts (*piemēram, izdzēšot attiecīgos citu datu subjektu datus*), tas varētu nepieļaujami ietekmēt dokumenta juridisko spēku, līdz ar to ir pieļaujams dokumentu glabāt arī ar citu personu datiem, kamēr tas ir nepieciešams klienta izpētes nodrošināšanas nolūka sasniegšanai.

Tomēr, ja ir konstatēts, ka klients ir iesniedzis dokumentu, kurš satur citu personu datus un tas nav nepieciešams kredītiestādei tās nolūku sasniegšanai (*piemēram, klienta izpētei*), šāds dokuments būtu jāiznīcina vai tajā esošie dati jāaizklāj, ja tas neatstāj ietekmi uz dokumenta juridisko spēku. Tomēr, ja šādus trešo personu datus kredītiestādes sistēmās nav iespējams atlasīt pēc šīs trešās personas parametriem, tad attiecīgajai trešās personas datu apstrādei nav piemērojamas Regulas prasības un datu subjekta tiesības.[23]

Darbinieku elektroniskā pasta vēstuļu uzraudzība

Nebūtu pieļaujama darbinieku elektroniskā pasta vēstuļu satura pastāvīga uzraudzība (izņemot atsevišķus gadījumus, kad šāda uzraudzība ir pamatota, piemēram, aizdomas, ka darbinieks izmanto iestādes e-pastu pretēji iekšējās kārtības noteikumos atrunātajam un tajos arī paredzēta kārtība šādai kontrolei vai disciplinārpārkāpumu izmeklēšanas nolūkā). Lai samazinātu ietekmi uz darbinieka privātumu, ieteicams ir izmantot tehniskus risinājumus, kas identificē riskus (*piemēram, atsevišķu atslēgas vārdu vai frāžu konstatēšana elektroniskā pasta tekstā vai kredītiestādes rīcībā esoša informācija, kas var liecināt par kredītiestādes interešu apdraudējumu – komercnoslēpuma, t.sk. datu, izpaušanu, interešu konflikta esamību, noziedzīga nodarījuma plānošana vai veikšana vai cita būtiska apdraudējuma kredītiestādes interesēm esamība*). Tādējādi darbinieki netiktu pakļauti pārmērīgai elektroniskā pasta vēstuļu kontrolei, bet datu apstrāde tiktu vērsta tikai uz personām, par kurām ir aizdomas par pārkāpumiem darba attiecību laikā. Tomēr, ņemot apstrādes mērogu, kredītiestādei ir jāizvērtē novērtējuma par ietekmes uz datu aizsardzību veikšanas nepieciešamība.

4.3. Datu glabāšanas ilgums

Datu glabāšanas ilgums ir cieši saistīts ar nepieciešamību izmantot datus konkrētiem nolūkiem. Līdz ar to, nosakot glabāšanas ilgumu, vērā ņemami vairāki faktori, kas uzskaitīti tabulā.

[23] Regulas 2. panta 1. punkts.

Tabula Nr. 4

Apsvērumi glabāšanas termiņa noteikšanai

Faktori	Glabāšanas termiņi
1. Vai dati nepieciešami spēkā esoša pakalpojuma līgumu izpildei?	Dati būtu jāglabā līdz brīdim, kad attiecīgais pakalpojuma līgums ir spēkā, vai atsevišķi datu veidi kamēr ar klientu ir darījuma attiecības. Tomēr pakalpojuma līguma izbeigšanas gadījumā ir jāpārliecinās, vai nav radušies citi pamatoti nolūki datu glabāšanai (skat. Tabulas turpmākajos punktos norādītos faktorus);
2. Vai dati ir jāglabā normatīvajos aktos noteikto pienākumu izpildei?	Ievērojot Latvijas tiesību aktos noteiktos glabāšanas termiņus, piemēram: 1) NILLTPFNL prasību izpildei – **visu darījumu attiecību laiku** un **5 gadus** (vai ilgāk, ja Kontroles dienests ir devis rīkojumu) NILLTPFNL 37. pantā noteiktajos gadījumos attiecībā uz klienta identifikācijas dokumentiem, informāciju par klientiem un tā kontiem, paziņojumu par patiesā labuma guvēju, saraksti ar klientu, citus klienta izpētes dokumentus; 2) Likuma "Par grāmatvedību" prasību izpildei, t.sk. **10 gadus** grāmatvedības reģistriem un grāmatvedības organizācijas dokumentiem, vai **5 gadus** attaisnojuma dokumentiem; 3) Finanšu instrumentu tirgus likumā noteiktajos gadījumos – **10 gadus** attiecībā uz ar finanšu instrumentiem veikto darījumu attaisnojumu dokumentu un citu dokumentu glabāšanu[24]; 4) Patērētāju tiesību aizsardzības likumā noteiktajos gadījumos – **1 gadu** pēc patērētāja kreditēšanas līgumā noteikto saistību izpildes attiecībā uz ar kredīta izsniegšanu saistīto dokumentāciju[25]; 5) FKTK noteikumu un norādījumu izpildei.
3. Vai ir nepieciešams datus saglabāt, lai aizsargātu kredītiestādes intereses dažādu prasījumu gadījumā pēc darījumu attiecību izbeigšanas?	Dažādu prasījumu noilgumu termiņi, piemēram: 1) **60 gadi** – Kredītiestāžu likuma 71. pantā noteiktais klienta prasījumu tiesību termiņš attiecībā uz noguldījumiem kredītiestādē; 2) **10 gadi** – vispārīgais saistību tiesību noilguma termiņš (Civillikuma 1895. pants); 3) **3 gadi** – no komercdarījuma izrietošie prasījumi (Komerclikuma 406. pants).
4. Klienta lietas glabāšana.	Ņemot vērā to, ka klienta lieta (klienta dokumenti, kuri tiek glabāti gan vienkopus, gan atsevišķi) var sastāvēt no dokumentiem ar dažādiem glabāšanas termiņiem, uzskatāms, ka kredītiestāde ir tiesīga uzglabāt visu dokumentu kopumu, t.sk. līgumus, 10 gadus pēc visu darījuma attiecību izbeigšanās ar klientu (atbilstoši Civillikuma 1895.pantā noteiktajam vispārīgajam saistību tiesību noilguma termiņam, lai aizsargātu savas leģitīmās intereses prasības gadījumā).
5. Klienta izpētes dokumentu glabāšana.	NILLTPFN likuma 37.panta otrā daļa paredz, ka likuma subjekts glabā visu klienta izpētes gaitā iegūto informāciju piecus gadus pēc darījuma attiecību izbeigšanas. Pēc minētā termiņa beigām minētie dokumenti (informācija) ir jāiznīcina/jādzēš, ja vien likuma subjekts nav saņēmis NILLTPFN likuma 37.panta trešajā daļā minēto norādījumu pagarināt glabāšanas termiņu.
6. Vai ir kādas citas svarīgas leģitīmas intereses, kuras datu dzēšanas gadījumā varētu tikt aizskartas? *Piemēram, datu glabāšana rezerves kopijās vai datu subjekts ir realizējis savas tiesības ierobežot datu apstrādi.*	Attiecībā uz rezerves kopiju veidošanu glabāšanas ilgums varētu tikt noteikts, kamēr rezerves kopija ir nepieciešama. Rezerves kopiju gadījumā būtu nepieciešams noteikt kārtību, cik bieži rezerves kopijas tiek sagatavotas un cik pēdējās rezerves kopijas ir saglabājamas. Vecāko kopiju dzēšanas laikā tiktu nodrošināta adekvāta datu subjektu datu dzēšana.

[24] Finanšu instrumentu tirgus likuma 124. panta pirmās daļas 9. un 10. punkts
[25] Patērētāju tiesību aizsardzības likuma 8. panta piektās daļas 3. punkts.

7. Pierādījumi par likumīgas datu apstrādes veikšanu iepriekšējā periodā. *Piemēram, pierādījumi par piekrišanas esamību iepriekš veiktām apstrādes darbībām.*	Tā kā normatīvie akti nenosaka saīsinātu noilguma termiņu datu subjektu prasījumiem pret kredītiestādi saistībā ar likumīgas datu apstrādes nodrošināšanu, ir piemērojams vispārējais civiltiesiskais noilguma termiņš 10 gadi. Līdz ar to, lai pierādītu likumīgas datu apstrādes nodrošināšanu, ir nepieciešams saglabāt likumīgas datu apstrādes pierādījumus 10 gadus pēc datu apstrādes pārtraukšanas. Tāpat, ja piekrišana sniegta telefonsarunas laikā, telefonsarunas ieraksta glabāšanas termiņš ir atkarīgs no tā, cik ilgu laiku ir paredzēts glabāt pierādījumu par piekrišanas sniegšanu/saņemšanu.
8. Pierādījumi par likumīgas datu apstrādes veikšanu, ja līgums netiek noslēgts, taču ir veikti pasākumi līguma noslēgšanai.	Pirms līguma noslēgšanas ar potenciālo klientu kredītiestādei var būt nepieciešams informāciju par konkrēto personu pārbaudīt publiskos reģistros. Ņemot vērā to, ka datu subjektam ir tiesības 2 gadu periodā saņemt informāciju par datu saņēmēju kategorijām, tad kredītiestādēm var būt tiesisks pamats (leģitīmā interese) informāciju par informācijas iegūšanas pamatu glabāt, lai pierādītu tās apstrādes leģitimitāti. Tomēr šāda datu apstrāde (glabāšana) ir jāvērtē no samērīguma aspekta.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Ja, vērtējot konkrētu datu glabāšanas termiņu, ir konstatējami dažādi pamatoti glabāšanas termiņi, piemēram, tiesību normas nosaka vienu glabāšanas termiņu, bet kredītiestāde konstatē, ka savu interešu aizsardzībai ir nepieciešams lielāks glabāšanas termiņš, pamatoti ir datus glabāt tik ilgi, lai izpildītu visus pamatotos glabāšanas nolūkus.

Izvērtējot datu glabāšanas termiņus, ir rekomendējams ņemt vērā arī Latvijas Finanšu nozares asociācijas izstrādātos Ieteikumus dažādu dokumentu glabāšanas termiņu noteikšanai.

Ieteicams regulāri pārskatīt dokumentu/datu glabāšanas nepieciešamību, meklējot iespējas saīsināt glabāšanas termiņus.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Vai būtu jānošķir dati, kas glabāti ikdienas vajadzībām, no tiem datiem, kas glabāti pēc darījumu attiecību izbeigšanas?

Ir ieteicams nodalīt datus, kuri nepieciešami ikdienas vajadzībām, no datiem, kuri tiek glabāti citiem nolūkiem, un noteikt atšķirīgus pieejas risinājumus, jo tas samazinātu to personu loku, kas varētu piekļūt datiem, kā arī minimizētu riskus, ja ikdienā izmantojamai datu bāzei notiktu neatļauta piekļuve.

Datu minimizēšanas atkārtota izvērtēšana, nosakot glabāšanas termiņus

Sniedzot klientam pakalpojumu, piemēram, uz līguma pamata, ir pamatota nepieciešamība pēc noteikta datu apjoma, lai pakalpojumu varētu pienācīgi sniegt, tomēr, vērtējot glabāšanas termiņus pēc darījuma attiecību izbeigšanas, ir jāpārvērtē arī šo nolūku sasniegšanai nepieciešamo datu apjomu, *piemēram, saglabājot datus par klienta darījumiem, lai aizsargātu kredītiestādes intereses dažādu iespējamo prasījumu pret kredītiestādi gadījumā, visticamāk, nebūs nepieciešams saglabāt ikdienišķu kredītiestādes saraksti ar klientu*.

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 28. un 29. apsvērumā un Regulas 5. pantā.

5. DATU SUBJEKTA TIESĪBAS

Pārzinim ir jānodrošina iespēja datu subjektam realizēt Regulas 12.– 22. pantā noteiktās tiesības, t.sk. tiesības uz informāciju, tiesības piekļūt saviem datiem, tiesības labot datus, tiesības tikt aizmirstam, tiesības ierobežot apstrādi, tiesības uz datu pārnesamību, tiesības iebilst un tiesības automatizēta individuālu lēmuma pieņemšanas procesā, tostarp profilēšanā, kā arī Regulas 14. un 34. pantā minēto saziņu attiecībā uz apstrādi, kā arī ziņošanu par datu labošanu vai dzēšanu, vai apstrādes ierobežošanu, vai par datu aizsardzības pārkāpumu.

Latvijas Finanšu nozares asociācijas GDPR Darba grupas ieskatā, datu aizsardzības tiesības ir uzskatāmas par personiska rakstura tiesībām, līdz ar ko to īstenošanai ir nepieciešams speciāls pilnvarojums. Tikšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR Darba grupu 2019. gada 7. martā Datu valsts inspekcija pauda viedokli, ka datu subjekts var pilnvarot citu personu veikt datu subjekta pieprasījumu. Taču, lai pārliecinātos par datu subjekta patieso gribu, šādam pilnvarojumam būtu jābūt detalizētam un precīzam – t.i. būtu jābūt tieši attiecināmam uz Regulā noteikto tiesību īstenošanu.

Visa saziņa un visas darbības, ko pārzinis īsteno saskaņā ar Regulu un saistībā ar datu subjekta pieprasījumu īstenošanu, jāveic bez maksas.

Ja pārzinis secina, ka pieprasījums ir acīmredzami nepamatots vai pārmērīgs, pārzinim ir pienākums uzskatāmi parādīt, ka pieprasījums ir acīmredzami nepamatots vai pārmērīgs. Kredītiestāde veic izvērtējumu, vadoties pēc konkrētās situācijas un konkrētā datu subjekta pieprasījuma. Lai izvērtētu, vai datu subjekta pieprasījums ir acīmredzami nepamatots vai pārmērīgs, pārzinis var ņemt vērā un vērtēt šādus faktorus:

1. pieprasījuma iesniedzēja un datu subjekta, kas norādīts pieprasījumā, vai par kuru dati tiek pieprasīti, identitāte;
2. pieprasāmo/labojamo datu apjoms un nepieciešamie resursi šāda pieprasījuma apstrādei;
3. datu subjekta pieprasījuma saturs, salīdzinot ar vēsturiskiem pieprasījumiem, lai izvērtētu, vai šāds pieprasījums nav jau iepriekš iesniegts un apstrādāts;
4. datums, kad datu subjekts pēdējo reizi iesniedzis pieprasījumu vai vērsies kredītiestādē saistībā ar datu apstrādi;
5. kādas darbības vēsturiski ir veiktas ar datu subjekta datiem un cik regulāras ir pārziņa apstrādes darbības/izmaiņas datu subjekta datos;
6. datums, kad datu subjekta datos pēdējo reizi izdarīti labojumi, dati dzēsti, bloķēti vai veiktas citas darbības/izmaiņas, pamatojoties uz pieprasījumu;
7. vai datu subjekts nav jau vienreiz saņēmis kredītiestādes atbildi uz datu subjekta iesniegto pieprasījumu;
8. vai pieprasījumā ietvertais juridiskais pamatojums vai faktisko apstākļu izklāsts pēc būtības nav mainījies salīdzinājumā ar iepriekš sniegto atbildi uz pieprasījumu;
9. citus konkrētā datu subjekta pieprasījuma aspekti, kas varētu norādīt, ka datu subjekta pieprasījums ir acīmredzami nepamatots vai pārmērīgs.

Pēc datu subjekta pieprasījuma izvērtējuma veikšanas ir jāizdara secinājumi un attiecīgi jāveic šādas darbības:

1. ja datu subjekta pieprasījums ir pamatots, kredītiestādei ir pienākums uz to ir reaģēt, sniegt atbildi un nodrošināt datu subjekta pieprasījuma izpildi bez maksas;

2. ja tiek secināts, ka datu subjekta pieprasījums ir acīmredzami nepamatots vai pārmērīgs, kredītiestāde var:

   a) pieprasīt saprātīgu maksu, kas noteikta kredītiestādes cenrādī, ņemot vērā administratīvās izmaksas, kas saistītas ar informācijas vai saziņas nodrošināšanu vai pieprasītās darbības veikšanu (piemēram, darbinieku resursu izmaksas, informācijas nesēja izmaksas, pasta pakalpojumu izmaksas, tomēr nav pieļaujams, ka datu subjekta tiesību īstenošanas risinājumu izstrādes izmaksas tiek pārnestas uz klientiem, kuri realizē savas tiesības, proti, noteiktajām izmaksām ir jāattiecas tieši uz konkrēto pieprasījumu);

   b) atteikties izpildīt pieprasījumu.

Gadījumos, kad datu subjekta pieprasījums nav saņemts valsts valodā vai tajā valodā, kurā šī kredītiestāde nodrošina savus pakalpojumus, kredītiestāde ir tiesīga piemērot saprātīgu samaksu, lai segtu tulkošanas izmaksas, vai arī atteikties izpildīt pieprasījumu.

Pārskatatbildības principa ievērošanai ieteicams izveidot datu subjektu pieprasījumu apstrādes procedūru, kā arī paredzēt datu subjektu pieprasījumu izpildes dokumentēšanu (t.sk. ar auditācijas pierakstiem), it īpaši gadījumos, kad pieprasījuma izpilde tiek pilnībā vai daļēji atteikta vai arī tiek pieprasīta samaksa par pieprasījuma izpildi vai arī pieprasījuma izpildes rezultātā dati tiek nodoti trešajām personām.

Turpmāk šajā nodaļā tiks atspoguļotas datu subjekta tiesības uz kurām attiecas iepriekš minētie datu subjekta pieprasījuma izvērtēšanas soļi, kas sniedz kredītiestādei iespēju izvērtēt datu subjekta pieprasījuma pamatotību un noteikt tālākās darbības, kas saistītas ar iesniegtā pieprasījuma apstrādi.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

5.1. Tiesības uz informāciju

Informācijas sniegšanas vispārējās prasības

Saskaņā ar Regulas 12. pantu pārzinis sniedz informāciju datu subjektam par datu apstrādi:

1. kodolīgā, pārredzamā un saprotamā, viegli pieejamā veidā (rakstiski, elektroniski un pēc datu subjekta pieprasījuma arī mutiski);

2. izmantojot skaidru un vienkāršu valodu, īpaši attiecībā uz informāciju, kas sniedzama bērniem;

3. bez maksas, izņemot gadījumus, ja datu subjekta pieprasījums ir acīmredzami nepamatots vai pārmērīgs.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Tabula Nr. 5

Kāda informācija sniedzama datu subjektam?

Sniedzamā informācija:	Ja dati ir iegūti no datu subjekta	Ja dati nav iegūti no datu subjekta	Tiesību piekļūt saviem datiem (5.2. nod.) realizācija
Kredītiestādes un attiecīgā gadījumā kredītiestādes kā pārziņa pārstāvja identitāte un kontaktinformācija	✓	✓	
Datu aizsardzības speciālista kontaktinformācija (ja tāds ir norīkots), *piemēram, datuspeciālists@kredītiestāde.lv*	✓	✓	
Apstrādes nolūki, kam paredzēti dati, kā arī apstrādes tiesiskais pamats	✓	✓	✓
Apstrādāto datu kategorijas		✓	✓
Kredītiestādes vai trešās personas leģitīmās intereses, ja apstrāde pamatojas uz šo tiesisko pamatu	✓	✓	
Datu saņēmēji vai saņēmēju kategorijas*	✓	✓	✓
Attiecīgā gadījumā – informācija par datu nosūtīšanu uz trešo valsti un piemērotās garantijas datu aizsardzībai	✓	✓	✓
Datu glabāšanas ilgums vai kritēriji glabāšanas termiņa noteikšanai	✓	✓	✓
Informācija par datu subjekta tiesību pastāvēšanu (*piemēram, tiesības piekļūt datiem, tiesības labot datus, tiesības dzēst datus, tiesības ierobežot datu apstrādi, tiesības iebilst pret datu apstrādi, tiesības uz datu pārnesamību*)	✓	✓	✓
Informācija par tiesībām atsaukt piekrišanu, ja apstrāde pamatota uz piekrišanu	✓	✓	
Informācija par tiesībām iesniegt sūdzību uzraudzības iestādei	✓	✓	✓
Informācija par datu iegūšanas avotiem		✓	✓
Informācija, vai datu sniegšana ir noteikta saskaņā ar likumu vai līgumu, vai tā ir priekšnosacījums, lai līgumu noslēgtu, kā arī informāciju par to, vai datu subjektam ir pienākums datus sniegt, un par sekām datu nesniegšanai	✓		
Informācija par automatizētu lēmumu pieņemšanas, t.sk. profilēšanas, veikšanu, informācija par lēmumu pieņemšanas loģiku, apstrādes nozīmīgumu un paredzamajām sekām	✓	✓	✓
Kad informācija sniedzama:	Datu iegūšanas laikā	1) Saprātīgā termiņā pēc personu datu iegūšanas (ne vēlāk kā viena mēneša laikā); 2) ja datus ir paredzēts izmantot saziņai ar datu subjektu – vēlākais tad, kad ar datu subjektu notiek pirmā saziņa; 3) ja datus ir paredzēts izpaust citam saņēmējam, vēlākais tad, kad dati pirmo reizi tiek izpausti.	Bez nepamatotas kavēšanās un jebkurā gadījumā mēneša laikā pēc pieprasījuma saņemšanas (vajadzības gadījumā minēto laikposmu var pagarināt vēl uz diviem mēnešiem, ņemot vērā pieprasījumu sarežģītību un skaitu)

* Tikšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR Darba grupu 2018. gada 21. maijā Datu valsts inspekcija pauda viedokli, ka pārzinim patstāvīgi no gadījuma uz gadījumu (*case by case*) ir jāizvērtē kādu informāciju un kādā apjomā sniegt datu subjektam, ja tas pieprasa informāciju par apstrādātāju saskaņā ar Regulas 15. panta 1. punkta "c" apakšpunktu. DVI ieskatā tikai datu saņēmēju kategoriju norādīšana, nenorādot atsevišķi katru datu saņēmēju (nosaukumu vai citus identifikatorus), kas var skart pārziņa vai apstrādātāja komerciālās intereses, atbilst Regulai.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Informācijas sniegšanas organizācija

Ņemot vērā, ka sniedzamās informācijas apjoms ir ievērojams, atkarībā no saziņas formas ir rūpīgi jāizvērtē, , kāda informācija ir sniedzama datu subjektam tieši un kāda pastarpināti, jo atsevišķos gadījumos visas informācijas sniegšana vienkopus var radīt pretējas sekas un datu subjekts nespēs uztvert informāciju. *Piemēram, informējot par videonovērošanu, nebūs iespējams visu informāciju izvietot uz informējošām uzlīmēm vai zīmēm, tādēļ saskaņā ar Fizisko personu datu apstrādes likuma 36. panta trešo daļu tur būtu jānorāda vismaz pārziņa nosaukums, kontaktinformācija, datu apstrādes nolūki, kā arī norāde par iespēju iegūt citu Regulas 13.pantā norādīto informāciju (piem., atsauce uz kredītiestādes mājaslapas adresi vai privātuma politiku*).

Papildus būtu ieteicams izmantot modernās tehnoloģijas informācijas sniegšanai, *piemēram, QR kodus* (*Quick Response Code*), lai datu subjektam būtu ērti iegūt papildu informāciju. Arī izmantojot saziņai interneta vidi, ir jāvērtē sniedzamās informācijas apjoms, un, iespējams, informācija būtu sadalāma tādā, kura ir izvietojama aktīvajā lietotāja zonā (bet salīdzinājumā ar videonovērošanas veikšanas brīdinājuma uzlīmēm, interneta vidē aktīvajā lietotāja zonā informāciju noteikti būs iespējams sniegt plašāku), un tādā, uz kuru var novirzīt ar norādēm (hipersaitēm), bet ņemot vērā to, lai šī papildu informācijas apskate netiktu apgrūtināta un tai piekļuve būtu tikpat ērta kā aktīvās vietnes sadaļas lietošana.

Šāds pats modelis būtu izvērtējams arī komunicējot ar klientu klātienē vai rakstveidā, jo ne vienmēr datu subjekts šo informāciju varēs uztvert vienlaicīgi un efektīvi. Līdz ar to būtu ieteicams apsvērt iespēju būtisko informēšanas sadaļu sniegt mutiski vai iekļaut rakstveida dokumentā, turklāt otru sadaļu iekļaut speciāli izveidotos uzskates materiālos, kas tiek izsniegti klientam vai pievienoti, *piemēram, līguma dokumentācijai*. Piemēram, vispārējie darījumu noteikumi varētu būt viens no tiem dokumentiem, kurā tiek sniegta informācija kredītiestādes klientam par kredītiestādes īstenoto personas datu apstrādi.

Tāpat, komunicējot ar klientu pa telefonu, pirms telefonsarunas ierakstīšanas ieteicams datu subjektu informēt par datu apstrādi, sniedzot atsauci uz kredītiestādes mājaslapas adresi vai privātuma politiku.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Gadījumi, kuros informāciju var nesniegt

Datu subjekta informēšanas nodrošināšana ir svarīgs pārskatatbildības elements, līdz ar to kredītiestādei būtu jācenšas informēt datu subjektus par to datu apstrādi, tomēr Regula paredz arī atsevišķus izņēmumu gadījumus, kad informāciju datu subjektam par tā datu apstrādes veikšanu var nesniegt. Šādus gadījumus, kad informāciju nav iespējams sniegt, būtu nepieciešams dokumentēt. Saskaņā ar Regulu šie gadījumi, kad informāciju var nesniegt ir šādi:

1. **ja informācija jau ir datu subjekta rīcībā**, *piemēram, ar datu subjektu tiek slēgts papildu pakalpojuma līgums un visa informācija tika sniegta, lai noslēgtu sākotnējo līgumu*. Tomēr kritiski ir jāizvērtē, vai klienta rīcībā ir visa nepieciešamā informācija un vai pārzinim ir iespējams pierādīt šādas informācijas esamību datu subjekta rīcībā. Ja ir konstatējams un pierādāms, ka klienta rīcībā ir daļēja informācija, tad būtu jāsniedz informācija tikai par trūkstošajām informācijas vienībām;

2. **ja šādas informācijas sniegšana nav iespējama vai tā prasītu nesamērīgi lielas pūles**, piemēram, pārmērīgi būtu nodrošināt kredītpieteikumos iekļauto potenciālo ķīlas devēju un galvinieku informēšanu, saņemot kredītpieteikumu, tomēr informēšana būtu jāveic brīdī, kad ar ķīlas devēju un galvinieku tiek noslēgts līgums.

