Pamatnostādnes 06/2020 par Otrās maksājumu pakalpojumu direktīvas un VDAR mijiedarbību

Versija 2.0

Pieņemtas 2020. gada 15. decembrī

Versiju vēsture

Versija 2.0	15.12.2020.	Pamatnostādņu pieņemšana pēc sabiedriskās apspriešanas
Versija 1.0	17.07.2020.	Pamatnostādņu pieņemšana sabiedriskajai apspriešanai

Satura rādītājs

Eiropas Datu aizsardzības kolēģija,

ņemot vērā 70. panta 1. punkta e) apakšpunktu Eiropas Parlamenta un Padomes Regulā (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu [persondatu] apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (turpmāk tekstā — "VDAR"),

ņemot vērā EEZ līgumu, un jo īpaši tā XI pielikumu un 37. protokolu, kas grozīts ar EEZ Apvienotās komitejas Lēmumu Nr. 154/2018 (2018. gada 6. jūlijs)[1],

ņemot vērā tās Reglamenta 12. un 22. pantu,

tā kā:

(1) Vispārējā datu aizsardzības regula paredz konsekventu noteikumu kopumu persondatu apstrādei visā ES.

(2) Otrā maksājumu pakalpojumu direktīva (Eiropas Parlamenta un Padomes Direktīva 2015/2366/ES (2015. gada 23. decembris), turpmāk tekstā — "*PSD2*") atceļ Direktīvu 2007/64/EK un paredz jaunus noteikumus, lai nodrošinātu tiesisko noteiktību patērētājiem, tirgotājiem un uzņēmumiem maksājumu ķēdē un modernizētu maksājumu pakalpojumu tirgus tiesisko regulējumu[2]. Dalībvalstīm bija jātransponē *PSD2* valsts tiesību aktos līdz 2018. gada 13. janvārim.

(3) Svarīga *PSD2* iezīme ir tiesiskā regulējuma ieviešana jauniem maksājumu iniciēšanas pakalpojumiem un konta informācijas pakalpojumiem. *PSD2* ļauj šo jauno maksājumu pakalpojumu sniedzējiem piekļūt datu subjektu maksājumu kontiem minēto pakalpojumu sniegšanas nolūkos.

(4) Attiecībā uz datu aizsardzību saskaņā ar *PSD2* 94. panta 1. punktu jebkura persondatu apstrāde, tostarp informācijas sniegšana par apstrādi *PSD2* vajadzībām, jāveic saskaņā ar VDAR[3] un Regulu (ES) 2018/1725.

(5) *PSD2* 89. apsvērums paredz, ka gadījumos, kad persondati tiek apstrādāti *PSD2* vajadzībām, būtu jānosaka precīzs apstrādes mērķis, jānorāda piemērojamais juridiskais pamats, jāpiemēro VDAR noteiktās drošības prasības un jāievēro tādi principi kā nepieciešamība, samērīgums, mērķa ierobežojums un samērīgs datu glabāšanas termiņš. Turklāt visās datu apstrādes sistēmās, kas tiek izstrādātas un izmantotas *PSD2* ietvaros, būtu jāiekļauj integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma[4].

(6) *PSD2* 93. apsvērums paredz, ka maksājumu iniciēšanas pakalpojumu sniedzējiem un konta informācijas pakalpojumu sniedzējiem, no vienas puses, un kontu apkalpojošajam maksājumu pakalpojumu sniedzējam, no otras puses, būtu jāievēro nepieciešamās datu aizsardzības un drošības prasības, kas noteiktas vai minētas šajā direktīvā vai iekļautas regulatīvajos tehniskajos standartos,

[1] Atsauces uz "dalībvalstīm" šajā dokumentā būtu jāsaprot kā atsauces uz "EEZ dalībvalstīm".
[2] *PSD2* 6. apsvērums.
[3] Tā kā *PSD2* tika pieņemta pirms VDAR, tajā joprojām ir atsauce uz Direktīvu 95/46. VDAR 94. pants nosaka, ka atsauces uz atcelto Direktīvu 95/46/EK uzskata par atsaucēm uz VDAR.
[4] PSD2 89. apsvērums.