   Tāpat ir pieļaujams neinformēt tās fiziskās personas, kuru dati ir kādos no klientu iesniegtajiem līgumiem vai ievākti no trešajām personām (piemēram, publiskiem reģistriem), kuru datus nav primāra nolūka apstrādāt. Datu subjekta informēšanas aizliegums atsevišķos gadījumos varētu tikt noteikts normatīvajos aktos, piemēram, NILLTPFNL izpildes ietvaros ir aizliegts informēt klientu par to, ka par darījumiem ir informēts Kontroles dienests, kā arī citos gadījumos, kad normatīvajos aktos ir aizliegts informēt personu par to, ka ziņas ir sniegtas prokuratūrai vai tiesai;

3. **ja informācijas iegūšana vai izpaušana ir skaidri paredzēta ES vai Latvijas tiesību aktos**, *piemēram, NILLTPFNL 18.pantā noteiktais gadījums patiesā labuma guvēja datu iegūšanai, Kredītiestāžu likuma 63. panta noteiktie izpaušanas gadījumi, Kredītinformācijas biroju likumā noteiktās tiesības iegūt un sniegt informāciju u.c.*;

4. **ja ir jāsaglabā datu konfidencialitāte, ievērojot dienesta noslēpuma glabāšanas pienākumu, ko reglamentē ES vai Latvijas tiesību akti**. Šis izņēmuma gadījums ir vairāk attiecināms uz valsts pārvaldes iestādēm.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Vai informēšanas prasības attiecas arī uz klientiem, kuru datu apstrāde uzsākta pirms Regulas piemērošanas sākuma dienas?

Informēšanas prasību izpilde ir attiecināma uz visiem datu subjektiem neatkarīgi no tā, vai datu apstrāde ir uzsākta pirms Regulas piemērošanas uzsākšanas vai pēc tās. Saprātīgs risinājums kā informēt esošos klientus/datu subjektus būtu informāciju par izmaiņām informācijas apjomā, kā arī pašu papildināto informāciju ziņas veidā nosūtīt klientiem elektroniskā pasta sūtījumā, izvietot paziņojumu kredītiestāžu internetbanku un citu pakalpojumu platformās, vai arī izvietot kredītiestādes interneta vietnē, lai informācija būtu pieejama arī citām datu subjektu grupām, piemēram, patiesā labuma guvējiem, trešajām personām, kuru dati tiek apstrādāti, lai nodrošinātu pakalpojumus klientiem.

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 58., 60., 61., 62. un 73. apsvērumā un Regulas 12., 13. un 14. pantā, kā arī EDAK 2020. gada 29. janvāra "Pamatnostādnēs 3/2019 par personas datu apstrādi, izmantojot videoierīces"[26].

(Ar grozījumiem, kas izdarīti 08.01.2021.)

[26] EDAK 2020. gada 29. janvāra "Pamatnostādnes 3/2019 par personas datu apstrādi, izmantojot videoierīces": https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_lv.pdf

5.2. Tiesības piekļūt saviem datiem

Tiesības piekļūt saviem datiem būtība

Šo tiesību ietvaros datu subjektam ir šādas tiesības:

1. **saņemt apstiprinājumu savu datu apstrādei**, respektīvi, uz datu subjekta pieprasījuma saņemt atbildi no kredītiestādes, ka datu subjekta dati tiek/netiek apstrādāti. Kredītiestādei ir pienākums sniegt atbildi arī tad, ja pieprasītāja datus kredītiestāde neapstrādā;

2. **piekļūt saviem datiem** – iegūstot savu datu (nevis dokumentu) kopiju, piemēram, izdruku ar datu subjekta datiem no sistēmas, kurā dati tiek glabāti, vai apstrādāto datu kopumu norādīt atbildes vēstulē datu subjektam;

3. **saņemt papildu informāciju par savu datu apstrādi** (līdzīgi kā tiesības tikt informētam realizācijas ietvaros).

Tiesības piekļūt saviem datiem mērķis

Šīs tiesības mērķis ir nodrošināt datu subjektiem tiesības piekļūt saviem datiem, lai jebkurā no datu apstrādes posmiem pārliecinātos par datu precizitāti un datu apstrādes likumību. Ja datu subjekts vēlās izmantot tiesības piekļūt saviem datiem un saņemt savu personas datu kopiju, lai tālāk šos datus nodotu citam saņēmējam, piemēram, tiesai, tad šāds pieprasījums nebūtu uzskatāms par datu subjekta pieprasījumu Regulas 15.panta izpratnē.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Datu kopija

Datu subjekta piekļuves tiesības ir realizējamas attiecībā uz datiem no datu apstrādes sistēmas, nevis dokumentiem, līdz ar to datu subjektam nav tiesību uzstāt uz dokumentu vai dokumentu kopiju izsniegšanu,[27] izņemot gadījumus, ja datu subjekts spēj pamatot īpašu nepieciešamību saņemt dokumenta kopiju, piemēram, ja tikai no dokumenta satura un formas objektīvi var izsecināt datu nozīmību un iespējamās sekas, kādas šāda apstrāde var atstāt uz datu subjektu. Tādējādi dokumentu kopijas, noraksti, izraksti un izdrukas būtu izsniedzamas par maksu, jo uz šiem gadījumiem neattiecas Regulas 12. panta piektajā daļā noteiktās datu subjekta tiesības piekļūt saviem datiem un saņemt savu datu kopiju bezmaksas. Atsevišķos gadījumos vai attiecībā uz atsevišķām datu subjektu kategorijām (piem., senioru segmentā) komercbankas var paredzēt izņēmumus.

Tāpat datu subjektam nav tiesību pieprasīt piekļūt konkrētiem failiem, kuri satur datus, kaut gan šāda piekļuves sniegšana var būt viens no risinājumiem, kā nodrošināt datu subjekta tiesības.

Tikšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR Darba grupu 2018. gada 21. maijā Datu valsts inspekcija pauda viedokli, ka, nodrošinot datu subjekta piekļuves tiesības atbilstoši Regulas 15.pantam, pārzinis nevar aprobežoties tikai ar datu kopiju. Proti, pārzinim būtu jāatbild uz visiem jautājumiem, kas ir uzskaitīti VDAR 15. panta pirmajā daļā.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

[27] Sk. arī: Latvijas Finanšu nozares Asociācija, FKTK un DVI, Infolapa "Mīti un patiesība. Vispārīgā datu aizsardzības regula: ko tā nozīmē man kā bankas klientam", Septembris, 2018: https://www.financelatvia.eu/wp-content/uploads/2018/09/Vispariga-datu-aizsardzibas-regula_-ko-ta-nozime-man-ka-bankas-klientam-1.pdf

Citu personu tiesību un brīvību ievērošana

Datu subjekta tiesības iegūt datus ir jāvērtē kontekstā ar citu personu (arī kredītiestādes un citu datu subjektu) tiesībām un brīvībām, *piemēram, datu subjektam nebūtu tiesības pieprasīt nerediģētu videonovērošanas ierakstu, kurā datu subjekts ir redzams kopā ar citām personām*. Šādu ierakstu varētu izsniegt tikai rediģētā veidā. Pieprasījuma izpildes rezultātā izsniegt informāciju, kas satur arī trešo personu datus nepārprotami var, ja ir saņemta šo personu piekrišana vai šāda informācija jau atrodas pieprasījuma iesniedzēja rīcībā. Citos gadījumos ir jāizvērtē, vai attiecīgajos apstākļos ir pieļaujams, ka pieprasījuma iesniedzējs saņem attiecīgos trešo personu datus.

Tāpat rūpīgi ir jāizvērtē informācijas sniegšana datu subjektam, kura dati atrodas cita klienta darbību pamatojošos dokumentos, kas iegūti veicot klienta izpēti (*piemēram, NILLTPFNL prasību ietvaros klients ir iesniedzis sadarbības līgumu ar citu fizisku personu*). Kredītiestādei ir jāapzinās, ka izsniedzot nerediģētu informāciju vai nerediģētu dokumentu, kredītiestāde var izpaust informāciju par to, ka līgumā norādītais datu subjekta sadarbības partneris ir kredītiestādes klients, tādējādi apdraudot Kredītiestāžu likumā nostiprināto klienta noslēpumu. Līdz ar to kredītiestādei kā pārzinim šis izvērtējums par izpaužamās informācijas apjomu ir jāveic īpaši rūpīgi, ņemot vērā to, ka noteikti dati tiek uzskatīti par neizpaužamiem atbilstoši Kredītiestāžu likumam.

Piemēram, auditācijas ierakstu izsniegšanu par personām, kuras piekļuvušas attiecīga datu subjekta datiem, sākotnēji varētu aizstāt ar norādi vienīgi uz datu saņēmēju kategorijām, kuri var piekļūt datiem (*piemēram, kredītiestādes darbinieki, apstrādātāja darbinieki*), un izsniegt informāciju par konkrētu personu, kas piekļuvusi datu subjekta datiem, pēc kompetentās valsts iestādes pieprasījuma (*piemēram, aizdomas par datu noplūdi*), tādējādi aizsargājot, piemēram, darbinieka tiesības uz savu datu aizsardzību, tai skaitā aizsargājot informāciju par sevi, proti, par savu nodarbinātību pie attiecīgā darba devēja.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Pieprasījumu izpildes termiņi

Pieprasīto informāciju kredītiestāde sniedz bez nepamatotas kavēšanās un jebkurā gadījumā mēneša laikā no pieprasījuma saņemšanas informē datu subjektu par veiktajām darbībām. Laika posmu pieprasījuma izpildei, ņemot vērā pieprasījumu sarežģītību un skaitu, var pagarināt vēl uz diviem mēnešiem. Par termiņa pagarināšanu datu subjekts jāinformē mēneša laikā no pieprasījuma saņemšanas.

Informācijas sniegšanas forma

Informāciju datu subjektam var sniegt, izmantojot dažādas pieejamās formas, pielāgojot to attiecīgā datu subjekta vajadzībām. Tomēr kā informācijas sniegšanas pamatforma būtu jānosaka papīra vai elektroniska forma (piemēram, internetbanka), kā arī būtu jābūt iespējai datu subjektu informēt arī mutiski, ja datu subjekts to pieprasa. Vērā ņemams apstāklis formas noteikšanā ir pierādījumu nodrošināšana kredītiestādei par sava pienākuma izpildi. Par labo praksi Regulas 63. apsvērumā atzīta attālinātas piekļuves nodrošināšana sistēmai, *piemēram, internetbankai, kas datu subjektam nodrošinātu tiešu piekļuvi saviem datiem*.

Ņemot vērā, ka sniegtajiem datiem jābūt saprotamiem, lai datu subjekts varētu pilnvērtīgi realizēt tiesības kontrolēt savu datu kvalitāti un apstrādes likumību, atsevišķos gadījumos var būt nepieciešams izsniegtajiem datiem pievienot papildu informāciju, kas ļautu saprast izsniegto datu nozīmi. *Piemēram, ja attiecībā uz personu ir izdarītas atzīmes iekšēju kodu veidā, datu subjektam ir jāsniedz attiecīgo apzīmējumu izskaidrojums*.

Attīstoties personu izpratnei par datu aizsardzību, datu subjektu pieprasījumu skaits varētu pieaugt un kredītiestādēm var nākties apstrādāt lielu pieprasījumu apjomu. Turklāt, ja kredītiestādēs noteikti personas datu veidi tiek glabāti novecojušās sistēmās, tad automatizēt datu subjektu piekļuves tiesību realizēšanas sistēmas var būt sarežģīts uzdevums. Papildus tam kredītiestādēs par klientiem var būt milzīgs datu apjoms, kur visas šīs informācijas izsniegšanas gadījumā var netikt sasniegts datu subjekta kā „ikdienas klienta" pieprasījuma mērķis, proti, saņemt informāciju par datu apstrādi uztveramā formātā.

Ņemot vērā, augstāk minētos apsvērumus, kredītiestādes var veidot datu subjektu piekļuves tiesību realizēšanas sistēmu ar daudzpakāpju pieeju.

Ja datu subjekta pieprasījumā nav norādīti specifiski datu veidi vai noteikts datu apjoms, kas interesē datu subjektu, tad sākotnēji kredītiestāde datu subjektam nodrošina pieeju aktuāliem pamatdatiem un sniedz vispārēju pārskatu par datiem, kas tiek apstrādāti kredītiestādē, norādot datu subjekta pamatinformāciju – datus par personu, kontaktinformāciju, informāciju par klienta produktiem, to termiņiem, sniedzot šādu pārskatu viegli uztveramā formā. Turklāt pirmās pakāpes atbildi uz datu subjekta pieprasījumu var pilnībā vai daļēji automatizēt (*piemēram, attiecībā uz informāciju, kas jau ir strukturēta kredītiestādes sistēmās*), tādējādi sniedzot iespēju pašam subjektam piekļūt šai informācijai (*piemēram, internetbankā*).

Tikšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR Darba grupu 2019. gada 7. martā Datu valsts inspekcija pauda viedokli, ka, ja personas dati vairs nav atlasāmi sistēmā, bet ir nodoti glabāšanai arhīvā, datu subjektu var informēt par šo faktu, kā arī pieprasīt samaksu par piekļuvi šiem datiem.

Ja no datu subjekta pieprasījuma jau izriet nepieciešamība piekļūt specifiskai informācijai, kuru neaptvertu pirmā atbilde vai arī datu subjekts pēc pirmās pakāpes atbildes saņemšanas izmanto savas tiesības un vēlas piekļūt kādai specifiskai informācijai, kredītiestādei pieprasījums jāapstrādā individuāli atkarībā no datu subjekta pieprasījuma, termiņu atbildes sagatavošanai skaitot no jauna. Tikšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR Darba grupu 2019. gada 7. martā Datu valsts inspekcija pauda viedokli, ka pārzinis var jautāt datu subjektam, ar kādu mērķi šis pieprasījums ir veikts un kādam mērķim ir paredzēts izmantot datus. Sniedzot atbildi uz datu subjekta pieprasījumu, būtu jāskatās no datu subjekta perspektīvas, jo datu subjekts izmanto Regulas 15. pantā paredzētās tiesības, lai labotu, dzēstu vai pārnestu savus datus. Līdz ar ko kredītiestāde var lūgt datu subjektu precizēt informācijas apjomu, uz kuru informāciju un kurām apstrādes darbībām pieprasījums attiecas, kā arī lūgt izskaidrot pieprasījuma pamatojumu (*piemēram, ja arī pēc pirmās atbildes saņemšanas datu subjekts lūdz piekļuvi pilnīgi visiem saviem datiem*). Šīs tiesības nodrošināšanu neietekmē fakts, ka datu subjekts iepriekš ir ticis informēts par datu apstrādes aspektiem.

Tikšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR Darba grupu 2019. gada 7. martā Datu valsts inspekcija pauda viedokli, ka personas dati, kas atrodami kredītiestādes memorandos par klientu vai piezīmēs pie klienta profila, var līdzināties subjektīvām piezīmēm tā saucamajā "Eksaminācijas lietā"[28]. Vienlaicīgi pārzinim var būt arī leģitīmā interese kredītiestādē esošo drošības prasību dēļ saglabāt savus iekšējos procesus nošķirtus no izpaušanas uz āru – šajā gadījumā personas dati būtu jānodala.

Turklāt Datu valsts inspekcija uzskata, ka IT apakšsistēmas, kas sniedz atbalstu un fiksē, kas ir piekļuvis datiem, jo īpaši IT drošības apakšsistēmas, pilda tehnisko risinājumu funkcijas, līdz ar ko dati no šīm sistēmām neattiecas uz datu subjektu pieprasījumu Regulas izpratnē, bet gan uz datu kontroli un pārziņa īstenoto kontroli pār datiem.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

[28] Sk.: Peter Nowak pret Data Protection Commissioner, Lieta C-434/16, 20.12.2017. spriedums: http://curia.europa.eu/juris/document/document.jsf?text=&docid=198059&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=635195

Saistība ar datu pārnesamību

Ja datu subjekts ir norādījis uz nepieciešamību piekļūt saviem datiem, lai tos saglabātu vai atkārtoti izmantotu, tad šāds pieprasījums būtu uzskatāms par datu pārnesamības tiesību realizēšanu un attiecībā uz datiem, kuri ir pakļauti datu pārnesamības tiesībām, būtu jāizpilda saskaņā ar prasībām par datu pārnesamību.[29] Nepieciešamības gadījumā kredītiestādei jāprasa datu subjekta skaidrojums par pieprasījuma būtību un mērķi.

Datu subjektu identifikācija

Svarīgs aspekts šīs tiesības realizācijā ir datu subjekta pietiekama identificēšana, jo šajā gadījumā apjomīgas informācijas izsniegšana neīstajai personai var radīt būtiskas negatīvas sekas datu subjektam. Līdz ar to uzmanība ir jāpievērš pieprasījuma iesniedzēja identitātes noskaidrošanai, kā arī veidam, kādā šī informācija tiks nodota datu subjektam (klātienē, elektroniski vai pa pastu), nodrošinot atbilstošu saņēmēja identifikāciju un nododamo datu drošību.

Pietiekama varētu būt identifikācija elektroniskajā vidē ar kredītiestāžu izsniegtiem internetbanku autorizācijas līdzekļiem vai nosūtot informāciju, izmantojot VAS "Latvijas Pasts" ierakstītu pasta sūtījumu vai kurjera, zvērināta tiesu izpildītāja vai notāra pakalpojumu, tādā veidā saprātīgi nodrošinot, ka sūtījums tiks izsniegts konkrētai personai. Ja datus plānots nosūtīt elektroniskā pasta vēstulē, papildus identifikācijas aspektam, būtu jāpārliecinās par datu drošu nosūtīšanu, *piemēram, drošību nodrošinot ar šifrēšanas līdzekļiem*.

Attiecībā uz datu subjekta identifikāciju videonovērošanas ierakstos, saprātīga un nepieciešama būtu kredītiestādes prasība pieprasītājam papildus identificēt sevi konkrētajā videonovērošanas ierakstā, iesniedzot savu fotogrāfiju vai aprakstot savas pazīmes (apģērbu, izskatu u.c.), kā arī norādot laiku un konkrētu vietu, kurā datu subjekts bija atradies un videonovērošanas ierakstā iekļuvis. Ja datu subjekta sniegtā informācija nav pietiekama, lai to identificētu, pamatoti ir lūgt datu subjektam iesniegt papildu informāciju, lai to būtu iespējams pārliecinoši identificēt. Papildus, vērtējot videoierakstu izsniegšanu, būtu izvērtējams vai videoierakstā nav identificējamas trešās personas, šādā gadījumā būtu jānodrošina šo trešo personu privātuma aizsardzība to attēlus aizklājot vai, ja tas nav iespējams, izvērtēt iespēju datu subjektam rakstiski izklāstīt apstākļus kādos viņš ir fiksēts videoierakstā.

Attiecībā uz datu subjekta identifikāciju balss (audio) ierakstos, datu subjektam, pieprasot informāciju par sevi, būtu jānorāda iespējamais zvanīšanas laiks, kā arī tālruņa numurs (ja informācijas atlase ir veicama pēc tālruņa numura). Izvērtējot šāda balss (audio) ieraksta izsniegšanu, kredītiestādei būtu jāizvērtē arī aspekts, ka balss (audio) ierakstā tiek fiksēti arī darbinieka, kurš sarunājas ar datu subjektu, dati. Līdz ar to papildus būtu lietderīgi noskaidrot balss (audio) ieraksta pieprasīšanas mērķi, un atkarībā no tā izvērtēt, vai balss (audio) ieraksta sadaļas, kurā fiksēts darbinieka teiktais, ir izsniedzams vai aizstājams ar rakstisku atšifrējumu par sarunas būtību, kā arī izvērtēt vai mērķa sasniegšanai ir nepieciešams identificēt kredītiestādes darbinieku, kurš ir balss (audio) ierakstā ir sarunājies ar datu subjektu.

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 59., 61., 63., 64. un 73. apsvērumā un Regulas 12. un 15. pantā.

[29] Sk.: Ieteikumu 5.4. nodaļu "Tiesības uz datu pārnesamību"

5.3. Tiesības labot datus

Tiesības labot datus būtība

Datu subjektam ir tiesības uz savu datu labošanu. Labošanas pieprasījumam ir jābūt argumentētam, ko kredītiestādei jāizvērtē, saņemot pieprasījumu. Ja kredītiestādei rodas šaubas par pieprasījuma pamatotību, kredītiestādei ir tiesības lūgt datu subjektam iesniegt papildu pierādījumus par datu labošanu. Tomēr papildu pierādījumus nebūtu adekvāti lūgt par tādu datu labošanu, kas ir pilnībā atkarīgi no datu subjekta ieskata, *piemēram, klienta dzīvesvieta, klienta e-pasta adrese, klienta tālruņa numurs*.

Kredītiestādei nav pienākuma labot tā sauktos subjektīvos datus, t.i., kredītiestādes radītos datus vai viedokli par datu subjektu, *piemēram, ka datu subjekts ir iekļauts noteiktā riska kategorijā*, pamatojoties uz kredītiestādes izvērtējumu, tomēr, ja datu subjekts iesniedz papildu informāciju, kas varētu ietekmēt kredītiestādes radītos subjektīvos datus, kredītiestādei šie dati būtu jāpārskata. Pārskatīšanas rezultātā kredītiestādei atkarībā no iesniegto papildu datu rakstura ir tiesības gan mainīt *subjektīvos datus*, gan saglabāt tos nemainīgus. Līdzīga situācija var būt sastopama attiecībā uz darbinieka subjektīvo vērtējumu, ko sniedzis darbinieka vadītājs, kura labošana ir darbinieka vadītāja vai darba devēja kompetencē.

Datu labošanu var prasīt tikai attiecībā uz faktiem, ko sniedzis datu subjekts vai ko kredītiestāde likumīgi pati ieguvusi, *piemēram, vārdi, nosaukumi, finanšu rādītāji, amati*. Attiecībā uz subjektīvu vērtējumu datu subjekts var tikai lūgt labot faktu par šāda vērtējuma esamību, nevis paša vērtējuma saturu.

Gadījumos, kad robeža starp objektīvajiem un subjektīvajiem datiem ir grūti nošķirama (*piemēram, attiecībā uz kāda izdarīta pārkāpuma konstatēšanu, kas ietver gan objektīvu informāciju (noteiktas pārkāpuma izdarīšanas darbības), gan subjektīvu informāciju (šīs darbības novērtējumu*), datu subjektam vienmēr ir jādod iespēja vismaz papildināt datus ar citu informāciju.

Var rasties praktiskas situācijas, kad tiesības labot datus tiek īstenotas reizē ar tiesībām ierobežot apstrādi (saistībā ar datu precizitāti). Ņemot vērā, ka šīs tiesības ir savstarpēji saistītas, ir iespējams arī paredzēt atbilstošu datu subjekta pieprasījumu procedūru, ievērojot iespēju abu tiesību vienlaicīgai realizācijai.

Vai ir jālabo informācijas avoti?

Tiesības labot datus nebūtu jāsaprot kā tiesības labot dokumentus, bet gan kā datu subjekta tiesības norādīt, lai attiecībā uz datu subjektu, radot tam jebkādas tiesiskas sekas, tiktu izmantota labotā informācija.

Piemēram, ja klients ir norādījis papīra dokumenta formā aizpildītā klienta anketā, ka tā kontakttālrunis ir attiecīgs tālruņa numurs, tad, izmantojot tiesības labot datus, ja klientam ir mainījies tālruņa numurs, kredītiestādei nav jālabo dati dokumentā (jo tas var ietekmēt dokumentu juridisko spēku), bet gan jānodrošina, ka turpmākā saziņā ar klientu tiks izmantots jaunais tālruņa numurs (piemēram, izdarot attiecīgas izmaiņas klientu pārvaldības datu bāzē).

Līdz ar to var secināt, ka labojums jāveic tajā brīdī, kad ir konstatēta datu neprecizitāte, un laboto datu sekas attieksies tikai uz turpmāko datu apstrādi un pieņemtiem lēmumiem. Savukārt atsevišķi vērtējami konkrēti gadījumi, kad kredītiestāde, izmantojot neprecīzus datus, ir pieņēmusi nepareizu lēmumu, kurš attiecīgi būtu jāpārskata, ievērojot normatīvajos aktos noteiktās prasības.

Datu labošana automatizētās sistēmās

Ņemot vērā, ka datu subjekta tiesības prasīt datu labošanu attiecas arī uz datu apstrādes sistēmām, šādām sistēmām būtu jānodrošina funkcionalitāte individuālu datu kopu labošanai tādā veidā, kas neietekmētu visas sistēmas darbību (sistēmas darbības kļūdas vai sistēmas darbības apturēšana, informācijas labošanas dēļ).

Papildus tam Regula paredz iespēju datu subjektam papildināt savus datus ar papildu informāciju. Tādējādi sistēmu funkcionalitātei ir jānodrošina arī iespēja papildināt jau sistēmā ietverto informāciju.

Ja datu subjekts vēlas labot datus, kas ir radīti kredītiestādē (tā saucamie "subjektīvie" dati), piemēram, personas kredītreitings, tad labošanas tiesība pamatā attiecas uz ievadītajiem datiem (dati, kuri ir par pamatu automatizētai apstrādei un lēmuma pieņemšanai), bet, labojot šos datus, datu subjektam būtu tiesības lūgt arī pārskatīt uz šo datu izvērtēšanas pamata kredītiestādes radīto papildu informāciju.

Ja persona tiek ietverta noteiktā kategorijā, kas atspoguļo noteiktus faktorus vai spējas (*piemēram, kredītspējas vai riskus*), un šis novērtējums ir balstīts uz nepareiziem faktiem (sākotnēji ievadīto informāciju), personai ir tiesības prasīt labot datus, uz kuriem balstīts minētais vērtējums (sākotnēji ievadīto informāciju), kā arī pārskatīt par personu izdarīto vērtējumu.

Tādējādi automatizētām sistēmām jābūt funkcionalitātei veikt atkārtotu apstrādi, ņemot vērā labotos datus.