IR PIEŅĒMUSI ŠĪS PAMATNOSTĀDNES.

1. IEVADS

1. Otrā maksājumu pakalpojumu direktīva (turpmāk tekstā — "*PSD2*") ir ieviesusi vairākas novitātes maksājumu pakalpojumu jomā. Lai gan tas rada jaunas iespējas patērētājiem un uzlabo pārredzamību šajā jomā, *PSD2* piemērošana rada zināmus jautājumus un bažas par nepieciešamību datu subjektiem pilnīgi kontrolēt savus persondatus. Vispārīgā datu aizsardzības regula (turpmāk tekstā — "VDAR") attiecas uz persondatu apstrādi, tostarp apstrādes darbībām, kas tiek veiktas saistībā ar maksājumu pakalpojumiem, kā paredz *PSD2*[5]. Tādējādi datu pārziņiem, kas darbojas jomā, uz kuru attiecas *PSD2*, vienmēr jānodrošina atbilstība VDAR prasībām, tostarp VDAR 5. pantā noteiktajiem datu aizsardzības principiem, kā arī attiecīgajiem E-privātuma direktīvas[6] noteikumiem. Kaut arī *PSD2*[7] un normatīvajos tehniskajos standartos par drošu lietotāja autentificēšanu un vienotiem un drošiem atklātiem saziņas standartiem (turpmāk tekstā — "*RTS*"[8]) ir iekļauti konkrēti noteikumi attiecībā uz datu aizsardzību un drošību, ir radusies neskaidrība par šo noteikumu interpretāciju, kā arī par vispārējās datu aizsardzības sistēmas un *PSD2* savstarpējo mijiedarbību.

2. 2018. gada 5. jūlijā Eiropas Datu aizsardzības kolēģija (EDAK) izdeva vēstuli par *PSD2*, kurā EDAK sniedza paskaidrojumus par jautājumiem attiecībā uz persondatu aizsardzību saistībā ar *PSD2*, jo īpaši par personu, kuras nav līgumslēdzējas puses, persondatu (tā dēvēto "kluso personu datu") apstrādi, ko veic konta informācijas pakalpojumu sniedzēji (turpmāk tekstā — "*AISP*") un maksājumu iniciēšanas pakalpojumu sniedzēji (turpmāk tekstā — "*PISP*"), par piekrišanas došanas un atsaukšanas procedūrām, *RTS* un sadarbību starp kontus apkalpojošajiem maksājumu pakalpojumu sniedzējiem (turpmāk tekstā — "*ASPSP*") saistībā ar drošības pasākumiem. Šo pamatnostādņu sagatavošana ietvēra informācijas vākšanu no ieinteresētajām personām gan rakstveidā, gan ieinteresēto personu pasākumos, lai noteiktu visaktuālākās problēmas.

3. Šo pamatnostādņu mērķis ir sniegt papildu norādījumus par datu aizsardzības aspektiem *PSD2* kontekstā, jo īpaši par saistību starp attiecīgajiem VDAR noteikumiem un *PSD2*. Šajās pamatnostādnēs galvenā uzmanība ir pievērsta persondatu apstrādei, ko veic *AISP* un *PISP*. Attiecīgi šajā dokumentā ir izklāstīti nosacījumi par piekļuves piešķiršanu *ASPSP* maksājumu kontu informācijai un par *PISP* un *AISP* veiktu persondatu apstrādi, tostarp prasības un drošības pasākumi attiecībā uz *PISP* un *AISP* veiktu persondatu apstrādi citiem nolūkiem, nevis sākotnējiem nolūkiem, kuriem dati ir vākti, jo īpaši, ja tie ir vākti konta informācijas pakalpojuma[9] sniegšanas ietvaros. Šajā dokumentā ir aplūkoti arī dažādi nepārprotamas piekrišanas jēdzieni saskaņā ar *PSD2* un VDAR,

[5] VDAR 1. panta 1. punkts.

[6] Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu [persondatu] apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (Direktīva par privāto dzīvi un elektronisko komunikāciju) (OV L 201, 31.7.2002., 37.–47. lpp.).

[7] *PSD* 94. pants u. c.

[8] Komisijas Deleģētā regula (ES) 2018/389 (2017. gada 27. novembris), ar ko Eiropas Parlamenta un Padomes Direktīvu (ES) 2015/2366 papildina attiecībā uz regulatīvajiem tehniskajiem standartiem par drošu lietotāja autentificēšanu un vienotiem un drošiem atklātiem saziņas standartiem (dokuments attiecas uz EEZ), C/2017/7782 (OV L 69, 13.3.2018., 23.–43. lpp.), pieejama šeit: https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:32018R0389&from=EN.

[9] Konta informācijas pakalpojums ir tiešsaistes pakalpojums, ar ko sniedz konsolidētu informāciju par vienu vai vairākiem maksājumu kontiem, kuri atrodas maksājumu pakalpojumu lietotāja turējumā vai nu pie cita maksājumu pakalpojumu sniedzēja, vai pie vairāk nekā viena maksājumu pakalpojumu sniedzēja.

"kluso personu datu" apstrāde, *PISP* un *AISP* veikta īpašo kategoriju persondatu apstrāde, VDAR noteikto galveno datu aizsardzības principu piemērošana, ieskaitot datu minimizēšanu, pārredzamību, pārskatatbildību un drošības pasākumus. *PSD2* ietver daudzfunkcionālus pienākumus, tostarp patērētāju aizsardzības un konkurences tiesību jomā. Apsvērumi par šīm tiesību jomām neietilpst šo pamatnostādņu darbības jomā.

4. Lai atvieglotu pamatnostādņu lasīšanu, turpmāk ir sniegtas šajā dokumentā izmantotās galvenās definīcijas.

1.1 Definīcijas

"Konta informācijas pakalpojuma sniedzējs ("AISP")" ir tāda tiešsaistes pakalpojuma sniedzējs, ar ko nodrošina konsolidētu informāciju par vienu vai vairākiem maksājumu kontiem, kuri atrodas maksājumu pakalpojumu lietotāja turējumā vai nu pie cita maksājumu pakalpojumu sniedzēja, vai pie vairāk nekā viena maksājumu pakalpojumu sniedzēja.

"Kontu apkalpojošais maksājumu pakalpojumu sniedzējs ("ASPSP")" ir maksājumu pakalpojumu sniedzējs, kas nodrošina un uztur maksātāja maksājumu kontu.

"Datu minimizēšana" ir datu aizsardzības princips, saskaņā ar kuru persondatiem jābūt adekvātiem, atbilstīgiem un jāietver tikai tas, kas nepieciešams to apstrādes nolūkos.

"Maksātājs" ir tāda fiziska vai juridiska persona, kura ir maksājumu konta turētāja un kura atļauj veikt maksājuma uzdevumu no šā maksājumu konta, vai gadījumā, ja maksājumu konta nav, fiziska vai juridiska persona, kas dod maksājuma uzdevumu.

"Maksājuma saņēmējs" ir fiziska vai juridiska persona, kas ir maksājumu darījuma naudas līdzekļu iecerētais saņēmējs.

"Maksājumu konts" ir tāds konts uz viena vai vairāku maksājumu pakalpojumu lietotāju vārda, ko izmanto maksājumu darījumu izpildei.

"Maksājumu iniciēšanas pakalpojumu sniedzējs ("PISP")" ir pakalpojuma sniedzējs, kas pēc maksājumu pakalpojumu lietotāja pieprasījuma iniciē maksājuma uzdevumu attiecībā uz maksājumu kontu, kurš atrodas cita maksājumu pakalpojumu sniedzēja turējumā.

"Maksājumu pakalpojumu sniedzējs" ir iestāde, kas minēta *PSD2* 1. panta 1. punktā[10], vai fiziska vai juridiska persona, uz kuru attiecas atbrīvojums saskaņā ar *PSD2* 32. vai 33. pantu.