Pārziņa pienākumi

Nodrošināt datu precizitāti ir viens no kredītiestādes kā pārziņa pamatpienākumiem, jo neprecīzi dati var radīt datu subjektam negatīvas sekas (*piemēram, kļūdaini ievietojot informāciju parādnieku sarakstā un tādējādi personai pazeminot kredītspējas rādītājus, vai kļūdaini informējot izmeklēšanas iestādes par klienta līdzdalību neparastos un aizdomīgos darījumos*), līdz ar to kredītiestādei ir jāveic dažādi organizatoriski pasākumi, lai nodrošinātu datu precizitāti un to regulāru atjaunošanu, *piemēram, līgumos iekļaujot klienta pienākumu nekavējoties ziņot par izmaiņām būtiskā informācijā, klātienē apkalpojot klientu, pārliecināties par pamatdatu atbilstību aktuālajiem, vai internetbankā ar noteiktu regularitāti pieprasot klientam pārbaudīt datu aktualitāti*.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Pieprasījumu izpildes termiņi

Kredītiestāde izskata pieprasījumu un, ja nepieciešams, labo datus bez nepamatotas kavēšanās un jebkurā gadījumā mēneša laikā no pieprasījuma saņemšanas informē datu subjektu par veiktajām darbībām. Laika posmu pieprasījuma izpildei, ņemot vērā pieprasījumu sarežģītību un skaitu, var pagarināt vēl uz diviem mēnešiem. Par termiņa pagarināšanu datu subjekts jāinformē mēneša laikā no pieprasījuma saņemšanas.

Vai ir jāinformē citi datu saņēmēji?

Kredītiestādei ir jāidentificē datu saņēmēji, kuriem labotie dati pirms to labošanas ir izpausti un, ja tas neprasa nesamērīgas pūles (piemēram, grūtības sameklēt informāciju par datu saņēmējiem, kas padara šādu identificēšanu tehniski sarežģītu vai dārgu attiecībā pret ieguvumu, ko datu subjekts gūst no šāda pieprasījuma), tie ir jāinformē par personas pieprasījuma izpildi. Kredītiestādei būtu jāpieliek saprātīgas pūles (piemēram, jāizmanto standarta, nozarē apstiprinātas pieejas mērķa sasniegšanai, neveicot visus kredītiestādei pieejamos pasākumus), lai pārbaudītu, vai apstrādātāji ir atbilstoši īstenojuši datu labošanas pieprasījumu un turpmāk apstrādā labotos datus.

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 73. apsvērumā un Regulas 12. un 16. pantā.

5.4. Tiesības uz datu pārnesamību

Tiesības uz datu pārnesamību būtība

Datu subjektam ir tiesības saņemt datus par sevi, lai tos saglabātu vai lai radītu iespēju datu atkārtotai izmantošanai, piemēram, nododot citam pakalpojumu sniedzējam. Šī tiesība apstrādājamo datu apjoma ziņā ir atšķirīga no tiesībām piekļūt saviem datiem, kur dati, kuriem datu subjekts var piekļūt, ir daudz lielākā apjomā.

Uz kādiem datiem attiecas pārnesamības tiesības?

Datu pārnesamības tiesības nav absolūtas un attiecas tikai uz noteiktu datu loku. Datiem jāatbilst šādām pazīmēm (obligātās), lai uz tiem varētu attiecināt pārnesamības tiesības:

1. **dati attiecas uz konkrēto datu subjektu, kurš izdarījis pieteikumu**:

   a) tai skaitā attiecas arī uz pseidonimizētiem datiem (tomēr neattiecas uz anonīmiem datiem, jo tos nav iespējams sasaistīt ar konkrētu personu);

   b) vērtējot izsniedzamo datu apjomu, jāņem vērā, lai datu nodošana nelabvēlīgi neietekmē citu personu tiesības uz datu aizsardzību;

2. **datus kredītiestādei ir iesniedzis pats datu subjekts:**

   a) tie ir ne tikai dati, ko datu subjekts ir iesniedzis, piemēram, izmantojot tiešsaistes pieteikuma formas, bet arī dati, kas radušies novērojot datu subjektu aktivitātes (piemēram, interneta vietņu izmantošanas vēsture, atrašanās vietas dati, dati no "gudrajām ierīcēm");

   b) tie nav dati, kurus ir radījusi pati kredītiestāde (piemēram, kredītiestādes radīts klienta kredītriska vērtējums vai klienta iedalīšana kādā no klientu grupām – profesionāls/neprofesionāls klients – būs uzskatāmi par kredītiestādes radītiem datiem un uz tiem neattieksies datu pārnesamības tiesība);

3. **attiecas uz tiem datiem, kuru apstrādes tiesiskais pamats ir datu subjekta piekrišana vai tā apstrāde pamatota ar nepieciešamību datus apstrādāt līguma izpildei (t.sk. sagatavot līgumu), kura puse ir datu subjekts;**

   a) pārnesamība būtu attiecināma uz informāciju par klienta veiktajām transakcijām kontā, klienta aizpildītiem elektroniskiem pieteikumiem dažādiem produktiem (piemēram, kredītriska produktiem);

   b) pārnesamība nebūtu attiecināma uz informāciju, kas apkopota, lai izpildītu NILLTPFNL prasības vai uz informāciju, kuru kredītiestāde ir patstāvīgi ievākusi, lai izvērtētu klienta kredītspēju;

4. **šādas informācijas apstrāde tiek veikta ar automatizētiem līdzekļiem**, proti, kredītiestādei nebūtu jānodrošina pārnesamība attiecībā uz papīra dokumentos fiksētu informāciju.

Tādējādi kredītiestādes sistēmās būtu jāizstrādā iespēja attiecīgās datu kategorijas iezīmēt vai atsevišķi atlasīt, lai datu subjekta pieprasījuma gadījumā būtu iespējams efektīvā veidā atlasīt un eksportēt datu subjekta informāciju, kas pakļauta pārnesamības tiesību realizācijai.

Būtu ieteicams izveidot risinājumu, kas ļauj datu subjektam nodrošināt pārnesamību uz atsevišķām informācijas daļām, ne tikai uz visu informāciju kopumā, tādējādi ļaujot datu subjektam izvēlēties atbilstošu pārnesamo informācijas apjomu.

29. panta darba grupa savā atzinumā[30] ir norādījusi, ka datu pārnesamībai pakļautā informācija var saturēt arī trešo personu datus, bet tas pats par sevi nav šķērslis pārnesamības nodrošināšanai, tomēr būtu izvērtējama šādu datu nodošanas ietekme uz trešās personas tiesībām un brīvībām. Ja paredzama nelabvēlīga ietekme, tad jārealizē pasākumi, lai pēc iespējas novērstu šādu nelabvēlīgu seku rašanos.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Vai sagatavojot datus pārnešanai ir jāpārbauda datu precizitāte?

Pārnešanas tiesību realizācija attiecas uz tādu informāciju, kāda ir kredītiestādes rīcībā, atsevišķa pienākuma datus pārbaudīt pirms nosūtīšanas kredītiestādei nav.

Vai pārsūtot datus pārsūtītie dati ir jādzēš?

Datu pārsūtīšana nenozīmē, ka zūd tiesības apstrādāt datus uz iepriekšējiem tiesiskiem pamatiem un iepriekš nodefinētiem nolūkiem, līdz ar to datu pārsūtīšana nenozīmē, ka pārsūtītie dati būtu dzēšami šī iemesla dēļ.

Datu pārsūtīšanas formāts

Dati ir jāiekļauj strukturētā, plaši izmantotā un mašīnlasāmā formātā (ļaujot programmām viegli identificēt, atšķirt un iegūt datus, kā arī atpazīt datu iekšēju struktūru), kas ir piemērots atkārtotai izmantošanai. Regula nenosaka konkrētu datu formātu un struktūru un pieļauj, ka katrai nozarei tās apstrādājamo datu veids un struktūra būs atšķirīgi, līdz ar to vienotas pieejas izveidošana var būt viena no nozares iniciatīvām.

Kā piemēri dažādu sistēmu savstarpēji izmantojamiem atvērtiem failu formātiem būtu [.xml un *.csv] formāti*[31]*. Kopā ar nodotajiem datiem būtu jānodod arī metadati, kas nepieciešami datu saņēmējam atkārtotai datu izmantošanai*.

Kam pārsūtāmi dati un kāds ir pārsūtīšanas veids?

Dati pēc datu subjekta izvēles ir nosūtāmi pašam datu subjektam (ņemot vērā identificēšanas nosacījumus, kas izklāstīti sadaļā par tiesībām piekļūt saviem datiem) vai arī tā norādītam pakalpojumu sniedzējam. Tomēr, pārsūtot datus tieši citam pakalpojumu sniedzējam, kredītiestādei nosūtīšana jāveic drošā veidā, par kādu puses vienojušās atsevišķi. Datu drošība ir jānodrošina gan attiecībā uz pārraides procesu (*piemēram, ar end-to-end šifrēšanu*), gan attiecībā uz saņēmēju (izmantojot stingrus identificēšanas un autentificēšanas līdzekļus).[32] Tomēr ar šiem pasākumiem nedrīkst pārlieku kavēt pārnesamības realizēšanu (*piemēram, nosakot maksu, izņemot turpmāk izklāstītos gadījumus*). Datu subjektam jāapzinās un kredītiestādei vēlams informēt, ka informācijas nodošanas rezultātā dati tiks nodoti trešajai personai, iespējams, izpaužot arī klienta noslēpumu.

Rekomendējams ir ieviest rīkus automātiskai datu lejupielādēšanai (kā tas tiek nodrošināts vairumā internetbanku sistēmās saistībā ar konta pārskatiem) vai iespējai datu subjektam pašam pārsūtīt datus tieši citam pakalpojumu sniedzējam, *piemēram, izmantojot iepriekšminētos internetbanku risinājumus*.

Ja dati tiek pārsūtīti datu subjektam, ieteicams datu subjektu informēt par datu uzglabāšanas drošību, jo ir liela iespēja, ka klienta rīcībā dati būs mazāk aizsargāti, salīdzinājumā ar kredītiestādes sistēmām.

[30] 2016. gada 13. decembra 29. panta darba grupas rekomendācijas "Pamatnostādnes par tiesībām uz datu pārnesamību" 11. lpp.
[31] Turpat, 17. lpp.
[32] Turpat, 16. lpp.

Pienākumi kredītiestādei, saņemot šādus datus

Ja kredītiestādei klients datu pārnesamības tiesību izmantošanas rezultātā nosūtīs datus, tai ir jānorāda minimāli nepieciešamais datu apjoms pakalpojuma nodrošināšanai. Ja kredītiestāde šādu tiesību ietvaros tomēr ir saņēmusi vairāk informācijas nekā tai būtu nepieciešams savu pakalpojumu nodrošināšanai, tai pārmērīgā informācija ir jādzēš vai, ja tas informācijas rakstura dēļ un sasaistes ar datu subjektu dēļ nav iespējams, tad šo informāciju nevajadzētu izmantot citiem nolūkiem, kā tikai klienta/datu subjekta norādītajam.

Pieprasījumu izpildes termiņi

Pārsūtīšanu kredītiestāde veic bez nepamatotas kavēšanās un jebkurā gadījumā mēneša laikā no pieprasījuma saņemšanas informē datu subjektu par veiktajām darbībām. Laika posmu pieprasījuma izpildei, ņemot vērā pieprasījumu sarežģītību un skaitu, var pagarināt vēl uz diviem mēnešiem. Par termiņa pagarināšanu datu subjekts jāinformē mēneša laikā no pieprasījuma saņemšanas.

Atbildība

Pārziņi, kuri ir izpildījuši datu pārnesamības pieprasījumu, nenes atbildību par tālāku apstrādi, ko veic pats datu subjekts vai cita persona, kura šos datus saņem.

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 68. un 73. apsvērumā un Regulas 12. un 20. pantā, kā arī 2016. gada 13. decembra 29. panta darba grupas rekomendācijās "Pamatnostādnes par tiesībām uz datu pārnesamību".

5.5. Tiesības uz dzēšanu (tiesības "tikt aizmirstam")

Tiesības uz dzēšanu jeb tiesības "tikt aizmirstam" būtība

Datu subjektam ir tiesības panākt, lai kredītiestāde bez nepamatotas kavēšanās dzēstu datu subjekta datus, un kredītiestādes pienākums ir bez nepamatotas kavēšanās dzēst datus, ja:

1. dati vairs nav nepieciešami vai izmantojami saistībā ar sākotnējiem nolūkiem, kādiem tie tika vākti vai citādi apstrādāti (*piemēram, datu subjekts var panākt datu dzēšanu, ja kredītiestāde datus ir vākusi loterijas organizēšanai, loterija noslēgusies un dati vairs nav izmantojami sākotnējam nolūkam*);

2. datu subjekts ir atsaucis savu piekrišanu, uz kuras pamata datu apstrāde tika veikta, un nav cita likumīga pamata apstrādei (*tomēr jāizvērtē, vai kredītiestādes leģitīmo interešu ietvaros nav nepieciešams noteiktu laiku glabāt pierādījumus, ka datu apstrāde piekrišanas spēkā esamības laikā bija likumīga*);

3. datu subjekts ir iebildis datu apstrādei un pēc leģitīmo interešu atkārtota izvērtējuma kredītiestāde atzīst, ka datu apstrādei nav tiesiskā pamata vai apstrāde notiek tirgvedības nolūkos (*piemēram, datu subjekts var panākt datu dzēšanu, ja kredītiestāde datus izmanto vienīgi reklāmas vai tirgvedības kampaņas nolūkos*);

4. dati ir apstrādāti nelikumīgi (piemēram, kredītiestāde, apstrādājot datus, nav ievērojusi Regulā noteiktās prasības attiecībā uz likumības principa ievērošanu);

5. dati ir jādzēš, jo to nosaka kredītiestādei piemērojamie tiesību akti;

6. dati ir savākti saistībā ar informācijas sabiedrības pakalpojumu piedāvāšanu bērnam uz piekrišanas pamata (*piemēram, datu subjekts var panākt datu dzēšanu, ja kredītiestāde datu subjekta datus ir vākusi laikā, kad datu subjekts ir bijis bērns, neskatoties uz datu subjekta vai personas, kurai ir vecāku atbildība pār bērnu, piekrišanu*).

Pieprasījumu izpildes termiņi

Kredītiestāde dzēš informāciju bez nepamatotas kavēšanās un jebkurā gadījumā mēneša laikā informē datu subjektu par veiktajām darbībām. Laika posmu pieprasījuma izpildei, ņemot vērā pieprasījumu sarežģītību un skaitu, var pagarināt vēl uz diviem mēnešiem.

Piemēri gadījumiem, kad var nedzēst datus

Datus var nedzēst, nevērtējot citus apstākļus, šādos gadījumos:

1. lai īstenotu tiesības uz vārda brīvību un tiesības uz informāciju;

2. lai izpildītu juridisku pienākumu, kas prasa veikt datu apstrādi (*piemēram, arī normatīvajos aktos noteiktos informācijas vai dokumentu glabāšanas termiņus, kas noteikti, piemēram, NLLTFNL, likumā "Par grāmatvedību", Kredītiestāžu likumā*);

3. lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot pārzinim piešķirtas oficiālas pilnvaras (*piemēram, ja kredītiestāde pierāda, ka plašākai sabiedrībai ir būtiski piekļūt konkrētajiem datiem ar nosacījumu, ka informācija nav nepietiekama, nebūtiska vai pārmērīga tās nolūkam*);

4. pamatojoties uz sabiedrības interesēm veselības jomā;

5. ja apstrāde ir nepieciešama arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēsturiskās pētniecības nolūkos, vai statistikas nolūkos, ciktāl minētās tiesības varētu neļaut vai būtiski traucēt sasniegt minētās apstrādes nolūkus.

Vai datu dzēšanu var aizstāt ar datu anonimizēšanu?

Ja kredītiestādē izveidotais informācijas sistēmu risinājums neatbalsta datu lauku vai personas profila pilnīgu dzēšanu un datu vai klienta profila izdzēšana var apdraudēt sistēmas funkcionēšanu, tad ir alternatīva iespēja datus anonimizēt, t.i., nodzēšot visus identifikatorus (datu laukus), pēc kuriem personu varētu atpazīt, padarot datus par anonīmiem. Pēc tiesiskām sekām anonimizēšanas process ir pielīdzināms datu dzēšanai.

Tāpat anonimizēšanas metodes izmantošanu var apsvērt gadījumos, kad statistiskiem rādījumiem ir nepieciešams saglabāt iepriekšējo klientu pakalpojumu izmantošanas paradumus, tādā veidā, ka, ja visi personas identifikatori ir dzēsti, personu nevar vairs uzskatīt par identificējamu un rezultātā palikušie dati nevarētu tikt uzskatīti par datiem. Tomēr, anonimizējot datus, rūpīgi ir jāizvēlas anonimizācijas metodes, lai kredītiestāde būtu pārliecināta, ka persona pēc atlikušās informācijas netiks atpazīta un identificēta, kā arī anonimizācijas procesa ievades dati ir neatgriezeniski zuduši. Plašāk par anonimizācijas metodēm, kā arī iespējām deanonimizēt datus, var lasīt 29. panta darba grupas 2014. gada 10. aprīļa "Atzinumā 05/2014 par anonimizācijas metodēm"[33].

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Vai ir jāinformē citi datu saņēmēji?

Kredītiestādei ir jāidentificē datu saņēmēji, kuriem dati ir izpausti un, ja tas neprasa nesamērīgas pūles (piemēram, grūtības sameklēt informāciju par datu saņēmējiem, kas padara šādu identificēšanu tehniski sarežģītu vai dārgu attiecībā pret ieguvumu, ko datu subjekts gūst no šāda pieprasījuma), tie ir jāinformē arī par personas pieprasījuma izpildi. Kredītiestādei būtu jāpieliek saprātīgas pūles (piemēram, jāizmanto standarta, nozarē apstiprinātas pieejas mērķa sasniegšanai, neveicot visus kredītiestādei pieejamos pasākumus), lai pārbaudītu, vai apstrādātāji ir atbilstoši īstenojuši datu dzēšanas pieprasījumu.

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 65., 66. un 73. apsvērumā un Regulas 12., 17. un 19. pantā.

[33] 29. panta darba grupas 2014. gada 10. aprīļa "Atzinumā 05/2014 par anonimizācijas metodēm". Pieejams: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_lv.pdf

5.6. Tiesības ierobežot apstrādi

Tiesības ierobežot apstrādi būtība

Datu subjektam ir tiesības pieprasīt, lai kredītiestāde ierobežotu apstrādi, t.i., kredītiestāde veiktu personas datu iezīmēšanu ar mērķi ierobežot to apstrādi nākotnē. Datu subjektam ir tiesības panākt, lai kredītiestāde ierobežotu apstrādi, ja pastāv kāds no tabulā uzskaitītajiem iemesliem.

Tabula Nr. 6

Datu apstrādes ierobežošanas iemesli

Iemesls	Ierobežojuma ilgums
1. datu subjekts apstrīd datu precizitāti	Uz laiku, kamēr kredītiestāde pārbauda datu precizitāti (izņemot gadījumus, kad kredītiestādei nepieciešams ievērot normatīvajos aktos noteiktos termiņus pienākumu izpildei)
2. apstrāde ir nelikumīga, un datu subjekts iebilst pret datu dzēšanu, tās vietā pieprasa datu izmantošanas ierobežošanu	Uz laiku, kādu datu subjekts ir pieprasījis, ja datu subjekta norādītais termiņš ir pamatots
3. kredītiestādei dati apstrādei vairs nav vajadzīgi, taču tie ir nepieciešami datu subjektam, lai celtu, īstenotu vai aizstāvētu likumīgās prasības	Uz laiku, kādu datu subjekts ir pieprasījis un pamatojis
4. datu subjekts ir iebildis pret apstrādi, kas pamatota ar kredītiestādes leģitīmajām interesēm (vai publisku uzdevumu veikšanu)	Uz laiku, kamēr tiek pārbaudīts, vai kredītiestādes leģitīmie iemesli ir svarīgāki par datu subjekta leģitīmajiem iemesliem

Jāņem vērā, ka vienlaicīgi ar datu apstrādes ierobežošanas pieprasījumu var tikt saņemti arī datu subjekta iebildumi apstrādei. Šādi pieprasījumi jāskata kopsakarā ar Ieteikumu 5.7. nodaļā aprakstītajām tiesībām iebilst pret datu apstrādi.

Ierobežošanas īstenošanas metodes

Ierobežot datu apstrādi var dažādos veidos: pārvietot attiecīgos datus uz citu apstrādes sistēmu, noteikt liegumu lietotājiem piekļūt attiecīgiem datiem sistēmā, publicēto/ nodoto datu pagaidu atsaukšanu/izņemšanu no publicētās vietas, ierobežoto datu atstatīšana no izmantošanas automatizētajās sistēmās, ierobežot iespējas tos izmainīt, kā arī izdarīt atzīmi sistēmā, ka šie dati ir ierobežoti, vai arī veikt citas nepieciešamās darbības.

No iepriekš minētā izriet, ka sistēmu funkcionalitātei ir jānodrošina iespēju iezīmēt atsevišķas konkrētā datu subjekta datu kategorijas, attiecībā uz kurām tiek ierobežota apstrāde, kas nodrošinātu minēto apstrādes ierobežošanas metožu īstenošanu. Turklāt automātiskās sistēmās jānodrošina, ka sistēmas darbība netiek traucēta saistībā ar apstrādes ierobežojumu. Problemātiska situācija varētu rasties, kad vieni un tie paši dati tiek izmantoti vairākiem nolūkiem, bet ierobežošana attiecas tikai uz vienu no nolūkiem. Kā risinājums šajā situācijā būtu noteikt datiem īpašu atzīmi, kas norādītu, kādiem nolūkiem datu apstrāde ir ierobežota.

Kādas ir tiesības apstrādāt datus, ja datu subjekts ierobežojis datu apstrādi?

Attiecīgi datus pēc ierobežojuma izteikšanas drīkst tikai glabāt, taču jebkāda datu apstrāde, izņemot glabāšanu, ir pieļaujama tikai ar datu subjekta piekrišanu vai tādēļ, lai celtu, īstenotu vai aizstāvētu leģitīmas intereses, vai lai aizsargātu citas fiziskas vai juridiskas personas tiesības, vai ES vai dalībvalsts svarīgu sabiedrības interešu dēļ.

Saskaņā ar Regulu kredītiestādei ir jāvērtē katrs gadījums atsevišķi, lai pēc ierobežojuma izteikšanas attiecīgi veiktu vai nu tikai datu glabāšanu, vai arī papildus glabāšanai veiktu arī cita veida datu apstrādi.

Pieprasījumu izpildes termiņi

Kredītiestāde ierobežo datu izmantošanu bez nepamatotas kavēšanās un jebkurā gadījumā mēneša laikā no pieprasījuma saņemšanas informē datu subjektu par veiktajām darbībām. Laika posmu pieprasījuma izpildei, ņemot vērā pieprasījumu sarežģītību un skaitu, var pagarināt vēl uz diviem mēnešiem. Par termiņa pagarināšanu datu subjekts jāinformē mēneša laikā no pieprasījuma saņemšanas.

Datu subjekta informēšana

Kredītiestādei pirms ierobežojumu atcelšanas par to ir jāinformē datu subjekts.

Citu personu informēšana

Tāpat Regula nosaka, ka par apstrādes ierobežojumu ir jāzina katram attiecīgo datu saņēmējam (gan ārējam, gan iekšējam), lai saņēmējam būtu informācija par šādu ierobežojumu un to būtu iespējams ievērot. Līdz ar to jānodrošina attiecīgo datu saņēmēju konstatēšana un uzskaite, kā arī attiecīgā gadījumā informēšana par attiecīgo datu apstrādes režīmu. Piemēram, ja apstrādes ierobežojums attiecas uz parāda informāciju, kas nodota kredītinformācijas birojam, kredītiestādei būtu jāinformē attiecīgais kredītinformācijas birojs, pretējā gadījumā trešās personas turpinās iegūt informāciju, kura tikusi ierobežota (*piemēram, dēļ strīda par datu precizitāti*) un pieņemt uz šādas potenciāli neprecīzas informācijas pamata lēmumus, kas ietekmē datu subjektu.

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 67. un 73. apsvērumā un Regulas 12., 18. un 19. pantā.

5.7. Tiesības iebilst

Tiesības iebilst būtība

Datu subjektam ir tiesības iebilst pret viņa datu apstrādi tabulā uzskaitītajos gadījumos.

Tabula Nr. 7

Tiesības iebilst pret datu apstrādi pamati un sekas

Pamats iebilšanas tiesību realizācijai	Sekas iebildumu izteikšanai
Apstrādei, kas pamatojas uz kredītiestādes leģitīmajām interesēm (Regulas 6. panta 1. punkta "e" apakšpunkts) vai sabiedrības interesēm un publisku uzdevumu veikšanu (Regulas 6. panta 1. punkta "f" apakšpunkts), tai skaitā profilēšanai, kas pamatojas uz iepriekš minētajiem tiesiskiem pamatiem	Saņemot personas pieprasījumu ar specifiskiem iemesliem saistībā ar subjekta īpašo situāciju kredītiestādei ir jāpārtrauc apstrādāt datus konkrētajiem nolūkiem, izņemot, ja kredītiestāde: 1) spēj norādīt uz pārliecinošiem apstrādes nolūkiem, kas ir par pamatu turpināt datu apstādi, neskatoties uz datu subjekta interesēm, tiesībām un brīvībām (tajā skaitā atkārtoti pārskatot interešu līdzsvarošanas rezultātu konkrētajai apstrādes darbībai); 2) izmanto datus, lai celtu, īstenotu vai aizstāvētu leģitīmas intereses Ja datu subjekts ir arī norādījis uz datu apstrādes ierobežojumu, tad līdz pieprasījuma izskatīšanai datu apstrāde ir jāpārtrauc līdz tiek konstatēts, vai kredītiestādei ir pamats turpināt apstrādi.
Apstrādei, kas nepieciešama tiešās tirgvedības vajadzībām, tai skaitā arī uz profilēšanu	Saņemot iebildumus par apstrādi, kredītiestādei ir jāpārtrauc apstrādāt datus konkrētajam nolūkam.
Apstrādei, kas tiek veikta zinātniskās vai vēstures pētniecības vai statistikas nolūkos	Saņemot iebildumus par apstrādi kredītiestādei ir jāpārtrauc apstrādāt datus konkrētajam nolūkam, izņemot, ja apstrāde ir vajadzīga, lai izpildītu uzdevumu sabiedrības interesēs.

Tiesības iebilst datu subjekts nevar realizēt, ja datu apstrādes pamats ir:

1) piekrišana
2) līgumisku attiecību nodibināšana un izpilde
3) juridiska pienākuma izpilde
4) datu subjekta vai trešo personu vitāli svarīgu interešu aizsardzība.

Pieprasījumu izpildes termiņi

Kredītiestāde izskata pieprasījumu un pārtrauc datu apstrādi bez nepamatotas kavēšanās un jebkurā gadījumā mēneša laikā informē datu subjektu par veiktajām darbībām. Laika posmu pieprasījuma izpildei, ņemot vērā pieprasījumu sarežģītību un skaitu, var pagarināt vēl uz diviem mēnešiem. Par termiņa pagarināšanu datu subjekts jāinformē mēneša laikā no pieprasījuma saņemšanas.