[10] *PSD2* 1. panta 1. punkts paredz noteikumus, saskaņā ar kuriem dalībvalstis izšķir šādas *maksājumu pakalpojumu sniedzēju* kategorijas:
a) kredītiestādes, kā definēts Eiropas Parlamenta un Padomes Regulas (ES) Nr. 575/2013 4. panta 1. punkta 1. apakšpunktā, tostarp to filiāles, kā definēts minētās regulas 4. panta 1. punkta 17. apakšpunktā, ja šādas filiāles atrodas Savienībā — neatkarīgi no tā, vai minēto filiāļu galvenie biroji atrodas Savienībā vai saskaņā ar Direktīvas 2013/36/ES 47. pantu un valsts tiesību aktiem — ārpus Savienības;
b) elektroniskās naudas iestādes, kā definēts Direktīvas 2009/110/EK 2. panta 1. punktā, tostarp saskaņā ar minētās direktīvas 8. pantu un valsts tiesību aktiem, minēto iestāžu filiāles, ja šādas filiāles atrodas Savienībā un to galvenie biroji atrodas ārpus Savienības, un vienīgi tiktāl, ciktāl minēto filiāļu sniegtie maksājumu pakalpojumi ir saistīti ar elektroniskās naudas emitēšanu;
c) pasta žiro norēķinu iestādes, kuras saskaņā ar valsts tiesību aktiem ir tiesīgas sniegt maksājumu pakalpojumus;
d) maksājumu iestādes;
e) ECB un valstu centrālās bankas, kad tās nerīkojas kā monetāras vai citas valsts iestādes;
f) dalībvalstis vai to reģionālās vai vietējās iestādes, kad tās nerīkojas kā valsts iestādes.

"Maksājumu pakalpojumu lietotājs" ir fiziska vai juridiska persona, kas izmanto maksājumu pakalpojumu kā maksātājs, maksājuma saņēmējs vai kā abi.

"Persondati" ir jebkura informācija par identificētu vai identificējamu fizisko personu (datu subjektu). Identificējama fiziska persona ir tāda, kuru var tieši vai netieši identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, minētās personas vārdu, uzvārdu, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem.

"Integrētā datu aizsardzība" attiecas uz produktā vai pakalpojumā iestrādātiem tehniskiem un organizatoriskiem pasākumiem, kas ir paredzēti datu aizsardzības principu efektīvai ieviešanai un nepieciešamo drošības pasākumu integrēšanai apstrādē, lai izpildītu VDAR prasības un aizsargātu datu subjektu tiesības.

"Datu aizsardzība pēc noklusējuma" attiecas uz atbilstošiem tehniskiem un organizatoriskiem pasākumiem, kas tiek īstenoti, lai nodrošinātu, ka pēc noklusējuma tiek apstrādāti tikai tādi persondati, kas ir nepieciešami katram konkrētajam apstrādes nolūkam.

"RTS" attiecas uz Komisijas Deleģēto regulu (ES) 2018/389 (2017. gada 27. novembris), ar ko Eiropas Parlamenta un Padomes Direktīvu (ES) 2015/2366 papildina attiecībā uz regulatīvajiem tehniskajiem standartiem par drošu lietotāja autentificēšanu un vienotiem un drošiem atklātiem saziņas standartiem.

"Trešās personas — pakalpojumu sniedzēji ("TPP")" ir gan *PISP*, gan *AISP*.

1.2 Pakalpojumi saskaņā ar *PSD2*

5. *PSD2* ievieš divus jaunus maksājumu pakalpojumu veidus (pakalpojumu sniedzējus): *PISP* un *AISP*. *PSD2* 1. pielikumā ir norādīti astoņi maksājumu pakalpojumi, uz kuriem attiecas *PSD2*.