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 69., 70., 71. un 73. apsvērumā un Regulas 12. un 21. pantā.

5.8. Tiesības attiecībā uz automatizētu individuālo lēmumu pieņemšanu

Automatizēts individuāls lēmums

Automatizēts individuāls lēmums ir lēmums, kura pamatā ir tikai automatizēta apstrāde, kas attiecībā uz datu subjektu rada tiesiskās sekas vai kas līdzīgā veidā ievērojami ietekmē datu subjektu. Automatizēta individuālo lēmumu pieņemšana var notikt gan iesaistot, gan neiesaistot profilēšanu.

Profilēšana

Profilēšana ir jebkura veida automatizēta personas datu apstrāde, kas izpaužas kā personas datu izmantošana nolūkā izvērtēt konkrētus ar fizisku personu saistītus personiskus aspektus, jo īpaši analizēt vai prognozēt aspektus saistībā ar minētās fiziskās personas sniegumu darbā, finanšu stāvokli, veselību, personīgām vēlmēm, interesēm, uzticamību, uzvedību, atrašanās vietu vai pārvietošanos.

No Regulas izriet, ka profilēšana ir automatizēts datu apstrādes veids, ar kuru iespējams analizēt rīcībā esošus datus, veikt uzvedības novērošanu un izdarīt prognozes saistībā ar datu subjektu.

Piemēram, profilēšana kredītiestādēs tiek veikta procesos, kas ir nepieciešami aizdevuma piešķiršanai un kreditēšanas nosacījumu noteikšanai, patēriņa kredīta piešķiršanai, kā arī aizdomīgu darījumu identificēšanas procesos.

Var izdalīt trīs galvenos veidus, kā profilēšana var tikt izmantota:

1) vispārīga profilēšana, kuras rezultātā netiek pieņemti individuāli lēmumi;
2) profilēšana, kuras rezultātā tiek pieņemts individuāls lēmums, piedaloties cilvēkam;
3) automatizēta individuāla lēmuma pieņemšana, kas ietver profilēšanu.

Profilēšanas rezultātā var tikt pieņemts lēmums, pamatojoties uz automatizētu apstrādi, savukārt "c" gadījumā lēmumu pieņem algoritms un cilvēka dalība ir nenozīmīga.

Datu subjekta tiesības, kas paredzētas Regulas 22. pantā attiecas tikai uz automatizētu individuālu lēmumu (tostarp profilēšanu), kura pieņemšanas procesā cilvēks nepiedalās vai tā iesaiste ir nenozīmīga un, kas attiecībā uz datu subjektu rada tiesiskās sekas vai līdzīgā veidā ietekmē datu subjektu.

Automatizētu lēmumu pieņemšanas būtiskums

Automatizētu lēmumu pieņemšana, tostarp profilēšana, var radīt datu subjektam ievērojamas tiesiskās sekas (tai skaitā arī negatīvas) vai līdzīgā veidā ievērojami ietekmēt datu subjektu (*piemēram, tiešsaistē iesniegta kredīta pieteikuma automātisks noraidījums vai tiešsaistē iesniegta kredīta pieteikuma nenoraidīšana, bet augstākas procentu likmes piešķiršana (likuma noteiktajās robežās*)). Līdz ar to datu subjektam ir jābūt informētam par to, ka iegūtie dati tiks izmantoti automatizētu individuālo lēmumu pieņemšanai (tostarp profilēšanai) un būtu jāspēj kontrolēt šādu lēmumu pieņemšana attiecībā uz to.

Lai gan noteiktos gadījumos arī individualizēts mārketings (kas parasti balstās uz profilēšanu) var būt ar ievērojamām sekām, tomēr vairumā gadījumu, kad šāda individualizēta mārketinga pieeja tiek attiecināta uz ļoti plašu kategoriju (*piemēram, klienti, kuriem bankā ir atvērts konts, bet nav nevienas maksājumu vai kredītkartes*), tad būtu uzskatāms, ka šāda profilēšana nerada ievērojamas sekas datu subjektam.

Regula paredz datu subjektam tiesības saņemt jēgpilnu pārskatu/informāciju par paredzēto apstrādi un apstrādē ietverto loģiku (tādā apmērā, ciktāl tas neskar kredītiestādes būtiskas intereses, *piemēram, komercnoslēpuma izpaušana vai intelektuālā īpašuma aizskārumi vai rada citus būtiskus riskus kredītiestādes interesēm*), ja tiek veikta automatizētu lēmumu pieņemšana (tostarp profilēšana). Ir jāveic atbilstoši pasākumi, lai kodolīgā, pārredzamā, saprotamā un viegli pieejamā veidā, izmantojot skaidru un vienkāršu valodu, datu subjektam sniegtu minēto informāciju un nodrošinātu saziņu attiecībā uz apstrādi. Informāciju sniedz rakstiski vai citā veidā (arī elektroniskā formā).

Kā piemēru profilēšanai varētu minēt klienta iekļaušanu klientu lokā atbilstoši kredītiestādes izvēlētajai mārketinga stratēģijai, kas balstās uz klientu sadalīšanu pa vecuma grupām (lai, piemēram, nepiedāvātu kredītus klientiem zem 18 gadu vecuma vai piedāvātu speciāli izstrādātus produktus jauniešu grupai līdz 25 gadu vecumam vai studentiem), kurām tiek piedāvāti speciāli veidoti ("custom made") kredītiestādes produkti vai pakalpojumi.

Tiesības atteikties

Datu subjektam ir tiesības nebūt automatizēta individuāla lēmuma, tostarp profilēšanas, subjektam, ja izpildās šādi kritēriji:

1) lēmuma pamatā ir tikai automatizēta apstrāde, tostarp profilēšana, un
2) lēmums attiecībā uz datu subjektu rada tiesiskās sekas vai līdzīgā veidā ietekmē datu subjektu.

Datu subjektam ir tiesības prasīt cilvēka iesaisti automatizēta lēmuma pieņemšanā, ja tas rada tiesiskās sekas vai līdzīgā veidā ietekmē datu subjektu, lai datu subjekts varētu paust savu viedokli un apstrīdēt lēmumu. Attiecīgajai personai jābūt ar spēju un autoritāti pārskatīt automatizēto lēmumu. Lai tiktu uzskatīts, ka cilvēks ir bijis iesaistīts lēmuma pieņemšanā, ir jānodrošina nozīmīga lēmuma pārskatīšana, kuru veic kompetents un pilnvarots cilvēks, ņemot vērā visus pieejamos datus lēmuma pieņemšanai. *Kā piemēru var minēt automatizēta procesa izstrādātu rekomendāciju lēmumam, kurš attiecas uz datu subjektu. Ja cilvēks šo lēmumu pārskata un ņem vērā citus iemeslus galējā lēmuma pieņemšanā, cilvēks tiek uzskatīts par iesaistītu lēmuma pieņemšanā*.

Tikšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR Darba grupu 2018.gada 21.maijā Datu valsts inspekcija pauda viedokli, ka datu subjekta kredītspējas vērtēšanai automatizētā veidā, kā rezultātā attiecībā uz datu subjektu tiek pieņemts automatizēts individuāls lēmums, ir attiecināms Regulas 22.panta 3.punkta regulējums – t.i. kredītiestādei būtu jānodrošina datu subjektam tiesības apstrīdēt pieņemto lēmumu un lūgt to pārskatīt, nodrošinot kredītiestādes darbinieka līdzdalību lēmuma pieņemšanā.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Izņēmumi

Datu subjektam nav tiesību atteikties no automatizētu individuālo lēmumu pieņemšanas, ja lēmums:

1. ir vajadzīgs, lai noslēgtu vai izpildītu līgumu starp datu subjektu un kredītiestādi (piemēram, maksājumu automatizēta kontrole, maksājumu uzdevumā norādītās informācijas automātiska pārbaude un lūgums pārskatīt maksājuma uzdevumu neatbilstošas informācijas gadījumā), un šajos gadījumos kredītiestādei ir jānodrošina cilvēka līdzdalība lēmuma pieņemšanā, lai datu subjekts varētu paust savu viedokli un apstrīdēt lēmumu;

2. ir atļauts saskaņā ar ES vai Latvijas tiesību aktiem, kuri ir piemērojami kredītiestādei un kuros ir arī noteikti atbilstīgi pasākumi, ar ko aizsargā datu subjekta tiesības un brīvības un leģitīmās intereses (piemēram, klientu izpēte un aizdomīgu un neparastu darījumu atklāšanas sistēmu uzturēšana NILLTPFNL prasību izpildē);

3. pamatojas uz datu subjekta nepārprotamu piekrišanu, un šajos gadījumos kredītiestādei ir jānodrošina cilvēka līdzdalība lēmuma pieņemšanā, lai datu subjekts varētu paust savu viedokli un apstrīdēt lēmumu.

Pieprasījumu izpildes termiņi

Kredītiestāde izskata pieprasījumu bez nepamatotas kavēšanās un jebkurā gadījumā mēneša laikā informē datu subjektu par veiktajām darbībām. Laika posmu, ņemot vērā pieprasījumu sarežģītību un skaitu, var pagarināt vēl uz diviem mēnešiem.

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 60., 71., 72. un 73. apsvērumā un Regulas 12. un 22. pantā, kā arī 29. panta darba grupas 2017. gada 3. oktobra "Pamatnostādnēs par automatizētu individuālu lēmumu pieņemšanu un profilēšanu regulas 2016/679 nolūkiem"[34]

(Ar grozījumiem, kas izdarīti 08.01.2021.)

[34] 29. panta darba grupas 2017. gada 3. oktobra "Pamatnostādnēs par automatizētu individuālu lēmumu pieņemšanu un profilēšanu regulas 2016/679 nolūkiem". Pieejams: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

6. TEHNISKIE UN ORGANIZATORISKIE PASĀKUMI ATBILSTĪBAS NODROŠINĀŠANĀ

6.1. Iekšējo normatīvo aktu pamatprasības

Lai gan Regula neparedz konkrētu dokumentu nepieciešamību, izņemot datu apstrādes reģistru, tomēr pārskatatbildības, caurredzamības labas pārvaldības principu ietvaros būtu ieteicams personas datu apstrādes procesus dokumentēt, lai uzskatāmi nodrošinātu kredītiestādes darbības atbilstību Regulai.

Personas datu aizsardzības procesi un prasības saskaņā ar Regulu var tikt iekļautas gan esošajos iekšējos dokumentos, tos papildinot, gan var tikt izveidoti atsevišķi jauni dokumenti, kas fokusējas uz konkrēto datu aizsardzības aspektu.

Pārskatatbildības kontekstā visuzskatāmāk demonstrēt personas datu aizsardzības prasību ievērošanu būtu ar atsevišķas personas datu aizsardzības politikas dokumenta izstrādi, kas aptvertu datu aizsardzības vispārējos principus, atbildīgos par politikas īstenošanu specificētus procesus attiecībā uz personas datu apstrādi, atsaucoties uz citiem iekšējiem normatīvajiem aktiem.

Piemēram, personas datu aizsardzības politika nosaka vispārējo principu, ka personas dati ir ievācami tikai tādā apjomā, kas nepieciešams, lai sasniegtu noteikto nolūku, bet tiek ietverta atsauce uz noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanas politiku, kurā noteikts ievācamais personas datu apjoms, kā arī paredzēti kritēriji, pēc kuriem iespējams noteikt, vai ievāktā informācija ir pietiekama attiecīgo noziedzīgi iegūtu legalizācijas un terorisma finansēšanas novēršanas prasību izpildei.

Būtu izvērtējama iekšējo procedūru izstrāde papildus jau esošajām procedūrām, kuras radītas, nodrošinot atbilstību Finanšu un kapitāla tirgus komisijas 2015. gada 7. jūlija normatīvajos noteikumos Nr. 112 “Finanšu un kapitāla tirgus dalībnieku informācijas sistēmu drošības normatīvie noteikumi” attiecībā uz šādām personas datu aizsardzības jomām vai aspektiem:

1) personas datu aizsardzības politika;

2) klientu personas datu apstrāde:
- privātuma politika;
- privātuma paziņojumi un klauzulas, piekrišanas;
- datu izmantošana marketinga nolūkiem;
- sīkdatņu un tiešsaistes aktivitāšu uzraudzība;

3) cilvēkresursu vadība un drošība:
- darbinieku un pretendentu datu apstrāde un informēšana;
- darbinieku ierīču, interneta un citu veidu uzraudzība, piekļuve darbinieku failiem un komunikācijai (var tikt integrēta iekšējās drošības politikā);
- videonovērošana;
- trauksmes cēlāju shēmas darbība;
- personāla apmācība;

4) piegādātāju un sadarbības partneru personas datu apstrāde ;

5) datu subjektu pieprasījumu izskatīšana un izpilde;

6) citu personu iesaiste datu apstrādē:
- datu nodošana citiem pārziņiem [t.sk. koppārziņu attiecību regulējums (piemēram, atbildība)];
- apstrādātāju piekļuve datiem (piemēram, prasības apstrādātāju līgumiem, kontroles procesi, mākoņdatošanas politika) – var tikt integrēts ārpakalpojumu politikā;
- datu nodošana ārpus ES vai starptautiskām organizācijām;
- datu iegūšana no trešajām personām (piemēram, ārējas datubāzes);

7) pārskatatbildības nodrošināšana:
- datu apstrādes reģistra vešana;
- datu aizsardzības speciālista darbība;
- novērtējuma par ietekmi uz datu aizsardzību kārtība;
- leģitīmu interešu izvērtējuma kārtība;

8) tehniskās un organizatoriskās prasības (var tikt integrētas informācijas drošības politikā):
- anonimizācijas un pseidonimizācijas procedūra;
- datu šifrēšana un piekļuves ierobežošana;
- datu aizsardzības pārkāpumu novēršanas plāns;

9) personas datu uzglabāšanas, arhivēšanas un iznīcināšanas kārtība (var tikt integrēta lietvedības procedūrā);

10) datu apstrādes speciālista amata apraksts;

11) datu aizsardzības pārkāpumi:
- reaģēšana un ziņošana par datu aizsardzības pārkāpumiem;
- datu aizsardzības pārkāpumu reģistrs;
- datu aizsardzības pārkāpuma paziņojuma veidlapa uzraudzības iestādei;
- datu aizsardzības pārkāpuma paziņojuma veidlapa datu subjektiem.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 74. apsvērumā un Regulas 24., 29. un 32. pantā.

6.2. Apstrādes darbību reģistra vešana

Vai kredītiestādei jāizveido apstrādes darbību reģistrs?

Kredītiestādei būtu jābūt vismaz kā pārziņa veikto apstrādes darbību reģistram. Personas datu apstrādes darbību reģistra vešana ir rekomendējams līdzeklis pārskatatbildības principa īstenošanai. Apstrādes darbību reģistrs var nebūt gadījumos, ja kredītiestāde nodarbina mazāk par 250 darbiniekiem un tās veiktā apstrāde nevarētu radīt risku datu subjektu tiesībām un brīvībām, apstrāde ir neregulāra un apstrāde neietver Īpašu kategoriju datus vai personas datus par sodāmību un pārkāpumiem. Praktiski, kredītiestādēm tikai retos gadījumos varētu būt iespējams neuzturēt apstrādes darbību reģistru.

Apstrādes darbību reģistrā būtu jāiekļauj arī kredītiestādes filiālēs veikto apstrādes darbību apraksts. Reģistrs ir jākārto pēc iespējas pārskatāmākā veidā, lai tas būtu saprotams ne tikai personām, kuras kārto attiecīgo reģistru, bet arī citām personām, kurām nepieciešams piekļūt apstrādes darbību reģistram, *piemēram, lai izskaidrotu datu apstrādes procesus un nolūkus datu subjektam*.

Ja kredītiestāde darbojas arī kā datu apstrādātājs citu pārziņu uzdevumā, kredītiestādei ir jāuztur arī kredītiestādes kā apstrādātāja veikto datu apstrādes darbību kategoriju reģistrs.

Datu apstrādes reģistra vešana uzticama personai, kurai ir pieejama informācija par visām apstrādes darbībām kredītiestādē, kā arī jānodrošina informācijas apmaiņa par jebkurām izmaiņām apstrādes darbībās, lai tās attiecīgi varētu atspoguļot aktuālā datu apstrādes reģistra versijā.

Datu apstrādes reģistra vešanas procesā var iesaistīt datu aizsardzības speciālistu tā funkciju robežās (*piemēram, lai izvērtētu, vai ir atbilstoši definēts datu apstrādes nolūks*).

Tabula Nr. 8

Kāda informācija iekļaujama reģistros?

Reģistrā iekļaujamā informācija	Kredītiestādes kā pārziņa darbību reģistrs	Kredītiestādes kā apstrādātāja darbību kategoriju reģistrs
Kredītiestādes (arī koppārziņu[35]) nosaukums un kontaktinformācija (adrese, tālrunis, e-pasts).	✓	
Apstrādāja nosaukums un kontaktinformācija (adrese, tālrunis, e-pasts).		✓
Pārziņ**a (tā pārstāvja), kura vārdā kredītiestāde kā apstrādātājs darbojas, nosaukums** (vārds, uzvārds) **un kontaktinformācija** (adrese, tālrunis, e-pasts).		✓
Datu aizsardzības speciālista vārds, uzvārds un kontaktinformācija (*piemēram, pēc kredītiestādes izvēles adrese, kur datu aizsardzības speciālists sasniedzams, vai e-pasts, kurš nodrošina saziņu ar datu aizsardzības speciālistu*).	✓	✓
Apstrādes nolūki (*piemēram, pakalpojumu sniegšana klientiem, patiesā labuma guvēja noskaidrošana, darījumu uzraudzība NILLTPFNL nolūku izpildei, pieteicēja kredītspējas pārraudzībai*)	✓	
Datu kategoriju apraksts (*piemēram, identifikācijas dati, finanšu dati u.tml.*)	✓	✓
Datu subjektu kategoriju apraksts (*piemēram, klienti, patiesā labuma guvēji, darbinieki, personas, kas iekļūst videonovērošanas zonā, maksājumu saņēmēji, apmeklētāji*).	✓	
Katra pārziņa vārdā veiktās apstrādes kategorijas		✓
Datu saņēmēju kategorijas, kuriem dati ir izpausti vai tos ir paredzēts izpaust (*piemēram, tiesa, pakalpojumu sniedzēji, valsts iestādes*).	✓	
Informācija par datu nosūtīšanu uz trešo valsti vai starptautisku organizāciju, šo valstu un organizāciju identifikāciju, garantiju dokumentācija (ja dati tiek nosūtīti Regulas 49. panta 1. punkta otrajā daļā norādītajā gadījumā) (*piemēram, nosūtāmo datu veidi, tiesiskie pamati*)	✓	✓
Ja iespējams – paredzētie termiņi dažādu datu kategoriju dzēšanai	✓	
Ja iespējams – tehnisko un organizatorisko drošības pasākumu vispārējs apraksts (*piemēram, norādot kā dati tiek aizsargāti pret fiziskās iedarbības riskiem, kā dati tiek aizsargāti pret datu nejaušu iznīcināšanu, pret kiberuzbrukumu draudiem vai šādu informāciju norādot citā saistītā dokumentā*)	✓	✓

(Ar grozījumiem, kas izdarīti 08.01.2021.)

[35] Saskaņā ar Regulas 26. pantu, ja divi vai vairāki pārziņi kopīgi nosaka apstrādes mērķus un veidus, tie uzskatāmi par kopīgiem pārziņiem.

Kādā formā reģistrs kārtojams?

Reģistrs kārtojams rakstiski, ieteicams to kārtot elektroniskā formātā, lai nodrošinātu ērtu un pieejamu informācijas formu.

Zemāk norādīts reģistra paraugs (pieņemot, ka tehnisko un organizatorisko drošības pasākumu vispārējs apraksts tiek kārtots atsevišķi), kuru iespējams pielāgot, ņemot vērā katras konkrētās kredītiestādes darbības atšķirības.

Tabula Nr. 9

Reģistrā iekļaujamo sadaļu paraugs

Pārziņa nosaukums	Datu aizsardzības speciālists	Apstrādes nolūki	Datu kategorijas	Datu subjektu kategorijas	Datu saņēmēju kategorijas	Informācija par datu nosūtīšanu uz trešo valsti	Glabāšanas termiņš
SIA "BANK", bank@bank.eu, t.27654321	Jānis Pēteris janis@bank.eu,	Darbinieku nodarbināšana	Identifikācijas dati, finanšu dati	Darbinieki	Valsts iestādes	Netiek nosūtīti dati	5 gadi
		Sava īpašuma aizsardzība	Atrašanās vietas dati, biometriskie dati	Personas, kuras iekļūst video novērošanas zonā	Pakalpojumu sniedzēji, valsts iestādes	Netiek nosūtīti dati	2 nedēļas

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Reģistra aktualizācija

Ņemot vērā to, ka komercdarbības vide ir mainīga, regulāri rodoties jauniem pakalpojumiem, jaunām normatīvo aktu prasībām vai mainoties esošām, nepieciešams nodrošināt, ka reģistrs tiek regulāri aktualizēts, līdz ar to nepieciešams noteikt atbildīgo personu par šī reģistra uzturēšanu.

Vai reģistrs ir izpaužams?

Reģistrs pēc pieprasījuma ir jādara pieejams uzraudzības iestādei.

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 30. pantā.

6.3. Novērtējums par ietekmi uz datu aizsardzību

Novērtējuma mērķis, būtība un saistība ar citiem procesiem

Novērtējums par ietekmi uz datu aizsardzību (turpmāk arī – novērtējums) ir paredzēts, lai identificētu un mazinātu riskus, lai veicinātu adekvātu datu aizsardzības risinājumu ieviešanu, kā arī lai novērstu reputācijas un uzticamības zaudēšanu.

Šobrīd kredītiestādēs ir dažādas pieejas novērtējuma veikšanai – ir gadījumi, kad atsevišķs novērtējums par ietekmi uz datu aizsardzību netiek veikts, citos gadījumos datu aizsardzības aspekti ir iekļauti kopējā risku izvērtējuma procesā (kā daļa no atbilstības riska), kā arī kredītiestādēs var būt noteikta atsevišķa procedūra un izveidota speciāla komisija attiecīgā novērtējuma veikšanai. Saistībā ar citiem risku vērtēšanas procesiem, kredītiestādēs datu aizsardzības ietekmes novērtējuma aspekti var būt iekļauti atbilstības risku izvērtējuma procedūrā, kā arī biznesa ietekmes izvērtējuma procedūrā.

Jāuzsver, ka Regula paredz novērtējumu tikai datu aizsardzības jomā. Savukārt privātuma riski ir ar plašāku saturu un privātuma risku vadība var izpausties arī plašāk, piemēram, attiecībā uz komunikācijas (kas arī var nesaturēt datus) privātuma aizsardzību, ietverot datu aizsardzību, kā arī var būt situācijas, kad privātuma riski nemaz neskar datu aizsardzības aspektus.

Ņemot vērā minēto, datu aizsardzības novērtējuma procesu var būt nepieciešams harmonizēt ar jau esošajiem privātuma un informācijas drošības risku pārvaldības procesiem. Pēc būtības novērtējums par ietekmi uz datu aizsardzību veido daļu no risku vadības procesa, bet konkrēti datu aizsardzības kontekstā. Tādējādi atkarībā no katras kredītiestādes vajadzībām un iekšējās organizācijas novērtējumu par ietekmi uz datu aizsardzību var iekļaut jau esošajos risku pārvaldības procesos, nodrošinot šī elementa atbilstību Regulas prasībām, vai arī nodalīt kā atsevišķu procedūru.

Lai varētu pilnībā ievērot Regulas nosacījumus par novērtējuma nepieciešamību un veikšanu, rekomendējams iekļaut esošajos atbilstības, informācijas drošības un privātuma risku vadības procesos (atkarībā no katras kredītiestādes vajadzībām) nepieciešamību izvērtēt datu apstrādes esamību un attiecīgās apstrādes risku līmeni personas tiesībām un brīvībām datu aizsardzības kontekstā. Šādā veidā, identificējot augsta līmeņa risku (pēc Regulā noteiktajiem kritērijiem, kas noteikti, ņemot vērā katras konkrētās kredītiestādes darbības specifiku), būtu iespējams uzsākt atsevišķu novērtējumu par ietekmi uz datu aizsardzību, tādējādi izpildot Regulas prasības.

Novērtējumam par ietekmi uz datu aizsardzību jābūt nepārtrauktam procesam visā apstrādes gaitā (no datu apstrādes uzsākšanas līdz datu izdzēšanai), nevis kā atsevišķam uzdevumam, kura galarezultāts ir ziņojums.[36] Tādējādi datu aizsardzības risku izvērtējumu būtu nepieciešams integrēt risku vadības procesos, lai nodrošinātu nepārtrauktu darbības risku izvērtējumu arī datu aizsardzības kontekstā.

Kad veicams novērtējums?

Novērtējums ir obligāti veicams, ja apstrāde var radīt augstu risku personas tiesībām un brīvībām. Uz augstu risku var norādīt datu apstrādes veids, izmantojamās tehnoloģijas, apstrādes raksturs, apstrādes apjoms, apstrādes konteksts, apstrādes nolūki. Novērtējuma veikšana ir dokumentējama, lai pierādītu šī pienākuma izpildi un atbilstību Regulai.

Augsts risks personas tiesībām un brīvībām ir konstatējams un novērtējums ir veicams vismaz šādos gadījumos (uzskaitījums nav izsmeļošs):

1. ar fiziskām personām saistītu personisku aspektu sistemātiska un plaša novērtēšana, kuras pamatā ir automatizēta apstrāde, tostarp profilēšana, un ar kuru pamato lēmumus, kas fiziskai personai rada tiesiskās sekas vai būtiski ietekmē fizisko personu.

   Piemēram, lielākā daļa kredītiestāžu sniedzamie pakalpojumi ir saistīti ar sistemātisku un plašu datu subjektu novērtēšanu, piemēram, kredītspējas vērtēšana vai klienta maksājumu saistību izpildes uzraudzība.

2. Īpašu kategoriju datu vai datu par sodāmību un pārkāpumiem apstrāde plašā mērogā.

   Piemēram, kredītiestādes darbinieku datu apstrādi saistībā ar sodāmību un pārkāpumiem, kā arī Īpašu kategoriju datu apstrādi, lai pārliecinātos par darbinieka atbilstību ieņemamajam amatam vai lai nodrošinātu līguma izpildi, nevarētu uzskatīt par plaša mēroga datu apstrādi, tomēr, ja pakalpojumu sniegšanas ietvaros tiek apstrādāti klientu vai Īpašu kategoriju dati, tā varētu tikt uzskatīta par plaša mēroga apstrādi.