6. *PISP* sniedz pakalpojumus, kas pēc maksājumu pakalpojumu lietotāja pieprasījuma iniciē maksājumu uzdevumus attiecībā uz lietotāja maksājumu kontu, kurš atrodas cita maksājumu pakalpojumu sniedzēja turējumā[11]. *PISP* var pieprasīt, lai *ASPSP* (parasti banka) iniciētu darījumu maksājumu pakalpojumu lietotāja vārdā. (Maksājumu pakalpojumu) lietotājs var būt fiziska persona (datu subjekts) vai juridiska persona.

7. *AISP* sniedz tiešsaistes pakalpojumus, ar ko nodrošina konsolidētu informāciju par vienu vai vairākiem maksājumu kontiem, kuri atrodas maksājumu pakalpojumu lietotāja turējumā vai nu pie cita maksājumu pakalpojumu sniedzēja, vai pie vairāk nekā viena maksājumu pakalpojumu sniedzēja[12]. Saskaņā ar *PSD2* 28. apsvērumu maksājumu pakalpojumu lietotājs jebkurā brīdī var uzreiz gūt vispārēju priekšstatu par savu finansiālo stāvokli.

8. Varētu tikt piedāvāti vairāki dažādi konta informācijas pakalpojumu veidi, pievēršot uzmanību to dažādajām funkcijām un mērķiem. Piemēram, daži pakalpojumu sniedzēji var piedāvāt lietotājiem tādus pakalpojumus kā budžeta plānošana un izdevumu uzraudzība. Persondatu apstrādi šādu pakalpojumu ietvaros nosaka *PSD2*. Pakalpojumi, kas saistīti ar maksājumu pakalpojumu lietotāja kredītspējas novērtēšanu, vai revīzijas pakalpojumi, kuri veikti, pamatojoties uz informācijas vākšanu ar konta informācijas pakalpojuma starpniecību, neietilpst *PSD2* darbības jomā, tāpēc uz tiem attiecas VDAR. Turklāt *PSD2* darbības jomā neietilpst arī konti, kas nav maksājumu konti

[11] *PSD2* 4. panta 15. punkts.
[12] *PSD2* 4. panta 16. punkts.

(piemēram, uzkrājumu, ieguldījumu konti). Jebkurā gadījumā VDAR ir piemērojamais tiesiskais regulējums attiecībā uz persondatu apstrādi.

1. piemērs. *HappyPayments* ir uzņēmums, kas piedāvā tiešsaistes pakalpojumu, kura ietvaros tiek sniegta informācija par vienu vai vairākiem maksājumu kontiem, izmantojot mobilo lietotni, lai nodrošinātu finanšu uzraudzību (konta informācijas pakalpojums). Izmantojot šo pakalpojumu, maksājumu pakalpojumu lietotājs var gūt ieskatu par atlikumiem un neseniem darījumiem divos vai vairākos maksājumu kontos dažādās bankās. Ja maksājumu pakalpojumu lietotājs izvēlas to darīt, šis pakalpojums piedāvā arī izdevumu un ienākumu kategorizāciju atbilstoši dažādām tipoloģijām (alga, brīvā laika pavadīšana, enerģija, hipotēka utt.), tādējādi palīdzot maksājumu pakalpojumu lietotājam veikt finanšu plānošanu. Šajā lietotnē uzņēmums piedāvā arī pakalpojumu maksājumu iniciēšanai tieši no lietotāja norādītā(-ajiem) maksājumu konta(-iem) (maksājumu iniciēšanas pakalpojums).

9. Šo pakalpojumu sniegšanai *PSD2* paredz juridiskos nosacījumus, saskaņā ar kuriem *PISP* un *AISP* var piekļūt maksājumu kontiem, lai sniegtu pakalpojumu maksājumu pakalpojumu lietotājam.

10. *PSD2* 66. panta 1. punktā un 67. panta 1. punktā noteikts, ka piekļuve maksājumu un konta informācijas pakalpojumiem un to izmantošana ir maksājumu pakalpojumu lietotāja tiesības. Tas nozīmē, ka maksājumu pakalpojumu lietotājam vajadzētu būt pilnīgi brīvai izvēlei attiecībā uz šādu tiesību izmantošanu un viņu nevar piespiest izmantot šīs tiesības.