3. publiski pieejamas teritorijas vai zonas sistemātiska uzraudzība plašā mērogā, piemēram, videonovērošanas veikšana.

[36] Sk. arī: http://www.piafproject.eu/ref/PIAF_D3_final.pdf 12.lpp.

29. panta darba grupa savā rekomendācijā ir sniegusi uzskaitījumu kritērijiem, kas varētu liecināt par augta riska esamību datu apstrādē (jo vairāk kritēriju datu apstrādē sastopami, jo augstāks risks), kas uzskaitīti tabulā.

Tabula Nr. 10

Augsta riska datu apstrādes kritēriji

Kritērijs	Kritērija apraksts
Profilēšana vai cita veida datu subjektu personisko aspektu izvērtēšana	*Piemēram, kredītiestādei izvērtējot savu klientu kredītspēju, krāpniecības riskus,, īpaši gadījumos, ja šī informācija tiek izmantota, lai pieņemtu datu subjektam saistošus lēmumus (piemēram, atteikt pakalpojumu).*
Automatizētu lēmumu pieņemšana, kas var radīt juridiski saistošas vai citādi būtiskas sekas datu subjektam	*Piemēram, kredītiestāde ar automatizētiem rīkiem identificē krāpniecības riskus un automatizēti nodrošina šīs informācijas pārsūtīšanu drošības dienestam vai tiesībaizsardzības iestādēm, vai kredītiestāde automatizētiem līdzekļiem izvērtē klienta pieteikumu un pieņem automatizētu lēmumu par kredīta piešķiršanu vai noraidīšanu.*
Pastāvīga vai sistemātiska datu subjektu novērošana	*Šis kritērijs ir īpaši svarīgs gadījumos, kad datu subjekts nav pietiekami informēts par datu apstrādi (vai dati tiek apstrādāti, kurš datus apstrādā un kādam nolūkam apstrāde tiek veikta), kā arī gadījumos, ja datu subjektam nav iespējas izvairīties no šādas datu apstrādes, piemēram, publiskās vietās.*
Īpašu kategoriju datu apstrāde	*Piemēram, kredītiestādei noskaidrojot klienta tautību vai biometriskās piekļuves kontroles sistēmu ieviešana kredītiestādes telpās.*
Datu apstrāde plašā mērogā	*Ja datu apstrādei ir pakļauta būtiska daļa klientu, tad tā būtu uzskatāma par apstrādi plašā mērogā.*
Tiek apvienotas datu bāzes	*Piemēram, kredītiestāde izlemj, lai sniegtu efektīvāk pakalpojumu, apvienot savu klientu datu bāzi ar publiski pieejamu datu bāzi, lai, piemēram, automatizēti fiksētu izmaiņas klienta dzīves veidā, piemēram, maksātspējas informācijā.*
Datu apstrāde attieksies uz mazāk aizsargātiem datu subjektiem	*Piemēram, apstrādājot bērnu, senioru vai darbinieku datus.*
Jaunu tehnoloģiju vai programmatūru izmantošana	*Jaunu tehnoloģiju vai programmatūru izmantošana, piemēram, sejas atpazīšanas sistēmas ieviešana, lai konstatētu, vai persona varētu radīt krāpniecības riskus, vienmēr ir saistīta ar nezināmiem riskiem, kā attiecīgie risinājumi ietekmēs datu subjekta tiesības uz savu datu aizsardzību, līdz ar to pie jebkuru jaunu tehnoloģisko vai programmatūras risinājumu izmantošanas būtu ieteicams izvērtēt nepieciešamību veikt novērtējumu.*

29. panta darba grupa[37] rekomendē, ja datu apstrādei ir piemērojami vismaz divi no iepriekš minētajiem kritērijiem, tad novērtējuma veikšana ir ieteicama, tomēr nevar izslēgt gadījumus, kad arī viena kritērija esamība arī varētu būt būtiska.

Piemēram, novērtējums ir jāveic gadījumos, ja kredītiestāde, lai pārvaldītu klientu kredītrisku, iegūst un saglabā datus no publiski pieejamas informācijas un arī no citām datu bāzēm – šī būtu apstrāde, kurai ir jāveic novērtējums, jo tā satur trīs no augstāk minētajiem kritērijiem: (1) tiek veikta datu subjekta personisko aspektu izvērtēšana; (2) tiek apvienotas datu bāzes; (3) kā arī notiek datu apstrāde plašā mērogā.

Kredītiestāžu darbības specifika ir tāda, ka to veiktās ikdienas klientu datu apstrādes darbības atbilst plaša mēroga apstrādei, kas ir viens no augsta riska apstrādes kritērijiem, tomēr, vērtējot riskus, ir jāņem vērā arī augstā kredītiestāžu regulācijas pakāpe, noteiktās minimālās informācijas drošības prasības, kas varētu būt pamatots arguments risku samazināšanai.

[37] 2017. gada 4. aprīļa 29. panta darba grupas rekomendācija "Pamatnostādnes novērtējuma par ietekmi uz datu aizsardzību (NIDA) veikšanai un noskaidrošanai, vai apstrāde "varētu radīt augstu risku" Regulas 2016/679 izpratnē" 11. lpp.

29. panta darba grupas vadlīnijās datu apstrāde plašā mērogā tiek izcelta kā augsta riska apstrādes kritērijs. Ņemot vērā piemērus, kas minēti 29. panta darba grupas vadlīnijās par datu aizsardzības speciālistu[38], klientu datu apstrāde kredītiestādes ikdienas darbībā varētu tikt uzskatīta par plaša mēroga apstrādi. Tādējādi praktiski visas kredītiestāžu klientu apkalpošanas ietvaros veiktās datu apstrādes darbībās konstatējams kritērijs, kas norāda uz augsta riska apstrādi.

No otras puses, ikdienas klientu apkalpošanas procesi kredītiestādēs ir strikti regulēti, kontrolēti un saprotami, tādējādi nebūtu pamatoti pieņemt, ka jebkuras kredītiestādes veiktās klientu datu apstrādes rada augstu risku datu subjektiem tikai tāpēc, ka apstrāde ir plaša mēroga, tādējādi pakļaujot minēto apstrādi iepriekšēja novērtējuma pienākumam. Izšķirošajam faktoram, lai noteiktu novērtējuma nepieciešamību, būtu jābūt slēdzienam par apstrādes riska pakāpi kopumā, nevis ņemot vērā tikai atsevišķus kritērijus.

Arī uzraudzības iestādēm ir pienākums publicēt sarakstu ar apstrādes darbībām, kurām obligāti nepieciešams novērtējums, taču jāņem vērā, ka šis saraksts var mainīties. Datu valsts inspekcija apstiprināja šo sarakstu 2018. gada 18. decembrī.[39] Līdz ar to gadījumos, kad kredītiestāde, ievērojot publicēto sarakstu ar apstrādes darbībām, pieņēmusi lēmumu par novērtējuma neveikšanu, balstoties uz apstrādes risku izvērtējumu, nepieciešams pastāvīgi veikt pārbaudi, vai attiecīgā apstrāde nav iekļauta uzraudzības iestādes izveidotajā sarakstā.

Pārrobežu apstrādes gadījumā nepieciešams izskatīt vadošās uzraudzības iestādes publicēto sarakstu. Ja pārzinim rodas aizdomas, ka attiecīgā apstrāde varētu būt iekļauta citas dalībvalsts uzraudzības institūcijas izveidotajā sarakstā, kurā tiks veikta attiecīgā apstrāde, nepieciešams konsultēties ar vadošo uzraudzības iestādi, lai noskaidrotu novērtējuma nepieciešamību, tajā skaitā, izmantojot sadarbības mehānismu.

Gadījumā, ja kredītiestādei nav skaidrs, vai novērtējums ir jāveic, ieteicams veikt novērtējumu, jo novērtējums ir efektīvs mehānisms kā nodrošināt atbilstību Regulai. Netiek izslēgta arī iespēja novērtējuma nepieciešamības jautājumos konsultēties ar uzraudzības iestādi. Tikšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR Darba grupu 2019. gada 7. martā Datu valsts inspekcija pauda viedokli, ka novērtējums uzskatāms par duālu rīku. No vienas puses, par tās neveikšanu paredzētas sankcijas, bet no otras – tas palīdz datu pārzinim saglabāt kontroli pār iekšējiem procesiem un sakārtot tos. Līdz ar ko DVI aicina neskatīties uz novērtējumu kā uz formālu likuma prasību.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Gadījumi, kad novērtējumu var neveikt

Novērtējumu var neveikt, ja apstrādes tiesiskais pamats ir juridiska pienākuma izpilde un pārzinim piešķirto oficiālo pilnvaru īstenošana (Regulas 6. panta 1. punkta "c" un "e" apakšpunkts), *piemēram, kredītiestādēm, izpildot NILLTPFNL prasības, ir tiesības neveikt novērtējumu, pamatojoties uz to, ka šāds pienākums ir noteikts likumā, savukārt attiecībā uz kredītspējas pārbaudi novērtējums būtu iespējams jāveic, jo neskatoties uz to, ka Patērētāju tiesību aizsardzības likumā ir noteikts pienākums veikt klienta kredītspējas pārbaudi, papildus likumā noteiktajam pienākumam, kredītiestādei ir arī savas kredītiestādes leģitīmās intereses neciest zaudējumus, un tādējādi tā rīkus kredītspējas izvērtēšanai izvēlās pati, veicot lielāka apjoma datu apstrādi salīdzinājumā ar likumā noteikto minimumu*. Tāpat novērtējumu var neveikt, ja plānotās apstrādes veids, konteksts, apjoms un nolūki ir līdzīgi apstrādei, kurai novērtējums jau ir veikts[40].

Uzraudzības iestādēm ir tiesības noteikt un publicēt sarakstu ar apstrādes darbībām, kurām nav nepieciešams novērtējums, līdz ar to kredītiestādēm ir nepieciešams sekot līdzi šāda saraksta saturam un izmaiņām tajā.

[38] 2016. gada 13. decembra 29. panta darba grupas rekomendācijas "Pamatnostādnes par datu aizsardzības speciālistiem (DAS)" 8. lpp.
[39] Sk.: Apstrādes darbību veidi, attiecībā uz kuriem ir jāveic datu aizsardzības ietekmes novērtējums saskaņā ar VDAR 35.panta 4.punktu, Datu valsts inspekcija. Pieejams: https://www.dvi.gov.lv/lv/wp-content/uploads/Saraksts-ar-tiem-apstr%C4%81des-darb%C4%ABbas-veidiem-attiec%C4%ABb%C4%81-uz-kuriem-ir-j%C4%81veic-nov%C4%93rt%C4%93jums-par-ietekmi-uz-datu-aizsardz%C4%ABbu-NIDA1.pdf
[40] Sk. arī Ieteikumu 6.3. nodaļas "Novērtējums par ietekmi uz datu aizsardzību" sadaļu "Apvienota vai kopīga novērtējuma veikšana".

Novērtējums par datu apstrādes darbībām, kuras uzsāktas pirms 2018. gada 25. maija

Pienākums veikt novērtējumu attiecas uz apstrādes darbībām, kas uzsāktas pēc 2018. gada 25. maija. Lai gan Regulā nav īpaši noteikts, vai pēc Regulas piemērošanas uzsākšanas jāveic novērtējums, tomēr, ja apstrādes darbībā ir notikušas būtiskas izmaiņas vai arī apstrādes radītie riski ir būtiski izmainījušies (*piemēram, tehnoloģiskas izmaiņas vai normatīvā regulējuma izmaiņas*), novērtējums būtu jāveic. Tikšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR Darba grupu 2019. gada 7. martā Datu valsts inspekcija aicināja negaidīt, kad pienāks uzņēmumā noteiktais kārtējais nolūku pārskatīšanas termiņš. Kaut arī iesākto procesu monitorēšanu DVI varētu uzskatīt par labo praksi, DVI ieskatā, datu pārzinis nevar paļauties tikai uz regulārām nolūku/procesu pārskatīšanas rutīnām. Attiecīgi, pēc 2018. gada 25. maija būtu jāpārbauda, vai apstrādes ietvaros netiek veiktas darbības, kas neatbilst iepriekš reģistrētiem nolūkiem (virsnolūkiem) vai arī paliek ārpus tiem.

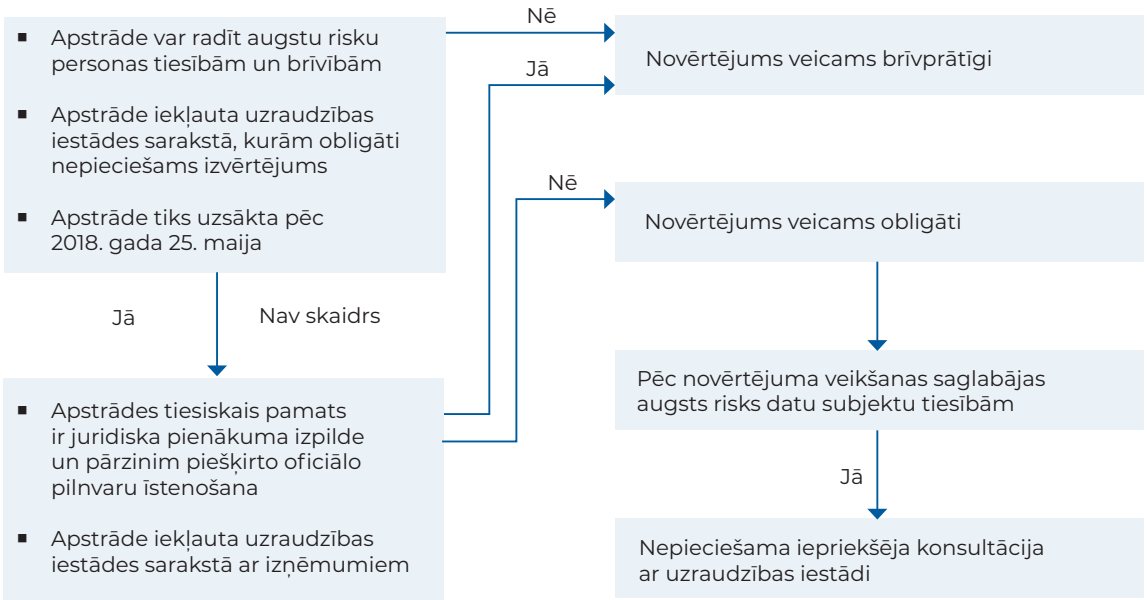
Tādējādi ir rekomendējams veikt novērtējumu arī paaugstināta riska apstrādes darbībām, kuras uzsāktas pirms Regulas piemērošanas, lai identificētu un izvairītos no šādas apstrādes radītajiem riskiem datu aizsardzības jomā. Savukārt apstrādes darbībām, kurām ir veikts datu apstrādes novērtējums iepriekš vai kuras ir reģistrētas Datu valsts inspekcijā, ja to raksturs un riski nav mainījušies pēc Regulas piemērošanas, nav nepieciešams veikt atkārtotu novērtējumu.

Tikšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR Darba grupu 2019. gada 7. martā Datu valsts inspekcija pauda viedokli, ka var saskatīt līdzības riskos kas attiecas uz uzņēmumu riskiem kas attiecināmi uz datu subjektu. Līdz ar ko, ja pirms 2018. gada 25. maija kredītiestāde veica ar iekšējiem procesiem saistīto risku izvērtējumu (pat tad, ja datu apstrāde netika specifiski izdalīta no datu subjekta skatpunkta), ar sekojošu datu apstrādes reģistrāciju DVI, kā arī ja reģistrētajā personas datu apstrādē kopš reģistrācijas brīža nav notikušas būtiskas izmaiņas, tad kredītiestāde ir izpildījusi prasības attiecībā uz novērtējuma veikšanu.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Shēma Nr. 1

Novērtējuma veikšanas nepieciešamības shematisks attēlojums:



Novērtējuma metodoloģija, saturs un forma

Regula paredz, ka novērtējumā ietver vismaz šādus elementus:

1) plānoto apstrādes darbību aprakstu un novērtējumu;
2) plānoto nolūku aprakstu un novērtējumu;
3) kredītiestādes vai trešās personas leģitīmo interešu aprakstu un novērtējumu;
4) novērtējumu par apstrādes darbību atbilstību nolūkiem, nepieciešamību un samērīgumu;
5) analīzi pasākumiem, kas paredzēti risku novēršanai un atbilstības Regulai demonstrēšanai.

Novērtējuma veikšanai Regula nenosaka konkrētu metodoloģiju, novērtējuma saturu vai formu. Līdz ar to novērtējuma veicējam ir iespējams izvēlēties savam apstrādes darbību raksturam atbilstošu novērtējuma veikšanas metodoloģiju, kā arī papildināt novērtējumā iekļaujamo elementu klāstu.

Saskaņā ar 29. panta darba grupas vadlīnijām, novērtējuma metodoloģijā jābūt vismaz šādiem kritērijiem, lai varētu pieņemt, ka novērtējumā ir atbilstoši izvērtēti visi datu aizsardzības aspekti:

1) jāsniedz sistemātisks apstrādes apraksts:
  a) nosakot apstrādes raksturu, apmēru, kontekstu un nolūkus;
  b) fiksējot datu veidus, saņēmējus un laikposmu, cik ilgi dati tiks glabāti;
  c) sniedzot funkcionālu apstrādes aprakstu un identificējot apstrādes resursus (aparatūru, programmatūru, tīklus, cilvēkus, dokumentus vai pārraides/saziņas kanālus);
  d) ņemot vērā apstrādes darbību atbilstību apstiprinātajiem rīcības kodeksiem;

2) jānovērtē apstrādes nepieciešamība un samērīgums, tajā skaitā:
  a) apstrādes atbilstību konkrētiem, skaidriem un leģitīmiem nolūkiem;
  b) apstrādes likumīgumu;
  c) datu adekvātumu un minimizēšanu;
  d) datu uzglabāšanas laiku;
  e) datu subjektu tiesību ievērošanu (piemēram, informēšanu, piekļuvi datiem, labošanu), kā arī, ja nepieciešams, veikt iepriekšēju apspriešanos ar uzraudzības iestādi;

3) pārvaldīt riskus attiecībā uz datu subjektu tiesībām un brīvībām:
  a) novērtējot riska avotus, raksturu, specifiku un nopietnību;
  b) izvērtējot iespējamo ietekmi uz datu subjektu tiesībām un brīvībām (gadījumā, ja notiek nelikumīga piekļuve, nevēlamas izmaiņas un datu pazušana) attiecībā uz katru iespējamo risku, kā arī nosakot pasākumus, kas paredzēti minēto risku novēršanai;

4) iesaistītas ieinteresētās puses (piemēram, datu aizsardzības speciālista viedoklis, datu subjekta un to pārstāvju viedokļi).

Novērtējuma veikšanas plāns

Tā kā Regula nenosaka novērtējuma veikšanas plānu, novērtējuma veicējam ir iespējams izvēlēties savam apstrādes darbību raksturam atbilstošu novērtējuma veikšanas plānu. Kā jau minēts iepriekš, novērtējums var tikt veikts gan atsevišķi, gan arī tas var tikt integrēts kādā citā risku vadības procesā.
Pieņemot, ka novērtējums tiek veikts kā atsevišķs process, galveno novērtējuma ietvaros veicamo soļu piemēri norādīti tabulā[41]

[41] https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Tabula Nr. 11

Piemērs novērtējuma veikšanas plānam

Solis	Veicamās darbības
Solis Nr. 1	Datu apstrādes esamības un novērtējuma nepieciešamības konstatēšana
Solis Nr. 2	Iesaistīto personu noteikšana (t.sk. konsultēšanās)
Solis Nr. 3	Datu un to plūsmu apraksts
Solis Nr. 4	Atbilstības (nolūku nozīmīguma, datu minimizācijas u.c.) izvērtējums
Solis Nr. 5	Datu aizsardzības risku identificēšana
Solis Nr. 6	Risinājumu izstrāde
Solis Nr. 7	Novērtējuma rezultātu apkopošana un dokumentēšana
Solis Nr. 8	Novērtējuma rezultātu integrēšana biznesa projekta izstrādē un realizēšanā
Solis Nr. 9	Pārskatīšana un pārbaude

Tomēr, ņemot vērā katras kredītiestādes specifiku, novērtējuma procesa organizēšana var atšķirties gan starp kredītiestādēm, gan pašā kredītiestādē (detalizētāki novērtējumi riskantākām apstrādes darbībām, novērtējumi, kas iekļaujas citā procesā utt.).

Novērtējumā iesaistītās personas

Kopumā kredītiestāde ir atbildīga par novērtējuma veikšanu, tomēr, veicot novērtējumu, var lūgt datu aizsardzības speciālista viedokli, kā arī ieteicams lūgt viedokli datu subjektiem vai to pārstāvjiem (*piemēram, arodbiedrībai*), kā arī apstrādātājam, ja to plāno iesaistīt apstrādes darbībās. Ieteicams noskaidrot arī datu apstrādē iesaistāmo struktūrvienību viedokli, piemēram, IT departamenta, lai sniegtu padomu risinājumiem, riska novēršanai vai mazināšanai, kā arī, ja nepieciešams, piesaistot neatkarīgus nozares ekspertus.

Apvienota vai kopīga novērtējuma veikšana

Novērtējuma veikšana nav ierobežota tikai konkrētam projektam. Apvienots novērtējums var tikt veikts vairākām apstrādes darbībām, ja to riski ir līdzīgi un tiek adekvāti ņemta vērā katras apstrādes būtība, nolūki, apjoms un konteksts. *Piemēram, ja tiek plānots ieviest divus jaunus, savā starpā līdzīgus kredītiestādes produktus (vai vienu produktu, kas pielāgots dažādiem klientu segmentiem), kuru realizācija prasa līdzīgu datu apstrādi. Nav nepieciešams veikt novērtējumu katram produktam atsevišķi, bet iespējams veikt apvienotu novērtējumu par abiem produktiem.*

Novērtējuma veikšana nav ierobežota tikai konkrētam pārzinim, bet arī vairākiem pārziņiem ir iespējams veikt kopīgu novērtējumu. *Piemēram, ja kredītiestādēm ir kopējs projekts (jaunas tehnoloģijas vai risinājuma ieviešana), ir pieļaujams, ka kredītiestādes, tajā skaitā arī sadarbojoties caur citiem nozares pārstāvjiem (piemēram, ar Latvijas Finanšu nozares asociācijas starpniecību), veic kopīgu novērtējumu vai, ja kredītiestādes grupas uzņēmumos tiek ieviesta vienota klientu datu apstrādes sistēma, uzņēmumu grupa var veikt vienotu novērtējumu šai datu apstrādes sistēmai.*

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Apspriešanās ar uzraudzības iestādi

Ja no novērtējuma izriet, ka, neskatoties uz kredītiestādes plānotajiem saprātīgiem aizsardzības un riska mazināšanas pasākumiem, saglabājas augsts risks datu subjektu tiesībām (piemēram, datu subjekti var tikti pakļauti ievērojamām vai neatgriezeniskām sekām vai ir acīmredzams, ka identificētie riski iestāsies), kredītiestādei pirms datu apstrādes uzsākšanas jāapspriežas ar uzraudzības iestādi.

Novērtējuma izpaušana

Novērtējumu nav nepieciešams publicēt vai citādi izpaust. Tomēr novērtējuma, tā daļas vai tā apkopojuma publicēšana var veicināt uzticamību kredītiestādei, kā arī nodrošināt caurspīdīguma un pārskatatbildības principa pilnīgu ievērošanu.[42]

Gadījumos, kad ir nepieciešama apspriešanās ar uzraugošo iestādi, tad novērtējuma izpaušana ir nepieciešama šī pienākuma izpildei. Tāpat izpaušana lielākā vai mazākā mērā ir nepieciešama, lai nodrošinātu citu personu iesaistīšanu novērtējumā vai arī kopīga novērtējuma veikšanā. Jebkurā gadījumā kredītiestādei nav nepieciešams caur novērtējumu izpaust tās komercnoslēpumus.

Novērtējuma un apstrādes pārskatīšana

Regula paredz, ka pārzinim jāizvērtē apstrādes atbilstība veiktajam novērtējumam vismaz tajā gadījumā, ja ir mainījies apstrādes riska profils. Tajā pašā laikā tiek rekomendēts veikt apstrādes atkārtotu novērtējumu, ņemot vērā apstrādes procesa vai citu apkārtējo apstākļu izmaiņas.[43]

Novērtējumā iekļaujamo jautājumu paraugi

1) Vai ir izvērtēta nepieciešamība konkrētā apjoma datu apstrādei? Vai ir iespējams sasniegt nolūku, neapstrādājot datus vai apstrādājot tos mazākā apmērā?
2) Vai ir precīzi definēts datu apstrādes nolūks, apstrādājamo datu veidi (t.sk. Īpašu kategoriju dati)? Vai datu apstrāde ir atbilstoši nolūka sasniegšanai?
3) Kāds tiesiskais pamats paredzēts datu apstrādei?
4) Vai tiks piesaistīti datu apstrādātāji? Vai ar apstrādātājiem ir noslēgti atbilstoši līgumi, kas paredz pārziņa kontroles tiesības?
5) Cik bieži un kādā veidā tiks pārskatīta datu apstrādes nepieciešamība un atbilstība apstrādes nolūkam?
6) Cik bieži un kādā veidā tiks precizēti vai atjaunoti apstrādātie dati?
7) Vai ir noteikts datu saņēmēju loks (iekšējais un trešo personu) un ierobežota piekļuve citām personām?
8) Vai ir noteikts datu glabāšanas ilgums un dzēšanas kārtība?
9) Vai ir noteikti mehānismi datu subjekta tiesību ievērošanai (piemēram, informēšanas, piekļuves tiesības)? Vai ir noteikta kārtībā, kādā reaģēt uz datu subjektu pieprasījumiem?
10) Vai ir skaidri noteikti datu saņēmēji ārpus ES, kā arī definēts šādas datu nodošanas tiesiskais pamats?
11) Vai datu apstrādes drošības nodrošināšanai paredzēti atbilstoši tehniskie un organizatoriskie pasākumi?

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 75., 76., 77., 84., 89., 90., 91., 92., 94. un 95. apsvērumā un Regulas 35. un 36. pantā, kā arī 2017. gada 4. aprīļa 29. panta darba grupas rekomendācijā "Pamatnostādnes novērtējuma par ietekmi uz datu aizsardzību (NIDA) veikšanai un noskaidrošanai, vai apstrāde "varētu radīt augstu risku" Regulas 2016/679 izpratnē".

6.4. Datu aizsardzības pārkāpumi

Kas ir datu aizsardzības pārkāpums?

Datu aizsardzības pārkāpums ir drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem. Ir jānošķir drošības incidents no datu aizsardzības pārkāpuma (kurā kaitējums tiek nodarīts tieši fizisko personu datiem, nevis, piemēram, juridisko personu datiem vai kredītiestādes mantai).

[42] 2017. gada 4. aprīļa 29. panta darba grupas rekomendācija "Pamatnostādnes novērtējuma par ietekmi uz datu aizsardzību (NIDA) veikšanai un noskaidrošanai, vai apstrāde "varētu radīt augstu risku" Regulas 2016/679 izpratnē".
[43] Turpat.

Kā vērtēt datu aizsardzības pārkāpuma ietekmi uz datu subjektu?

Jāvērtē ir jebkāda fiziska, materiāla vai nemateriāla kaitējuma nodarīšana datu subjektam, t.sk. datu subjekta zaudētās iespējas kontrolēt savus datus vai tā tiesību ierobežošana, diskriminācijas iespējamība, identitātes zādzības vai viltošanas risks, finansiāla zaudējuma iespējamība, pseidonimizētu datu atklāšana, iespējams kaitējums reputācijai, ar dienesta noslēpumu aizsargātu datu konfidencialitātes zaudēšanas iespējamība vai jebkāda cita attiecīgajai fiziskajai personai īpaši nelabvēlīgas ekonomiskās vai sociālās situācijas rašanās.

Tāpat, izvērtējot pārkāpuma raksturu, ir jāņem vērā pārkāpuma veids (*piemēram, vai dati publicēti, vai nepamatoti iznīcināti*), datu raksturs (*piemēram, Īpašu kategoriju dati, finanšu dati, paroles*) un apjoms, datu subjekta identifikācijas iespējamība, seku būtiskums datu subjektam (*piemēram, publicējot datus, kas ir zināmi jau sabiedrībai, vai rūpīgi slēptus no sabiedrības datus – minētajos gadījumos sekas datu subjekta privātumam būs atšķirīgas),* datu subjektu kategorijas *(piemēram, bērniem, personām ar veselības problēmām aizskārums radīs atšķirīgas sekas*), skarto datu subjektu skaits.

Tikšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR Darba grupu 2019. gada 7. martā Datu valsts inspekcija vērsa uzmanību, ka ziņošanas pienākuma atslēgas kritēriji ir minēti regulas 33. pantā. DVI ieskatā, uzraudzības iestādei nav jāziņo par personas datu aizsardzības pārkāpumu, ja ir maz ticams, ka pārkāpums radīs risku datu subjektiem. Neskatoties uz to, datu pārzinim ir iekšēji jādokumentē visi konstatētie datu aizsardzības pārkāpumi, kā arī jāpamato, kāpēc ir maz ticams, ka riski iestāsies, un kāpēc riski nav augsti. Katrs gadījums ir vērtējams atsevišķi.

Arī gadījumos, kad pārkāpuma rezultātā ir izpausti tikai tādi personas dati, ar kuru palīdzību fizisko personu var identificēt tikai pārzinis, piemēram, kartes numurs vai klienta numurs bez papildu identifikatoriem, DVI var saskatīt riskus attiecībā uz datu subjektu, jo kartes numurs var būt zināms ne tikai klientam un kredītiestādei, bet, piemēram, arī interneta veikaliem. Ja pēc kartes numura izpaušanas, karte tiek bloķēta, tad ir maz ticams, ka pārkāpums rezultēsies ar risku klientam. Savukārt, ja klients pats pazaudē karti, tad tas nav uzskatāms par kredītiestādes datu aizsardzības pārkāpumu. Par tādiem var neuzskatīt arī tā saucamos "skimmeri", ja vien kredītiestāde ir ievērojusi nepieciešamos tehniskos un organizatoriskos drošības pasākumus.

DVI iesaka, ka tajā gadījumā, kad datu pārzinim rodas šaubas par datu aizsardzības pārkāpuma radīto riska līmeni, tomēr ziņot DVI par pārkāpumu. Pretējā gadījumā, ja DVI kļūs zināms par notikušo pārkāpumu no citām personām, DVI var piemērot pārzinim sodu par ziņošanas pienākuma nepildīšanu, ja tas būs gadījums, kas būtu bijis DVI jāziņo.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Tabula Nr. 12

Vai ir jāziņo par datu aizsardzības pārkāpumu?

Pārkāpuma apraksts	Ziņošana uzraudzības iestādei (bez nepamatotas kavēšanās, bet ne vēlāk kā 72 stundu laikā)	Ziņošana Datu subjektam (bez nepamatotas kavēšanās)
Bez riska grupa: Pārkāpums, kas maz ticams, ka varētu radīt risku fizisku personu tiesībām un brīvībām.	×	×
Riska grupa: Pārkāpums rada risku, kurš neatbilst bez risk un augsta riska grupai.	✓	×
Augsta riska grupa: Pārkāpums var radīt augstu risku fizisku personu tiesībām un brīvībām.	✓	✓

Saskaņā ar Regulas noteikumiem[44] paziņojums datu subjektam nav jāsniedz, ja tiek izpildīts jebkurš no šādiem nosacījumiem:

- kredītiestāde ir īstenojusi atbilstīgus tehniskus un organizatoriskus aizsardzības pasākumus un minētie pasākumi ir piemēroti datiem, ko skāris datu aizsardzības pārkāpums, jo īpaši tādi pasākumi, kas personas datus padara nesaprotamus personām, kurām nav pilnvaru piekļūt datiem, piemēram, šifrēšana;

- kredītiestāde ir veikusi turpmākus pasākumus, ar ko nodrošina, lai, visticamāk, vairs nevarētu materializēties iepriekš minētais augstais risks (Augsta riska grupa) attiecībā uz datu subjektu tiesībām un brīvībām;

- tas prasītu nesamērīgi lielas pūles. Šādā gadījumā tā vietā izmanto publisku saziņu vai līdzīgu pasākumu, ar ko datu subjekti tiek informēti vienlīdz efektīvā veidā.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Kā ziņot uzraudzības iestādei, ja nav zināma visa informācija, kas iekļaujama paziņojumā?

Paziņojumā uzraudzības iestādei ir jānorāda šāda informācijas par pārkāpumu:

1) pārkāpuma rakstura apraksts, t.sk. skarto datu subjektu kategorijas un aptuvenais skaits, skarto datu kategorijas;
2) datu aizsardzības speciālista vārds, uzvārds un kontaktinformācija, vai informācija par citu kontaktpersonu;
3) pārkāpuma iespējamās sekas;
4) pasākumu, ko kredītiestāde ir veikusi vai plāno veikt, lai novērstu pārkāpumu un/vai mazinātu iespējamās nelabvēlīgās sekas, aprakstu.

Ja gadījumā uz ziņošanas brīdi nav apkopota visa informācija, lai nodrošinātu tās sniegšanu uzraudzības iestādei, sniedzama būtu informācija, kas kredītiestādei ir zināma, un, tiklīdz tas ir iespējams, papildināt ziņojumu un nosūtīt to atkārtoti uzraudzības iestādei.

Ziņošana uzraudzības iestādei jāveic, izmantojot uzraudzības iestādes interneta vietnē pieejamo datu aizsardzības pārkāpuma ziņošanas veidlapu vai platformu. Gadījumos, kad uzraudzības iestādes interneta vietnē pieejamā pārkāpumu ziņošanas platforma nav pieejama, pārziņi ir tiesīgi izmantot citus pārkāpuma paziņošanas kanālus (*piemēram, iesniedzot Dokumentu juridiskā spēka likumam atbilstošu dokumentu, kurā norādīta iepriekš minētā informācija, uzraudzības iestādei*).

(Ar grozījumiem, kas izdarīti 08.01.2021.)

[44] Regulas 34. panta 3. punkts.

Tabula Nr. 13

Piemēri datu aizsardzības pārkāpumiem un to riska sadalījumam

Datu aizsardzības pārkāpuma apraksts	Bez riska grupa	Riska grupa	Augsta riska grupa
Kiberuzbrukuma gadījumā trešās personas ir ieguvušas klienta paroles un lietotāja vārdus			✓
Internetbankas sistēmas neplānots īss pārtraukums	✓		
Datu nesēja (piem., dokumentu, CD, USB), kurš satur līgumu ar klientu) nozaudēšana, ja informācija nav šifrēta un ir brīvi pieejama			✓
Izpausta informācija par klienta darījumu, par kuru ir bijis raksts interneta ziņu portālos	✓		
"Šifrēšanas atslēgas" noplūde		✓	
Šifrētu datu noplūde "šifrēšanas atslēgai" paliekot kredītiestādes kontrolē	✓		
Neatgriezeniska datu pazaudēšana (piemēram datu nesēju un visu rezerves kopiju fiziska iznīcināšana, vai "atšifrēšanas atslēgas" iznīcināšana)			✓
Kredītiestādes darbinieka datora nozaudēšana, kurā visa informācija ir šifrēta.	✓		
Nosūtīts konta pārskats uz citas personas (ne klienta) e-pasta adresi, ja šī cita persona var tikt uzskatīta par "uzticamības personu"[45]			✓
Komerciāli paziņojumi ir nosūtīti klientiem norādot adresātus visiem saņēmējiem redzamā veidā ("*Cc:*" laukā, nevis "*Bcc:*" laukā)	✓		
Klientu datu bāzes daļējs vai pilnīgs zudums			✓
Neautorizēta klientu datu apstrāde, ja tā ir notikusi kredītiestādes iekšienē un tas nerada risku klientam		✓	

Katrā situācijā ir papildus jāizvērtē attiecīgā pārkāpuma raksturs un specifika. Šis ir uzskatāms par ilustratīvu uzskaitījumu, lai palīdzētu izvērtēt datu aizsardzības pārkāpuma būtiskumu, turklāt papildus būtu jāizvērtē iepriekš minētie gadījumi, kad var neziņot datu subjektam.

Tikšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR Darba grupu 2019. gada 7. martā Datu valsts inspekcija pauda viedokli, ka gadījumos, kad personas datu aizsardzības pārkāpums ir izpaudies kā e-pasts nosūtīšana cilvēciskās kļūdas rezultātā, nepareizā adresāta apliecinājums par kļūdaini izsūtītā e-pasta dzēšanu samazina risku datu subjektam. Taču arī šajā gadījumā būtu jāvērtē riski un jādokumentē izvērtējums, kāpēc ir maz ticams, ka pārkāpums radīs risku datu subjektiem. Vienlaikus DVI aicina vērtēt, kāds ir izpausto personas datu apjoms, raksturs un to sensitivitāte, tai skaitā vai izpaustie dati var tikt izmantoti, piemēram, krāpšanai vai identitātes zādzībai. Būtisks aspekts izvērtējumam par iespējamo ietekmi uz datu subjektu ir nepareizā adresāta apliecinājums, ka dati ir dzēsti un izmantoti netiks. Gadījumā, ja šāds apliecinājums nav saņemts, tas automātiski nenozīmē, ka datu subjektam iestājušies augsti riski. Pārzinim ieteicams dokumentēt savus centienus sazināties ar nepareizo adresātu un lūgumu dzēst nepamatoti saņemtos datus, kā arī dokumentēt apliecinājumu par kļūdaini izsūtīto datu dzēšanu.

Turklāt Datu valsts inspekcijas ieskatā individuāli būtu jāvērtē arī gadījumi, kad personas datu aizsardzības pārkāpuma rezultātā izpaustie dati ir atrodami publiskajos reģistros un datubāzēs, kurām var piekļūt ar vai bez maksas. DVI ieskatā būtu jāvērtē izpausto datu apjoms, vai tika izpausti tikai tie dati, kas atrodami publiskajos reģistros.

DVI ieskatā, pēc līdzīgiem principiem būtu jārīkojas gadījumos, kad personas datu aizsardzības pārkāpuma rezultātā izpaustie dati ir šifrēti ar modernu algoritmu un šifra atslēgas konfidencialitāte nav skarta.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

[45] 29. panta darba grupas 2018. gada 6. februāra "Pamatnostādnēs par personas datu aizsardzības pārkāpumu paziņošanu saskaņā ar Regulu 2016/679": https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

Vai ziņojot par datu aizsardzības pārkāpumu uzraudzības iestādei ir jānorāda arī konkrētu klientu identitāte, kurus skar datu aizsardzības pārkāpums?

Regula neuzliek par pienākumu informēt uzraudzības iestādei par konkrētām personām, kuras datu aizsardzības pārkāpums ir skāris, bet norādīt datu subjektu kategorijas un aptuveno datu subjektu skaitu, kuras datu aizsardzības pārkāpums varētu būt skāris.

Vai par datu aizsardzības pārkāpumu ir jāziņo, ja tas ir novērsts?

Fakts, ka datu aizsardzības pārkāpums ir novērsts, pats par sevi nevar būt atbrīvojošs priekšnoteikums ziņošanai uzraudzības iestādei par datu aizsardzības pārkāpumu, jo datu aizsardzības pārkāpumu novēršana negarantē, ka tas būtiski neietekmēs datu subjektus, kuru dati tika skarti datu aizsardzības pārkāpuma ietvaros, kā arī ziņošanai ir papildu nolūks – ļaut uzraugošai institūcijai kontrolēt kredītiestādes veiktās darbības, lai šādi datu aizsardzības pārkāpumi turpmāk neatkārtotos.

Kādā termiņā par datu aizsardzības pārkāpumu jāziņo uzraudzības iestādei?

Regulas 33. panta pirmā daļa nosaka, ka personas datu aizsardzības pārkāpuma gadījumā pārzinim jāziņo par pārkāpumu uzraudzības iestādei bez nepamatotas kavēšanās un, ja iespējams, ne vēlāk kā 72 stundu laikā no brīža, kad pārkāpums tam kļuvis zināms.

Tikšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR darba grupu 2018. gada 21. maijā Datu valsts inspekcija pauda viedokli, ka saskaņā ar 29. panta darba grupas Tehnoloģiju apakšgrupas viedokli, par personas datu aizsardzības pārkāpuma 72 stundu laika brīža atskaites punktu būtu uzskatāms brīdis, kad pārzinis ir konstatējis personas datu aizsardzības pārkāpumu. Līdz ar to pārzinis Datu valsts inspekcijai nekavējoties iesniedz Sākotnējo ziņojumu un turpina izvērtēt visus notikuma (incidenta) apstākļus un veic pasākumus, lai mazinātu un novērstu pārkāpuma sekas.

Papildus Datu valsts inspekcija uzskata, ka pārzinim būtu jāvadās no saviem apsvērumiem, vērtējot 72 stundu laika brīdi. Tomēr šaubu gadījumā, par incidentu būtu jāziņo pēc iespējas ātrāk. DVI ieskatā, par incidentu būtu jāziņo tiklīdz pārzinim ir kļuvušas zināmas atbildes uz Regulas 33. panta 3. punktā ietvertajiem jautājumiem. DVI vērš uzmanību uz to, ka novēlotas ziņošanas gadījumā pārzinim ir pienākums norādīt kavēšanās iemeslus. Tāpat pārzinim ir pienākums dokumentēt noteiktā incidenta izvērtēšanu.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Kam būtu jāziņo par datu aizsardzības pārkāpumu?

Tikšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR Darba grupu 2018. gada 21. maijā Datu valsts inspekcija vērsa uzmanību, ka saskaņā ar Regulas 33. panta pirmo daļu pienākums ziņot par personas datu aizsardzības pārkāpumiem ir datu pārzinim. Gadījumos, kad pārzinis ir reģistrēts Eiropas Savienības dalībvalstī un Latvijā ir atvērta filiāle, par pārkāpumu būtu jāziņo vadošajai uzraudzības iestādei, kuras jurisdikcijā būs notikušā datu aizsardzības pārkāpuma izmeklēšana, kā arī citām iesaistītām iestādēm. Personas datu apstrādes aizsardzības ziņojuma veidlapā[46] ir paredzēta sadaļa "Pārrobežu un citi paziņojumi", kurā datu pārzinis norāda informāciju vai paziņojums ir pārrobežu paziņojums, kas nosūtīts vadošajai uzraudzības iestādei un ka datu pārzinim ir jāinformē citas iesaistītās iestādes, norādot ES valstu sarakstu, uz kurām pārkāpums attiecas.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 75., 76., 77., 85., 86., 87. un 88. apsvērumā un Regulas 33. un 34. pantā, kā arī 29. panta darba grupas 2018. gada 6. februāra "Pamatnostādnēs par personas datu aizsardzības pārkāpumu paziņošanu saskaņā ar Regulu 2016/679"[47]

(Ar grozījumiem, kas izdarīti 08.01.2021.)

[46] Personas datu apstrādes aizsardzības paziņojuma veidlapa, Datu valsts inspekcija. Pieejams: https://www.dvi.gov.lv/lv/personas-datu-apstrades-aizsardzibas-parkapuma-pazinojuma-iesniegsana/

[47] 29. panta darba grupas 2018. gada 6. februāra "Pamatnostādnēs par personas datu aizsardzības pārkāpumu paziņošanu saskaņā ar Regulu 2016/679": https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

6.5. Tehnisko resursu izmantošanas ieteikumi

Šīs apakšnodaļas ieteikumi izstrādāti, pieņemot ka kredītiestāde un tās sistēmas izpilda Finanšu un kapitāla tirgus komisijas 2015. gada 7. jūlija normatīvos noteikumus Nr. 112 "Finanšu un kapitāla tirgus dalībnieku informācijas sistēmu drošības normatīvie noteikumi". Šie noteikumi primāri nosaka prasības informācijas sistēmu aizsardzības procedūrām un tehniskajiem risinājumiem, kas aizsargā pret ārēju apdraudējumu.

Saskaņā ar Regulu, lai nodrošinātu datu apstrādes drošību atbilstoši riska (*piemēram, nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem*) lielumam, papildus augstākminētajos noteikumos izteiktajām prasībām kredītiestādei būtu nepieciešams nodrošināt minētos pasākumus:

1) datu pseidonimizāciju un šifrēšanu;
2) spēju nodrošināt apstrādes sistēmu un pakalpojumu nepārtrauktu konfidencialitāti, integritāti, pieejamību un noturību;
3) spēju laicīgi atjaunot datu pieejamību un piekļuvi tiem gadījumā, ja ir noticis fizisks vai tehnisks negadījums;
4) procesu regulāra tehnisko un organizatorisko pasākumu efektivitātes testēšanu, izvērtēšanu un novērtēšanu, lai nodrošinātu apstrādes drošību.

Šajā aspektā ietilpst gan visu tīkla aizsardzības pasākumu izvērtēšana (ugunsmūri, anti vīrusu programmas, pārsūtīšanas satura šifrēšana, informācijas atspoguļošana uz pārnēsājamām ierīcēm, to dzēšana, ja ierīce tiek nozagta vai pazaudēta utt., *backup* risinājumi, lai nodrošinātu, ka dati nepazūd utt.), gan arī fiziskās aizsardzības pasākumi (servera telpu fiziska aizsardzība pret ielaušanos, servera aizsardzība plūdu gadījumā, pārnēsājamo datu nesēju aizsardzība – *USB Flash*, panēsājamie cietie diski, CD/DVD utt). Tāpat arī jāizvērtē būtu lietotāju identifikācijas kārtība, vai tā ir pietiekami droša, iespējams, jāizvērtē, vai nav nepieciešamība pēc divu līmeņu identifikācijas – paroles un fiziskās klātbūtnes (*piemēram, ID kartes*).

Kredītiestādei jānodrošina katras atsevišķas IT sistēmas, kas iesaistīta datu apstrādē, dokumentācija un tās regulāra pārskatīšana un atjaunošana.

Izvērtēšanai ir jāpakļauj šādi elementi, kas var ietekmēt sistēmas drošību un tajā esošos datus:

1) nodrošināt, ka tikai pilnvarotas personas piekļūst informācijas resursiem (*piemēram, portatīviem datoriem, USB, planšetēm*);
2) jebkuru apstrādes darbību veic tikai attiecīgi pilnvarotas personas;
3) informācijas saglabāšana par veiktajām darbībām ar datiem (*piemēram, ievietošana, labošana, dzēšana, nodošana apstrādātājam, nodošana trešajām personām, nodošanas laiku, personu, kas saņēmusi informāciju*);
4) nodalīt dažādas datu kategorijas pēc to nozīmības, būtiskuma (*piemēram, "parastie dati" un īpašu kategoriju dati (informācija par veselības stāvokli)*) un spēt nodalīt pieejas;
5) nodrošināt, ka informācijas nesēji (DVD, CD, USB, cietie diski) tiek iznīcināti pilnībā un neatgriezeniski, kā arī to, ka iznīcināšanu veic tikai pilnvarotas personas;
6) paroles garumus un uzbūves nosacījumus (atbilstoši jaunākajām drošības tendencēm) izvērtēšana;
7) rīcība, ja lietotāja parole ir kļuvusi zināma trešajai personai (*piemēram, lietotāja pieejas nekavējoša bloķēšana*);
8) datu segmentācija, nodalot aktīvi izmantojamo datu bāzi no pasīvi izmantojamās, iespējams, otrajai ierobežojot pieejas, tādējādi nodrošinoties, gadījumiem, ja tiks nelikumīgi "iegūta" aktīvi izmantojamā datu bāze, tomēr daļa no informācijas, kas tiek glabāta pasīvajā datu bāzē, tiks saglabāta drošībā.
9) risku identificēšana, izvērtēšana un attiecīgu risinājumu piemeklēšana, lai riskus novērstu;
10) datu drošība ārpus biroja (*piemēram, šifrēšana, attālināta datu dzēšana*);
11) programmu atjauninājumi.

Datu apstrādei "mākonī" jāizvērtē, vai nav nepieciešams drošības audits, vai nepieciešams ieviest komunikācijas šifrēšanu, sevišķus pasākumus datu aizsardzībai, ja sadarbība tiek izbeigta (*piemēram, datu dzēšana, atgriešana, rezerves kopiju dzēšana*).

Ja kredītiestādei ir zudis tiesiskais pamats turpmākai datu izmantošanai un apstrādei ikdienas pakalpojumu sniegšanai, bet ir saglabājies vai radies kāds cits tiesiskais pamats, *piemēram, klients atteicies no kredītiestādes pakalpojumiem, bet jāglabā dati grāmatvedības vajadzībām*, tad būtu nepieciešams liegt plašu piekļuvi šādu klientu datiem informācijas sistēmās. Iespējamie mehānismi būtu datu pseidomizācija un attiecīgas klienta ieraksta arhīva kopijas izveide, kurai piekļuve nodrošināma tikai īpašos gadījumos, *piemēram, atbilstoši tiesībsargājošo un uzraudzības institūciju pieprasījumiem*.

Datu šifrēšana

Minimālais ieteicamais līmenis būtu nodrošināt, ka tiek šifrēti:

1) visi datu nesēji uz kuriem tiek vai potenciāli var tikt uzglabāti personas dati un kuri var kļūt publiski pieejami (piemēram, pārnēsājamās USB atmiņas ierīces);
2) potenciāli personas datus saturoša datu pārraide, izmantojot publiskos elektroniskos sakaru tīklus.

Tādejādi nodrošinot, ka šie dati nevar tikt nejauši nodoti neautorizētai personai. Šo tehnisko kontroli būtu ieteicams attiecināt vismaz uz tiem kredītiestādes darbiniekiem, kuri piekļūst vai ir tiesīgi iegūt no informācijas sistēmām datus, kā arī uz attiecīgajām informācijas sistēmām un to izmantotajiem datu nesējiem.

Vienots mehānisms klienta datu nodošanai citam tirgus dalībniekam

Regula paredz iespēju datu subjektam pieprasīt datu pārnešanu no viena tirgus dalībnieka pie otra. Ieteicamais mehānisms būtu izveidot vienotu strukturētu datu formātu, piemēram, XML (*eXtensible Markup Language*), kas ļautu eksportēt pilnu klienta datu kopu vienlaicīgi gan subjektam, gan informācijas sistēmai saprotamā formā, nodrošinot nepieciešamos datu aizsardzības mehānismus drošai šo datu pārnešanai.

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 74., 75., 76., 77., 78. un 83. apsvērumā un Regulas 24., 25. un 32. pantā.

7. APSTRĀDĀTĀJS

7.1. Apstrādātāja statuss un atbildības sadalījums

Kas ir apstrādātājs?

Par apstrādātāju uzskatāms ir kredītiestādes sadarbības partneris (fiziska vai juridiska persona, iestāde vai cita nošķirta struktūra), kura kredītiestādes vārdā un interesēs apstrādā datus, pamatojoties uz rakstveida līgumu, *piemēram, kredītiestādē par apstrādātāju būtu uzskatāms kredītiestādes sadarbības partneris, kurš nodrošina savu serveru iznomāšanu kredītiestādes datu glabāšanai; tulkošanas pakalpojumu sniedzējs, ja partnerim tiek nodoti tulkošanai tādi dokumenti, kas satur datus; kurjera pakalpojumu sniedzēji*, ja tiem tiek atklāti sūtījumā esošie personas dati to tālākai apstrādei; *kredītiestāžu piesaistīti sadarbības partneri (aģenti), kas nodrošina klientu identifikāciju vai komunikāciju ar klientu*.

Apstrādātājs ir uzskatāms par pārziņa "iekšējā lokā" esošu personu, tādēļ apstrādātājam, apstrādājot kredītiestādes datus, nav nepieciešams atšķirīgs tiesiskais pamats no tā, ar kuru datu apstrādi pamato pārzinis, bet pārzinim ir jāuzņemas atbildība par apstrādātāja veiktajām darbībām kredītiestādes uzdevumā.

Atsevišķos gadījumos arī kredītiestāde var būt apstrādātāja statusā citam pārzinim, piemēram, apdrošināšanas starpniecības ietvaros piedāvājot klientiem citu uzņēmumu sniegtos dzīvības vai nedzīvības apdrošināšanas pakalpojumus.

Šaubu gadījumos, kad kredītiestāde vēlas skaidri definēt savu vai sadarbības partnera tiesisko statusu attiecībā uz kādu datu apstrādi, ir iespējams konsultēties ar uzraudzības iestādi.

Noteiktajos gadījumos pakalpojuma sniedzējs netiek uzskatīts par apstrādātāju. Piemēram, par kredītiestādes apstrādātāju nebūtu uzskatāmi zvērinātie notāri, jo notārs neapstrādā personas datus kredītiestādes vārdā vai kredītiestādes noteikto personas datu apstrādes nolūku ietvaros, bet gan pilda funkcijas, kuras ir noteiktas Notariāta likumā. Faktiski notāra veiktās personas datu apstrādes nolūki ir noteikti Notariāta likumā, kredītiestāde vēršas pēc juridiska pakalpojuma, kuru notārs pilda saskaņā ar saviem profesionālajiem pienākumiem. Minētajā gadījumā gan kredītiestāde, gan notārs ir pārzinis, un abiem ir savi pienākumi attiecībā uz personas datu apstrādi kā pārziņiem. Līdzīgu viedokli ir pauduši Lielbritānijas datu aizsardzības iestāde (angļu val. – Information Commissioner's Office, ICO) savās Vadlīnijās "Pārzinis un apstrādātājs: kāda ir atšķirība un kādas ir pārvaldības sekas"[48].

Par apstrādātāju nebūtu jāuzskata arī zvērināti advokāti vai juristi, kuri apstrādā personas datus saistībā ar klientu juridisko pārstāvību.[49] Tāpat par neatkarīgiem pārziņiem ir uzskatāmi zvērinātie revidenti vai zvērinātu revidentu komercsabiedrība – apstrādājot personas datus revīzijas ietvaros, saskaņā ar rakstveidā noslēgto revīzijas pakalpojumu līgumu.[50]

(Ar grozījumiem, kas izdarīti 08.01.2021.)

[48] Information Commissioner's Office, "Data controllers and data processors: what the difference is and what the governance implications are": https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf, page 12.
[49] Sk.: 29. panta darba grupas 2010. gada 16. februāra "Atzinums 01/2010 par "datu pārziņa" un "datu apstrādātāja" jēdzienu", 28.lpp.: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_lv.pdf
[50] Datu valsts inspekcija, Par revidenta statusu sniedzot revīzijas pakalpojumus, 29.01.2019.: https://www.dvi.gov.lv/lv/zinas/par-revidenta-statusu-sniedzot-revizijas-pakalpojumus/

Tabula Nr. 14

Kurš ir atbildīgs par Regulas pārkāpumiem?

Atbildības veids	Pārzinis	Apstrādātājs
		Tikai, ja apstrādātājs nav izpildījis tam Regulā adresētos pienākumus vai rīkojies pretēji pārziņa likumīgiem norādījumiem.
Kaitējums datu subjektam, kas nodarīts ar apstrādi, kas pārkāpj Regulu	✓	✓
Administratīvā naudas soda piemērošana	✓	✓

Apstrādātāja atbildība

Apstrādātāja atbildība attiecībā uz likumīgu datu apstrādi var izpausties divos veidos, ja apstrādātājs neievēro kredītiestādes norādījumus saistībā ar datu apstrādi vai ja apstrādātājs neizpilda Regulā tieši uz apstrādātāju attiecināmos pienākumus. Neskatoties uz starp pārzini un apstrādātāju noslēgtā līguma noteikumiem, apstrādātājam ir arī šāda Regulā noteiktā tiešā atbildība, apstrādājot datus pārziņa uzdevumā, *piemēram*:

1) *bez pārziņa rakstveida piekrišanas neizmantot apakšapstrādātājus*;
2) *sadarboties ar uzraudzības iestādi, ja tiek veikta pārziņa apstrādāto datu likumības pārbaude*;
3) *nodrošināt datu drošību, tos apstrādājot*;
4) *kārtot apstrādātāja rīcībā nodoto datu apstrādes reģistru*;
5) *informēt pārzini par incidentiem (t.sk. datu aizsardzības pārkāpumiem), kas skar pārziņa atbildībā esošus datus*;
6) *piesaistīt datu aizsardzības speciālistu, ja tas nepieciešamas saskaņā ar Regulas prasībām*.

Vai kredītiestāde var ar līgumu nodot atbildību apstrādātājam?

Nē, pārzinis saglabā atbildību gan iespējamās administratīvās atbildības gadījumā, gan arī iespējamo datu subjektu prasījumu gadījumā. Pret apstrādātāju kredītiestāde var vērsties regresa kārtībā.

7.2. Apstrādātāja izvēle un līguma noslēgšana

Kredītiestādē jābūt izstrādātam iekšējam regulējumam, kas nosaka kārtību kā veicama un uzraugāma datu apstrāde, kas veikta iesaistot apstrādātāju. Kredītiestādei jānodrošina, ka apstrādātājs spēj nodrošināt vismaz tādu pašu datu aizsardzības līmeni, kādu attiecīgām datu kategorijām nodrošina pati kredītiestāde.

Kredītiestādei jānodrošina apstrādātāju veikto datu apstrāžu pārvaldība, kas definē veicamās aktivitātes visa apstrādātāja veikto datu apstrāžu pārvaldības dzīves cikla laikā. Datu apstrādes pārvaldība attiecināma gan uz ārējiem, gan iekšējiem (grupas ietvaros) pakalpojumu sniedzējiem.

Apstrādātāju veikto datu apstrāžu pārvaldības dzīves ciklam jāiekļauj šādas aktivitātes, kuru veikšanu nepieciešams dokumentēt līguma īpašniekam vai kādam citam apstiprinātam atbildīgajam:

1. **padziļināta izpēte** – potenciālā apstrādātāja sākotnējā izpēte par apstrādātāja kompetenci un pieredzi, finansiālo stāvokli, iekšējo kontroles vidi, informācijas sistēmu pārvaldības ietvaru, esošajām sertifikācijām, iespējamo interešu konfliktu un citiem kritērijiem, kurus kredītiestāde apstiprinājusi kā kritērijus izvēloties apstrādātāju. Izpētes ietvaros būtu jāiekļauj potenciālo risku un materialitātes novērtējuma veikšana.

2. **līguma sagatavošana** – sagatavojot līgumu, vēlams izvērtēt šādus aspektus un pārliecināties par attiecīgu risku kontroli:

    a) apstrādātāja darbības novērtēšanas kritēriji un potenciālā rīcība neizpildes gadījumā;
    b) datu apstrādes nosacījumi;
    c) saistības attiecībā uz informācijas drošību un IT operāciju nodrošināšanu;
    d) apstrādātāja darbībā iesaistītie apakšuzņēmumi un to funkcijas pakalpojuma sniegšanas ietvaros;
    e) datu glabāšanas un datu atrašanās vieta;
    f) vai līguma pārtraukšana neietekmēs pakalpojuma sniegšanas nepārtrauktību un kvalitāti;
    g) pārzinim un tā revidentiem ir piekļuves tiesības informācijai, kas nodrošina pakalpojuma sniegšanu un pēc laicīga paziņojuma saņemšanas apstrādātājs nodrošina piekļuvi apstrādātāja telpām un citai informācijai, kas nodrošina pakalpojuma izpildi;
    h) pienākums laicīgi informēt par notikumiem, kas varētu būtiski ietekmēt spēju sniegt pakalpojumu efektīvi atbilstoši līguma nosacījumiem;
    i) pienākumu sniegt IT pārvaldību raksturojušu dokumentāciju, kā arī pēc nepieciešamības trešo pušu veiktu pārbaužu rezultātus (piemēram, ārējā audita ziņojumi, IT drošības auditi utt.).

3. **lēmuma pieņemšana un līguma parakstīšana** – lēmuma par līguma slēgšanu ar apstrādātāju pieņemšanā ieteicams iesaistīt atbildīgās struktūrvienības, piemēram, personāla daļas, ja tiek slēgts līgums par algas aprēķina pakalpojuma sniegšanu. Kredītiestādei jānodrošina iekšēja apstrādātāju reģistra uzturēšana un aktualizēšana, lai kontrolētu un uzskaitītu piesaistītos apstrādātājus.

4. **novērtēšana un ziņošana** – ieteicams regulāri veikt apstrādātāja sniegtā pakalpojuma kvalitātes un efektivitātes izvērtēšanu, novērtējot tādus aspektus kā incidenti un to ietekme uz kredītiestādi, jāpieņem lēmums par turpmāko rīcību (turpināt sadarbību, veikt izmaiņas līguma nosacījumos, pārtraukt līgumu).

Eiropas Banku iestāde (angļu val. *European Banking Authority, EBA*) ir izstrādājusi darba vadlīnijas ārpakalpojumu pārvaldībai attiecībā uz mākoņpakalpojumu sniedzējiem (EBA/REC/2017/03), kuras ieteicams ņemt vērā ārpakalpojuma pārvaldības procesa nodrošināšanai.[51]

(Ar grozījumiem, kas izdarīti 08.01.2021.)

[51] Sk.: Eiropas Banku iestāde, Ieteikumi mākoņpakalpojumu izmantošanai: https://eba.europa.eu/sites/default/documents/files/documents/10180/2170125/47c9c6b5-c20f-4665-90d4-f07ed0f8b261/Recommendations%20on%20Cloud%20Outsourcing%20(EBA-Rec-2017-03)_LV.pdf

Kas jāņem vērā izvēloties apstrādātāju?

Jāizvēlas tikai tādi apstrādātāji, kas sniedz pietiekamas garantijas, ka tiks īstenoti atbilstoši tehniskie un organizatoriskie pasākumi, lai nodrošinātu Regulas prasību izpildi un datu subjektu aizsardzību. Apstrādātājs sniegtās garantijas var pamatot arī ar pievienošanos un atbilstību apstiprinātam rīcības kodeksam vai sertifikācijas mehānismam.

Rakstiska līguma nepieciešamība

Rakstisks līgums starp kredītiestādi un apstrādātāju ir obligāti nepieciešams, pretējā gadījumā apstrādātājs tiks uzskatīts par trešo personu jeb citu pārzini un datu nodošanai būs nepieciešams kāds no tiesiskiem pamatiem. Ņemot vērā to, ka apstrādātājs darbojas kredītiestādes interesēs un uzdevumā, rakstveida līgums palīdzēs abām pusēm izprast savas tiesības un pienākumus saistībā ar rīcību ar datiem, kuri nodoti apstrādātājam apstrādei. Rakstveida līgums ir nepieciešams arī gadījumos, ja apstrādātājs nodod atsevišķas apstrādes darbības apakš-apstrādātājam, šajā gadījumā būtu jānodrošina, ka līgumā ar apakš-apstrādātāju ir ietverti vismaz tādi paši noteiktumi kādi ir ietverti līgumā ar apstrādātāju.

Tikšanās laikā ar Latvijas Finanšu nozares asociācijas GDPR darba grupu 2018. gada 21. maijā Datu valsts inspekcija pauda viedokli, ka Regula neuzliek par pienākumu pārzinim slēgt atsevišķu datu apstrādes līgumu ar apstrādātāju. Apstrādi, ko veic apstrādātājs, var reglamentēt arī ar sadarbības līgumu. Tāpat līgumā starp pārzini un apstrādātāju, nav obligāti jāparādās apzīmējumam "pārzinis" vai "apstrādātājs", bet drīzāk ir jābūt skaidram lomu sadalījumam un uzdevumu aprakstam. Katrs līgums tiks vērtēts no gadījuma uz gadījumu (case by case), ņemot vērā tā būtību un funkcionalitāti.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Tabula Nr. 15

Kādas prasības būtu jānosaka līgumā ar apstrādātāju?

Līgumā iekļaujamā informācija	Regulas noteiktās minimālas prasības	Papildu ieteikumi
1. Līguma priekšmets	☐	☐
2. Datu apstrādes plānotais ilgums (līguma termiņš)	☐	☐
3. Datu apstrādes raksturs un nolūks	☐	☐
4. Apstrādei uzticēto datu veids	☐	☐
5. Apstrādei nodoto datu subjektu kategorijas	☐	☐
6. Kredītiestādes tiesības un pienākumi:		☐
▪ rakstveidā sniegt saistošus norādījums par datu apstrādei piemērojamiem tehniskiem un organizatoriskiem pasākumiem		☐
▪ kontrolēt apstrādātāja spēju izpildīt līgumu un savus pienākumus, kā arī nodrošināt datu drošību;		☐
▪ vienpusēji izbeigt līgumu, ja apstrādātājs nepilda uzņemtās saistības vai neveic pietiekamus pasākumus datu aizsardzībai;		☐
7. Apstrādātāja pienākumi:	☐	
▪ datus apstrādāt tikai pēc kredītiestādes dokumentētiem norādījumiem (izņemot, ja to pieprasa ES vai dalībvalsts tiesību akti, kas piemērojami apstrādātājam);	☐	
▪ informēt kredītiestādi par apstrādes faktu pirms apstrāde ir uzsākta, ja apstrādātājam saskaņā ar tam piemērojamiem tiesību aktiem ir pienākums veikt kredītiestādes nodoto personu datu apstrādi;	☐	

▪ nodrošināt, ka personas, kuras ir iesaistītas apstrādē, ir apņēmušās ievērot konfidencialitāti, izņemot, ja šāds pienākums ir noteikts ar likumu;	☐	
▪ nodrošināt, ka personas, kuras ir iesaistītas apstrādē, neapstrādā datus bez vai neatbilstoši pārziņa norādījumiem;	☐	
▪ īstenot atbilstīgus tehniskus un organizatoriskus pasākumus, lai nodrošinātu tādu drošības līmeni, kas atbilst novērtētam riskam, piemēram: • veikt datu pseidonimizāciju un šifrēšanu; • nodrošināt apstrādes sistēmu un pakalpojumu nepārtrauktu konfidencialitāti, integritāti, pieejamību un noturību; • laicīgi atjaunot datu pieejamību un piekļuvi tiem gadījumā, ja noticis fizisks vai tehnisks negadījums; • regulāru tehnisko un organizatorisko pasākumu testēšanu, izvērtēšanu un novērtēšanu, lai nodrošinātu datu apstrādes drošību;	☐	
▪ bez iepriekšējas konkrētas kredītiestādes rakstiskas atļaujas nepiesaistīt citu apstrādātāju, vai, ja līgumā kredītiestāde ir atļāvusi cita apstrādātāja patstāvīgu piesaisti, nekavējoties, tiklīdz zināms par cita apstrādātāja piesaisti, informēt par to kredītiestādi, lai tā varētu nepieciešamības gadījumā iebilst pret šāda apstrādātāja piesaisti;	☐	
▪ papildus apstrādātāja (apstrādātāja apakšuzņēmuma) piesaistes gadījumā nodrošināt, ka papildus apstrādātājs ievēro visus tos pašus pienākumus attiecībā uz kredītiestādes datu apstrādi, kādi ir noteikti primāram apstrādātājam;	☐	
▪ ņemot vērā nodoto datu apstrādes raksturu, sniegt kredītiestādei atbalstu atbildēt uz datu subjektu pieprasījumiem un nodrošināt datu subjektu tiesību īstenošanu;	☐	
▪ ņemot vērā nodoto datu apstrādes raksturu un pieejamo informāciju, sniegt kredītiestādei atbalstu datu apstrādes drošības nodrošināšanā;	☐	
▪ nekavējoties paziņot kredītiestādei par datu aizsardzības pārkāpuma konstatēšanu;	☐	
▪ ņemot vērā nodoto datu apstrādes raksturu un pieejamo informāciju, sniegt kredītiestādei atbalstu datu aizsardzības pārkāpumu fiksēšanā un paziņošanā uzraudzības iestādei un/vai datu subjektam;	☐	
▪ ņemot vērā nodoto datu apstrādes raksturu un pieejamo informāciju, sniegt kredītiestādei atbalstu novērtējuma par ietekmi uz datu aizsardzību veikšanā un/vai iepriekšējās apspriešanās ar datu uzraudzības iestādi nodrošināšanā;	☐	
▪ pēc pakalpojuma sniegšanas pabeigšanas saskaņā ar kredītiestādes norādījumiem dzēst vai atdot visus datus (dzēšot visas kopijas) kredītiestādei, ja vien ES vai dalībvalsts tiesību akti neparedz datu saglabāšanu;	☐	
▪ sniegt kredītiestādei visu informāciju, lai apliecinātu apstrādes darbību atbilstību Regulai;	☐	
▪ nodrošināt revidentiem piekļuvi apstrādātāja telpām un informācijai, kā arī sniegt skaidrojumus revidentiem nodoto datu apstrādes procesu revīzijas veikšanai;	☐	
▪ iecelt datu aizsardzības speciālistu (ja tas nepieciešams saskaņā ar Regulas noteikumiem)	☐	
▪ sadarboties ar uzraudzības iestādi, ja tā īsteno savas izmeklēšanas pilnvaras, t.sk. nodrošināt piekļuvi apstrādātāja telpām, kur tiek veikta nodoto datu apstrāde;	☐	
▪ informēt kredītiestādi par jebkuru saņemto datu subjekta pieprasījumu saistībā ar nodoto datu apstrādi;		☐
▪ apmācīt apstrādātāja darbiniekus par datu aizsardzības jautājumiem un kredītiestādes norādījumiem attiecībā uz nodoto datu apstrādi;		☐

(Ar grozījumiem, kas izdarīti 08.01.2021.)

Saskaņā ar Kredītiestāžu likuma 10.[1] pantu atsevišķi līgumi ar datu apstrādātājiem ir jāsaskaņo ar Finanšu un kapitāla tirgus komisiju, kā arī šajā gadījumā jāiekļauj papildus minētajā normā minētie noteikumi.

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 81., 82., 83. un 95. apsvērumā un Regulas 28., 29. un 32. pantā, kā arī EDAK 2020. gada 2. septembra "Pamatnostādnēs 07/2020 par pārziņa un apstrādātāja jēdzienu VDAR kontekstā"[52].

[52] EDAK 2020. gada 2. septembra "Pamatnostādnes 07/2020 par pārziņa un apstrādātāja jēdzienu VDAR kontekstā": https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf (angļu val.)

8. DATU AIZSARDZĪBAS SPECIĀLISTS

8.1. Datu aizsardzības speciālista kvalifikācijas un garantijas

Datu aizsardzības speciālista kvalifikācija

Datu aizsardzības speciālistu ieceļ, pamatojoties uz viņa profesionālo kvalifikāciju, jo īpaši speciālām zināšanām datu aizsardzības tiesību un prakses jomā, un spēju pildīt Regulā noteiktos uzdevumus. Par datu aizsardzības speciālistu var nozīmēt personu, kura atbilst spēkā esošo normatīvo aktu prasībām.

Visatbilstošākie kandidāti datu aizsardzības speciālista amatam būtu juristi ar specializāciju datu aizsardzības un IT tehnoloģiju jomā vai arī sertificēti informācijas sistēmu auditori ar specifiskām zināšanām datu aizsardzības tiesību un prakses jomā.

Datu aizsardzības speciālistam ir jāspēj neatkarīgi veikt kredītiestādes datu apstrādes izvērtējums, neskatoties uz to, vai datu aizsardzības speciālists ar kredītiestādi ir noslēdzis darba līgumu vai pakalpojumu līgumu, kā arī jāpalīdz kredītiestādei vai kredītiestādes sadarbības partnerim uzraudzīt, kā kredītiestādes iekšējos procesos un darbībās tiek ievērotas Regulas prasības.

Ir pieļaujams norīkot vairākus personas datu aizsardzības speciālistus, kā arī datu aizsardzības speciālists var veidot profesionāļu komandu, kas spēj nodrošināt Regulas prasību ievērošanu kredītiestādes darbībā, tajā skaitā datu aizsardzības speciālista vietā komunicēt ar datu subjektiem un sadarboties ar uzraudzības iestādi.

Datu aizsardzības speciālists uzskatāms par autonomu uzraugu datu aizsardzības jomā, jo datu aizsardzības pārvaldības sistēmā tam ir nozīmīga loma, ņemot vērā izvirzītos nosacījumus iecelšanai (noteikti konkrēti gadījumi, kad datu aizsardzības speciālista iecelšana ir obligāta, kā arī profesionālās kvalifikācijas prasības), amatam (atbildīgs un neatkarīgs diskusiju dalībnieks par dažādiem datu jautājumiem) un uzdevumiem (uzraugot Regulas prasību ievērošanu, informējot un sniedzot konsultācijas, sadarbojoties ar uzraudzības iestādēm u.c.). Turklāt kredītiestādēm jānodrošina, lai datu aizsardzības speciālists un viņa komanda savus uzdevumus varētu veikt efektīvi arī gadījumos, kad vairākām kredītiestādēm, struktūrām ir iecelts viens datu aizsardzības speciālists.

Datu aizsardzības speciālista statuss

Kredītiestādēm jāņem vērā, ka datu aizsardzības speciālistam nevar tikt dotas norādes saistībā ar viņa uzdevumu veikšanu, turklāt datu aizsardzības speciālists ir tieši atbildīgs kredītiestādes augstākās vadības priekšā. Līdz ar to datu aizsardzības speciālistam kredītiestādē nodrošināms tāds statuss, lai viņa dalība un viedoklis par datu jautājumiem tiktu pienācīgi novērtēts un uztverts kā svarīga un neatņemama ikviena procesa daļa. Tādējādi datu aizsardzības speciālista autoritārā statusa nodrošināšanai kredītiestādēm jāievēro, ka:

1. datu aizsardzības speciālists nodrošina ar datu aizsardzību saistīto aspektu izvērtēšanu kredītiestādē, konsultē kredītiestādi un datu subjektus ar datu aizsardzību saistītos jautājumos, kā arī sadarbojas ar uzraudzības iestādi datu aizsardzības jautājumus;

2. datu aizsardzības speciālistam ir saistoša konfidencialitātes ievērošana saistībā ar uzdevumu veikšanu;

3. datu aizsardzības speciālists, pildot savus pienākumus, pienācīgi ņem vērā ar apstrādes darbībām saistīto risku, ņemot vērā apstrādes raksturu, apjomu, kontekstu un nolūku;

4. datu aizsardzības speciālists tiek pienācīgi un laikus iesaistīts visos jautājumos saistībā ar datu aizsardzību;

5. datu aizsardzības speciālistam ir jāsaņem atbalsts tā uzdevumu izpildē, nodrošinot resursus, kas nepieciešami, lai veiktu uzdevumus, un nodrošinot piekļuvi datiem un apstrādes darbībām;

6. datu aizsardzības speciālists nesaņem nekādus norādījumus attiecībā uz tam uzdoto uzdevumu veikšanu un sagaidāmo rezultātu, t.sk. nesaņem norādījumus konkrētas interpretācijas vai izpratnes nodrošināšanai strīdus jautājumos;

7. datu aizsardzības speciālists var veikt arī citus pienākumus kredītiestādē, bet nodrošinot, lai netiktu radīts interešu konflikts;

8. datu aizsardzības speciālists ir tieši atbildīgs kredītiestādes augstākās vadības priekšā;

9. kredītiestāde nevar nodot atbildību par Regulas ieviešanu datu aizsardzības speciālistam. Atbilstības Regulai nodrošināšana ir kredītiestādes atbildība;

10. datu aizsardzības speciālistam piešķirams pietiekams darba laiks savu uzdevumu veikšanai;

11. datu aizsardzības speciālistam piešķirams pietiekams finanšu resursu, infrastruktūras un, ja nepieciešams, darbinieku nodrošinājums;

12. datu aizsardzības speciālistam nodrošināmas regulāras apmācības un kvalifikācijas uzturēšanas pasākumi;

13. nav iespējams datu aizsardzības speciālista funkcijas nodalīt tikai attiecībā uz kādu daļu no organizācijas datu apstrādes darbībām.

Datu aizsardzības speciālists var būt gan kredītiestādes darbinieks, gan arī var tikt piesaistīts kā ārpakalpojuma sniedzējs.

Tātad datu aizsardzības speciālists kredītiestādē ir augsti informēts, pietiekami nodrošināts ar nepieciešamajiem resursiem, autonoms lēmumu pieņemšanā un tieši atbildīgs par kredītiestādes augstākās vadības informēšanu par datu aizsardzības jautājumiem, sniedzot padomus un ieteikumus vai sagatavojot iesniegšanai darbību gada pārskatu.

Ņemot vērā, ka datu aizsardzības speciālists ir tieši atbildīgs kredītiestādes augstākās vadības priekšā, ir pieļaujams, ka datu aizsardzības speciālista darbības novērtēšanu kredītiestādes vadība īsteno ar kredītiestādes iekšējā audita palīdzību. Iekšējais audits var novērtēt datu aizsardzības speciālista darbību no procedurālā viedokļa, ievērojot datu aizsardzības speciālista neatkarīgo statusu, proti viņam nevar tikt dotas norādes saistībā ar uzdevumu veikšanu, nevērtējot datu aizsardzības speciālista sniegtās norādes un izteiktos viedokļus.

8.2. Interešu konfliktu novēršana

Datu aizsardzības speciālists var veikt arī citus pienākumus kredītiestādē, bet tādā gadījumā nepieciešams nodrošināt, ka datu aizsardzības speciālista darbībā nerodas interešu konflikts.

Kā viens no veidiem interešu konflikta novēršanai būtu paredzēt pilna laika noslodzi datu aizsardzības speciālista funkciju veicējam (vismaz datu aizsardzības speciālista pienākumu uzsākšanas pirmajā posmā).

Interešu konflikts varētu rasties gadījumos, kad datu aizsardzības speciālists veiktu pienākumus, kas var tiešā veidā ietekmēt organizācijas datu apstrādes darbības, kuras uzrauga datu aizsardzības speciālists.

Interešu konfliktu visticamāk radītu datu aizsardzības speciālista amata savienošana ar organizācijas augstāko vai vidējo vadību (*piemēram, izpilddirektors, operacionālais direktors, finanšu direktors, IT departamenta vadītājs, personāla departamenta vadītājs, juridiskā departamenta vadītājs, mārketinga departamenta vadītājs*), kā arī cita līmeņa speciālistiem, ja tiem ir tiesības noteikt datu apstrādes nolūkus un līdzekļus kredītiestādē.

Ja datu aizsardzības speciālists kredītiestādē veic arī citas funkcijas, tad šīs personas darbībai datu aizsardzības speciālista amatā jābūt atsevišķam uzdevumu plānam, kas nepārklājas ar citām funkcijām. Arī datu aizsardzības speciālista snieguma novērtējums nedrīkst būt saistīts ar snieguma vērtējumu citu pienākumu izpildē.

Pat ja datu aizsardzības speciālists ir piesaistīts kā ārpakalpojuma sniedzējs, tad interešu konflikts var rasties, ja šī pati persona veic arī citas darbības, kas skar datu aizsardzības jautājumus, *piemēram, pārstāv kredītiestādi tiesā sakarā ar datu aizsardzības pārkāpumu*.

8.3. Datu aizsardzības speciālista nozīmēšana un attiecību izbeigšana

Vai datu aizsardzības speciālists ir obligāts?

Datu aizsardzības speciālists ir obligāti ieceļams, ja pārziņa pamatdarbība sastāv no apstrādes darbībām, kurām to būtības, apmēra un/vai nolūku dēļ nepieciešama regulāra un sistemātiska datu subjektu novērošana plašā mērogā, kā arī ja pārziņa pamatdarbība ietver Īpašo kategoriju un datu par sodāmību un pārkāpumiem apstādi plašā mērogā.

Līdz ar to konstatējams, ka finanšu pakalpojumu sniegšana, ja tas tiek sniegts fiziskām personām, atbilst šiem kritērijiem un kredītiestādēm ir nepieciešams iecelt datu aizsardzības speciālistu. Ja kredītiestāde nesniedz finanšu pakalpojumus fiziskām personām, kredītiestādei jāizvērtē savas darbības atbilstība iepriekšminētajiem kritērijiem, lai konstatētu datu aizsardzības speciālista iecelšanas nepieciešamību.

Kopīgs datu aizsardzības speciālists uzņēmuma grupai

Kredītiestāžu grupa var iecelt kopīgu datu aizsardzības speciālistu vairākiem grupas uzņēmumiem, bet jāspēj nodrošināt, ka datu aizsardzības speciālists spēs veikt savus uzdevumus visās grupas ietvaros esošajās kredītiestādēs, nodrošinot darbinieku un datu subjektu piekļuvi datu aizsardzības speciālistam (*piemēram, valodas barjera, pieejamība uzreiz pēc nepieciešamības un bez kavēšanās*). Viens datu aizsardzības speciālists vairākām grupas uzņēmumiem ir pieļaujams, ja kredītiestādes ir ar līdzīgām funkcijām, ģeogrāfiski vai organizatoriski saistītas.

Datu aizsardzības speciālista aizvietošana un attiecību izbeigšana

Regulā nav noteikts, kā un kad datu aizsardzības speciālistu var aizvietot vai atlaist, vispārīgi nosakot, ka viņu nevar negodīgi atlaist vai piemērot sankcijas par viņa tiešo uzdevumu veikšanu. Proti, datu aizsardzības speciālistu nevar atlaist vai piemērot sankcijas (*piemēram, labumu nepiešķiršanu kopā ar citiem darbiniekiem vai karjeras attīstības aizkavēšanu*) par padoma sniegšanu attiecībā uz novērtējumu par ietekmi uz datu aizsardzību. Taču šāda padoma nesniegšana gadījumos, kad tas būtu jādara, var uzskatīt par darba līgumā vai pakalpojuma līgumā noteikto pienākumu pienācīgu nepildīšanu, par ko datu aizsardzības speciālistam var iestāties noteikta atbildība – sankcijas vai līgumattiecību izbeigšana.

Tādējādi datu aizsardzības speciālista atlaišanas iemesls var būt saistīts, piemēram, ar zādzību vai citu rupju kredītiestādes kā darba devēja noteikumu pārkāpumu saskaņā ar Darba likumā noteiktiem gadījumiem, kas nav tieši saistīti ar datu aizsardzības speciālista pienākuma izpildi. Savukārt gadījumā, kad datu aizsardzības speciālists sniedz pakalpojumus datu aizsardzības jomā pamatojoties uz noslēgto pakalpojuma līgumu, tā izbeigšanas nosacījumi ir atkarīgi no šajā līgumā noteiktām prasībām. Līdz ar to kredītiestādei ir tiesības uzraudzīt datu aizsardzības speciālistu, lai konstatētu tā pienākuma veikšanu atbilstoši noslēgtajam darba līgumam vai pakalpojuma līgumam.

Ievērojot datu aizsardzības speciālistam izvirzītās prasības un noteiktos pienākumus, kā arī Regulas prasības un Darba likumā darbiniekam noteiktās tiesības, iespējama datu aizsardzības speciālista aizvietošana viņa prombūtnē ar citu personu, kura atbilst datu aizsardzības speciālistam izvirzītajām prasībām.

Ja datu aizsardzības speciālista funkcijas tiek veiktas saskaņā ar pakalpojuma līgumu, kas noslēgts ar personu vai uzņēmumu, kas neietilpst kredītiestādes grupas uzņēmumos, svarīgi būtu pakalpojuma līgumā jau sākotnēji noteikt skaidrus pienākumus, sadalot konkrētas funkcijas konkrētām personām, un rīcību datu aizsardzības speciālista aizvietošanas gadījumā.

Datu aizsardzības speciālista aizvietošanas gadījumā jānodrošina, ka tiek ievērotas visas viņam izvirzītās prasības, tajā skaitā nerodas interešu konflikts, viegli sasniedzams pa norādīto kontaktinformāciju, kā arī negodīgi netiek piemērotas sankcijas un atlaišana. Taču katrā šādā gadījumā kredītiestādē atsevišķi izvērtējams aizvietošanas ilgums, datu aizsardzības jautājuma nozīme un iespējamā ietekme uz kredītiestādes lēmuma pieņemšanu.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

8.4. Datu aizsardzības speciālista uzdevumi

Datu aizsardzības speciālista uzdevumi un statuss:

1. informēt un konsultēt kredītiestādi un tās darbiniekus, kuri veic datu apstrādi, par viņu pienākumiem;

2. uzraudzīt, vai tiek ievērota Regula un citi tiesību akti (arī iekšējie normatīvie akti) par datu aizsardzību, tostarp pienākumu sadale, apstrādes darbībās iesaistīto darbinieku informēšana un apmācība, un ar to saistītās revīzijas;

3. ievākt informāciju, lai identificētu apstrādes procesus, analizēt un pārbaudīt apstrādes procesu atbilstību Regulai, un informēt, sniegt padomus un rekomendācijas kredītiestādei saistībā ar datu apstrādi;

4. pēc pieprasījuma sniegt padomus attiecībā uz novērtējumu par ietekmi uz datu aizsardzību un pārraudzīt tā īstenošanu;

5. sadarboties ar uzraudzības iestādi;

6. būt par uzraudzības iestādes kontaktpunktu jautājumos, kas saistīti ar apstrādi, t.sk. saistībā ar iepriekšējo apspriešanos u.c. jautājumiem;

7. konsultēt datu subjektus, kuri vērsušies pie datu aizsardzības speciālista.

Rekomendējams:

1. nodrošināt datu aizsardzības speciālistu ar augstākās vadības atbalstu savu uzdevumu veikšanai;

2. nodrošināt datu aizsardzības speciālistu dalību vidējā un augstākā līmeņa vadītāju sanāksmēs;

3. iesaistīt datu aizsardzības speciālistu jebkuru lēmumu pieņemšanā, kas skar datu aizsardzības jautājumus, kā arī nodrošināt iespēju iepazīties ar attiecīgiem dokumentiem, lai izteiktu viedokli un sniegtu padomu;

4. konsultēties ar datu aizsardzības speciālistu, ja iestājies datu aizsardzības pārkāpums;

5. skaidri definēt datu aizsardzības speciālista uzdevumus, statusu un funkcijas kredītiestādes iekšējos normatīvajos aktos vai amata aprakstā, kā arī ietvert attiecīgo noregulējumu līgumā ar datu aizsardzības speciālistu;

6. gadījumā, ja datu aizsardzības speciālists individuāli nav spējīgs paveikt visus noteiktos uzdevumus vai arī personai kādā jomā trūkst nepieciešamās speciālās zināšanas vai pieredze (piemēram, informācijas sistēmu pārbaudei), tad datu aizsardzības speciālistam ir iespējams veidot atsevišķu komandu, lai nodrošinātu nepieciešamo kapacitāti.

Lēmumu pieņemšana

Lēmumus par datu aizsardzības jautājumiem pieņem pati kredītiestāde, balsoties uz datu aizsardzības speciālista viedokli. Datu aizsardzības speciālists lēmumus nepieņem.

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 97. apsvērumā un Regulas 37., 38. un 39. pantā, kā arī 2016. gada 13. decembra 29. panta darba grupas rekomendācijā “Pamatnostādnes par datu aizsardzības speciālistiem (DAS)”.

9. DATU NODOŠANA ĀRPUS ES

ES, kur piemērojama Regula, datu subjektiem ir nodrošināts paaugstināts to tiesību aizsardzības līmenis, t.sk. kredītiestādei kā pārzinim nodrošinot likumīgu un samērīgu datu apstrādi, nodrošinot datu drošību, kā arī datu subjektam dodot iespēju kontrolēt savus datus, realizējot savas tiesības uz datu dzēšanu, labošanu, pārnesamību utt., kā arī nodrošinot efektīvu datu subjektu tiesību aizsardzību gan vēršoties uzraudzības institūcijās, gan arī vēršoties pie datu apstrādātājiem par nodarīto kaitējumu.

ES teritorijā datu subjektiem nodrošinātam tiesību aizsardzības līmenim nebūtu jāsamazinās arī gadījumos, ja dati dažādu nolūku dēļ (*piemēram, pakalpojumu sniegšanas, kredītiestādes leģitīmo interešu ievērošanai*) tiek nosūtīti pārziņiem, apstrādātājiem vai citiem saņēmējiem ārpus ES. Turklāt ar nosūtīšanu jāsaprot ne tikai datu nodošanu citam pārzinim vai apstrādātājam, kurš atrodas ārpus ES, bet arī datu izvietošanu (*piemēram, servera, kuros glabājas dati, izvietošana*) kredītiestādei piederošos infrastruktūras objektos valstīs, kas nav ES. Datu subjektiem ES nodrošināto tiesību aizsardzības līmeņa saglabāšanu var nodrošināt ar tālāk uzskaitītiem instrumentiem.

Ar Regulas normām personas datu aizsardzības jomā aktualizēti jau pastāvošie principi, lai tie atbilstu mūsdienu prasībām, tajā skaitā harmonizējot un izstrādājot vienotus nosacījumus un prasības datu nodošanai ārpus ES. Vienlaikus paredzēta iespēja izveidot sertifikācijas mehānismus, lai uzskatāmi parādītu, ka personas datu aizsardzības apstrādes darbības, ko veic pārziņi un apstrādātāji, atbilst Regulai, kā arī paredzēta iespēja pārziņiem izstrādāt vienotus rīcības kodeksus, lai veicinātu Regulas atbilstošu un vienveidīgu piemērošanu konkrētās nozarēs.

9.1. Pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību

Kredītiestāde drīkst nosūtīt datus uz trešo valsti, ja Eiropas Komisija ir nolēmusi, ka konkrētās valsts teritorija vai atsevišķi sektori, vai attiecīga starptautiskā organizācija nodrošina datiem pietiekamu aizsardzības līmeni.

Informāciju par Eiropas Komisijas pieņemtiem lēmumiem var noskaidrot Eiropas Komisijas mājas lapā: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

9.2. Pamatojoties uz atbilstošām garantijām

Ja kredītiestādei ir nepieciešams nosūtīt datus uz valsti ārpus ES, bet attiecībā uz kuru Eiropas Komisija nav pieņēmusi lēmumu par aizsardzības līmeņa pietiekamību, kredītiestāde drīkst nosūtīt datus uz trešo valsti vai starptautisko organizāciju, ja kredītiestāde sniedz atbilstošas garantijas un datu subjektam ir pieejami efektīvi tiesiskās aizsardzības līdzekļi un īstenojamas datu subjektu tiesības.

Kā nodrošināt atbilstošas garantijas?

Atbilstošas garantijas kredītiestāde var nodrošināt kādā no šādiem veidiem:

1. trešā valstī veiktai datu apstrādei vai datu saņēmējam piemērojot saistošos uzņēmuma noteikumus (*binding corporate rules*);
2. sadarbības līgumam piemērojot Eiropas Komisijas vai uzraudzības iestādes izstrādātas (un Eiropas Komisijas apstiprinātas) standarta datu aizsardzības klauzulas;
3. trešā valstī esošam datu saņēmējam vai apstrādātājam piemērojot saskaņā ar Regulu apstiprinātu rīcības kodeksu;
4. trešā valstī esošam datus saņēmējam vai apstrādātājam piemērojot saskaņā ar Regulu apstiprinātus sertifikācijas mehānismus;
5. piemērojot starp publiskām iestādēm vai struktūrām juridiski saistošu un tiesisku instrumentu;
6. saņemot uzraudzības iestādes atļauju, ja ar trešā valstī esošu pārzini vai apstrādātāju tiek slēgts līgums bez iepriekš minētajām apstiprinātajām standarta klauzulām.

9.3. Pamatojoties uz atkāpēm īpašās situācijās

Ja kredītiestādei ir nepieciešams nosūtīt datus uz valsti ārpus ES, bet attiecībā uz kuru Eiropas Komisija nav pieņēmusi lēmumu par aizsardzības līmeņa pietiekamību un nav nodrošinātas atbilstošas garantijas, kredītiestāde drīkst nosūtīt datus uz trešo valsti vai starptautisko organizāciju, ja izpildās kāds no šādiem nosacījumiem:

1. datu subjekts ir skaidri piekritis nosūtīšanai, balstoties uz pietiekamu iepriekš sniegu informāciju par iespējamiem riskiem, ko šāda nosūtīšana varētu radīt;
2. nosūtīšana ir vajadzīga, lai izpildītu līgumu starp datu subjektu un kredītiestādi vai īstenotu pasākumus pirms līguma noslēgšanas, kas pieņemti pēc datu subjekta pieprasījuma (*piemēram, maksājumu veikšanas nodrošināšana, informācijas nodošana maksājumu karšu organizācijām un korespondentbankām, lai izpildītu līguma noteikumus*);
3. nosūtīšana ir vajadzīga līguma noslēgšanai starp kredītiestādi un citu fizisku vai juridisku personu datu subjekta interesēs vai šāda līguma izpildei;
4. nosūtīšana ir nepieciešama, ja ir ES vai Latvijas tiesību aktos nostiprināti svarīgi iemesli sabiedrības interesēs (*piemēram, normatīvos aktos noteiktā informācijas apmaiņa noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanas nolūkiem*) un šajā gadījumā sabiedrības intereses ir jāinterpretē šauri un šis tiesiskais pamats pielietojams izņēmuma gadījumos;
5. nosūtīšana ir vajadzīga, lai celtu, īstenotu vai aizstāvētu likumīgās prasības (*piemēram, tiesvedībai*);
6. nosūtīšana ir vajadzīga, lai aizsargātu datu subjekta vai citu personu īpaši svarīgas intereses, ja datu subjekts ir fiziski vai tiesiski nespējīgs dot savu piekrišanu;
7. nosūtīšanu izdara no reģistra, kurš ir paredzēts, lai sniegtu informāciju sabiedrībai (*piemēram, tiek nosūtīta informācija, kas ir atspoguļota publiskos reģistros – zemesgrāmata, Uzņēmuma reģistra kārtotajos reģistros*).

Saskaņā ar Regulas 48. pantu trešās valsts tiesas spriedums un valsts administratīvās iestādes lēmums, ar kuru kredītiestādei ir uzlikts pienākums nosūtīt vai izpaust datus, var tikt atzīts un izpildāms vienīgi tad, ja tas ir balstīts uz starptautisku nolīgumu, piemēram, savstarpējās palīdzības lūgumu, kas ir spēkā starp pieprasītāju trešo valsti un ES vai kādu tās dalībvalsti. Tomēr šajā gadījumā kredītiestādei būtu jāņem vērā arī Kredītiestāžu likuma V nodaļā norādītie ierobežojumi datu izpaušanai.

Ja nav iespējams attiecināt kādu no iepriekš minētajiem pamatojumiem datu nosūtīšanai, kredītiestādei ir tiesības veikt izņēmuma nosūtīšanu, ja nosūtīšana neatkārtojas un attiecas vienīgi uz ierobežotu skaitu datu subjektu, kā arī ir vajadzīga kredītiestādes pārliecinošām leģitīmām interesēm, attiecībā uz kurām datu subjekta intereses vai tiesības un brīvības nav svarīgākas, un kredītiestāde ir novērtējusi visus apstākļus saistībā ar datu nosūtīšanu un, pamatojoties uz minēto novērtējumu, kredītiestāde ir sniegusi atbilstošas garantijas attiecībā uz datu aizsardzību. Šādā gadījumā kredītiestāde par šo nosūtīšanu informē uzraudzības iestādi un datu subjektu.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

9.4. Datu nodošanas izvērtējums

Apkopojot iepriekš minēto, kredītiestādei nepieciešams strukturēt informācijas analīzi un veicamās darbības, lai noskaidrotu, vai datu nodošana ārpus ES atbilst Regulas prasībām. , Piemērs šāda novērtējuma veikšanai norādīts tabulā.

Tabula Nr. 16

Piemērs novērtējuma procesam datu nodošanas ārpus ES gadījumā

Situācijas analīzes solis	Kritērijs	Piemēri
1.	Pārbaudāms, vai Eiropas Komisija par konkrēto trešo valsti, tās teritoriju vai konkrētiem sektoriem vai starptautisko organizāciju ir pieņēmusi lēmumu un iekļāvusi publicētā sarakstā, ka ir vai vairs nav nodrošināts pietiekams datu aizsardzības līmenis.	
2.	Kad pārbaudīts, ka Eiropas Komisija nav pieņēmusi lēmumu par pietiekamu datu aizsardzības līmeni, tad kredītiestāde var sūtīt datus uz trešo valsti vai starptautisko organizāciju tikai tad, ja tā ir sniegusi atbilstošas garantijas ar nosacījumu, ka datu subjektiem tiek nodrošinātas tiesības un efektīvi tiesiskās aizsardzības līdzekļi, proti: 1) vai ir piemērojami saistošie uzņēmumu noteikumi (Binding Corporate Rules), 2) vai sadarbības līgumam piemērojamas apstiprinātas standarta datu aizsardzības klauzulas, 3) vai ir piemērojams apstiprināts rīcības kodekss, 4) vai ir piemērojami apstiprināti sertifikācijas mehānismi, 5) vai starp publiskām institūcijām piemērojams juridiski saistošs instruments.	Korporatīvās pārvaldības prasību izpildei vai arī grupas ietvaros kopīgi veiktu funkciju realizēšanai būtu iespējams organizēt datu apmaiņu uz apstiprinātu saistošo uzņēmuma noteikumu pamata.
3.	Kredītiestāde var nodrošināt nepieciešamās garantijas datu nosūtīšanai, ar trešā valstī esošu pārzini vai apstrādātāju noslēdzot līgumu bez iepriekšējā solī minētajām apstiprinātajām standarta klauzulām. Šādā gadījumā jāsaņem kompetentās uzraudzības iestādes atļauja.	
4.	Datu nosūtīšana vai vairākkārtēja nosūtīšana uz trešo valsti vai starptautisko organizāciju iespējama, ja: 1) datu subjekts skaidri piekritis, pamatojoties uz iepriekš sniegto informāciju, 2) pēc datu subjekta pieprasījuma nepieciešams izpildīt līgumu vai veikt darbības pirms līguma noslēgšanas, 3) ir svarīgi iemesli sabiedrības interesēs, 4) nepieciešams likumīgo interešu īstenošanai vai aizstāvēšanai, 5) datu subjekts ir fiziski vai tiesiski nespējīgs dot savu piekrišanu īpaši svarīgu savu vai citu personu interešu aizsardzībai, 6) nosūtīšanu izdara no reģistra, lai sniegtu informāciju sabiedrībai.	Nepieciešama informācijas apmaiņa noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanas nolūkiem. Informācijas nodošana korespondentbankai vai maksājumu karšu organizācijai, lai nodrošinātu maksājumu uzdevumu izpildi.

5.	Ja iepriekšējos soļos nav izpildījies neviens no nepieciešamajiem kritērijiem, kredītiestāde var nosūtīt datus uz trešo valsti vai starptautisku organizāciju, ja: 1) nosūtīšana neatkārtojas, 2) datu subjektu skaits ir ierobežots, 3) nosūtīšana nepieciešama kredītiestādes leģitīmām interesēm, 4) kredītiestāde ir novērtējusi visus apstākļus un sniegusi atbilstošas garantijas datu aizsardzībai. Kredītiestādei jāinformē uzraudzības iestāde un datu subjekti par nosūtīšanu un leģitīmām interesēm. Kredītiestādei jānodrošina visu veikto soļu darbība, garantijas un novērtējuma dokumentēšana.	

Šīs nodaļas jautājumi ir izklāstīti arī Regulas 101., 102., 103., 104., 105., 107., 108., 109., 110., 111., 112., 113., 114. un 115. apsvērumā un Regulas 44., 45., 46., 47., 48. un 49. pantā.

9.5. Darbinieku personas datu nodošana

Darba e-pasts un darba tālruņa numurs uzskatāmi par kredītiestādi raksturojošu informāciju, ar kuru kredītiestāde ir tiesīga rīkoties pēc saviem ieskatiem, t.sk. nodot korporatīvajiem uzņēmumiem vai vienā koncernā esošajām kredītiestādēm. Vadoties no ES iedibinātās prakses, darbiniekam darba e-pasts vai darba tālrunis jāizmanto darba vajadzībām, minēto saziņas līdzekļu lietošanu privātām vajadzībām darba devējam ir tiesības ierobežot (t.sk. aizliegt pilnībā). Ieteicams darba e-pasta vai darba tālruņa izmatošanu regulēt ar kredītiestādes iekšējiem normatīvajiem dokumentiem. Citu darbinieku datu nodošana trešajām valstīm jāregulē darba līgumu ietvaros, ievērojot 29.panta darba grupas atzinumu par darbinieku personas datu apstrādi darbavietās.

(Ar grozījumiem, kas izdarīti 08.01.2021.)

10. SADARBĪBA AR UZRAUDZĪBAS IESTĀDI

Kredītiestādes apņemas sadarboties ar uzraudzības iestādi tās pienākumu izpildē. Saskaņā ar Regulas noteikumiem, kredītiestādei ir nepieciešams sadarboties ar uzraudzības iestādi vismaz šādos gadījumos:

1) personas datu aizsardzības pārkāpuma gadījumā, ziņojot par to uzraudzības iestādei un pārvaldot to;
2) novērtējuma par ietekmi uz datu apstrādi veikšanas gadījumā, ja, neskatoties uz plānotiem tehniskiem un organizatoriskiem pasākumiem, saglabājas augsts risks datu subjekta tiesībām;
3) paziņojot uzraudzības iestādei par iecelto datu aizsardzības speciālistu.

Ja datu subjektam ir pretenzijas pret kredītiestādi, tad pirms vēršanās uzraudzības iestādē, tam ir vispirms jāvēršas pie attiecīgās kredītiestādes un, ja jautājumu nevar atrisināt ar kredītiestādes iesaisti, tad klients var vērsties uzraudzības iestādē.

Kredītiestādes atbalsta regulāru komunikāciju ar uzraudzības iestādi par nozarē aktuāliem problēmjautājumiem, un pēc iespējas iekļauj problēmjautājumu iespējamos risinājumus šajos Ieteikumos.

Kredītiestādes, kuras veic pārrobežu datu apstrādi, galvenokārt uzraudzīs vadošā uzraudzības iestāde, kas atrodas galvenajā uzņēmējdarbības veikšanas vietā. Kredītiestādei tādējādi jāsadarbojas tikai ar vienu – vadošo uzraudzības iestādi saistībā ar visām datu apstrādes darbībām, kas tiek veiktas visā ES. Papildus uzraudzību var veikt arī vietējās uzraudzības iestādes, kuru jurisdikcijā notiek datu apstrāde, ja šādu uzraudzību paredz vietējos normatīvajos aktos noteikts pienākums vai kāda cita piešķirta publiska funkcija.

Lai vietējā uzraudzības iestāde saņemtu kontroli pār datu apstrādi, kas notiek tās jurisdikcijā, ir jāsazinās ar vadošo uzraudzības iestādi. Vadošā uzraudzības iestāde var vietējai uzraudzības iestādei atļaut vai atteikt veikt kontroli pār datu apstrādi savā jurisdikcijā. Galvenais noteikums par sadarbību uzraudzības iestāžu starpā ir, lai iesaistīto iestāžu darbības ir saskaņotas, lai netiek veiktas savstarpēji nekoordinētas darbības.

Uzraudzības iestāžu darbībā var iejaukties Eiropas Datu aizsardzības kolēģija, ja, piemēram, vietējā uzraudzības iestāde iebilst pret vadošās uzraudzības iestādes darbībām, un iestādes savā starpā nevar atrisināt radušos situāciju.

Pastāv iespēja, ka uzraudzība starp dalībvalstīm atšķirsies, jo:

1) dalībvalstu resursi un attieksme pret datu aizsardzību starp dalībvalstīm atšķiras;
2) dalībvalstīs noteikto prasību praktiska izpilde var atšķirties no Regulā noteiktās;
3) pastāv plaša neatbilstība starp teorētiskajām pilnvarām, kas sniegtas dalībvalsts iestādēm, un šo pilnvaru īstenošanu praksē.

IETEIKUMU IZMANTOŠANAS IEROBEŽOJUMI

Ieteikumi ir sagatavoti latviešu valodā Latvijas Finanšu nozares asociācijas uzdevumā, balstoties uz sagatavošanas brīdī spēkā esošo regulējumu un sniegtajām 29. panta darba grupas rekomendācijām, kā arī ņemot vērā plānotās izmaiņas tiesību aktos, kuriem izstrādāti projekti, kuri uz šo Ieteikumu sagatavošanas brīdi vēl nav pieņemti un stājušies spēkā.

Ieteikumi ir skaidrojošs, praktisks palīgmateriāls kredītiestāžu sektoram Latvijā sagatavošanas procesā, lai kredītiestādes varētu atbilstoši piemērot Regulas prasības, ievērojot 29. panta darba grupa viedokli un tās ietvaros izdotās, kā arī plānotās vadlīnijas.

Vienlaikus Ieteikumi satur praktiskus piemērus saistībā ar Regulas prasībām, tomēr katras atsevišķas kredītiestādes darbības saistībā ar Regulas prasību ieviešanu ir atkarīgas no konkrētās situācijas un apstākļiem katrā konkrētā kredītiestādē, tajā skaitā produktu un pakalpojumu veidiem, klientu skaita un struktūras, IT sistēmas uzbūves, iekšējiem normatīviem aktiem un izstrādāto kārtību.

Šie Ieteikumi ir skatāmi kopumā, jo atsevišķu to daļu nesaistīta analīze var novest pie maldinošiem secinājumiem.

Šajos Ieteikumos ietvertie secinājumi un rekomendācijas nav saistoši uzraudzības iestādēm vai citām personām. Šie Ieteikumi ir paredzēti vienīgi Latvijas Finanšu nozares asociācijas biedriem informatīvos nolūkos un nav paredzēti citām trešajām personām.

(Ar grozījumiem, kas izdarīti 08.01.2021.)