11. Piekļuvi maksājumu kontiem un maksājumu kontu informācijas izmantošanu daļēji reglamentē *PSD2* 66. un 67. pants, kuros noteikti drošības pasākumi (personas) datu aizsardzībai. *PSD2* 66. panta 3. punkta f) apakšpunkts paredz, ka *PISP* nepieprasa no maksājumu pakalpojumu lietotāja citus datus, izņemot tos, kas nepieciešami, lai sniegtu maksājumu iniciēšanas pakalpojumu, un *PSD2* 66. panta 3. punkta g) apakšpunkts paredz, ka *PISP* neizmanto nekādus datus, nepiekļūst tiem vai neuzglabā tos nekādos citos nolūkos kā vienīgi, lai veiktu konta informācijas pakalpojumu, ko nepārprotami pieprasījis maksājumu pakalpojumu lietotājs. Turklāt *PSD2* 67. panta 2. punkta d) apakšpunkts ierobežo *AISP* piekļuvi informācijai no izraudzītajiem maksājumu kontiem un par saistītajiem maksājumu darījumiem, savukārt *PSD2* 67. panta 2. punkta f) apakšpunkts paredz, ka *AISP* neizmanto nekādus datus, nepiekļūst tiem vai neuzglabā tos nekādos citos nolūkos kā vienīgi, lai veiktu konta informācijas pakalpojumu, ko nepārprotami pieprasījis maksājumu pakalpojumu lietotājs, saskaņā ar datu aizsardzības noteikumiem. Pēdējos no minētajiem noteikumiem uzsvērts, ka konta informācijas pakalpojumu kontekstā persondatus var vākt tikai konkrētiem, skaidriem un leģitīmiem nolūkiem. Tāpēc *AISP* līgumā būtu skaidri jānorāda, kādiem konkrētiem nolūkiem personas konta informācijas dati tiks apstrādāti saistībā ar tā sniegto konta informācijas pakalpojumu. Saskaņā ar VDAR 5. pantu līgumam vajadzētu būt likumīgam, taisnīgam un pārredzamam, un tam jāatbilst arī citiem tiesību aktiem patērētāju tiesību aizsardzības jomā.

12. Atkarībā no konkrētajiem apstākļiem maksājumu pakalpojumu sniedzējs saskaņā ar VDAR varētu būt datu pārzinis vai apstrādātājs. Šajās pamatnostādnēs "pārziņi" ir tie maksājumu pakalpojumu sniedzēji, kuri atsevišķi vai kopā ar citiem nosaka persondatu apstrādes nolūkus un līdzekļus. Plašākus norādījumus par iepriekš minēto var atrast EDAK Pamatnostādnēs 07/2020 par datu pārziņa un apstrādātāja jēdzieniem VDAR.

2 LIKUMĪGAIS PAMATOJUMS UN TURPMĀKA APSTRĀDE SASKAŅĀ AR *PSD2*

2.1 Apstrādes likumīgais pamatojums

13. Saskaņā ar VDAR datu pārziņiem jābūt likumīgam pamatojumam, lai apstrādātu persondatus. VDAR 6. panta 1. punkts ir pilnīgs un ierobežojošs sešu juridisko pamatu saraksts persondatu apstrādei saskaņā ar VDAR[13]. Pārzinis pats nosaka atbilstošo juridisko pamatu un nodrošina, ka tiek izpildīti visi šā juridiskā pamata nosacījumi. Noteikšana, kurš pamats ir derīgs un vispiemērotākais konkrētā situācijā, ir atkarīga no apstākļiem, kādos notiek apstrāde, tostarp apstrādes nolūka un saistības starp pārzini un datu subjektu.

2.2 VDAR 6. panta 1. punkta b) apakšpunkts (apstrāde ir nepieciešama līguma izpildei)

14. Maksājumu pakalpojumi tiek sniegti, pamatojoties uz līgumu starp maksājumu pakalpojumu lietotāju un maksājumu pakalpojumu sniedzēju. Kā norādīts *PSD2* 87. apsvērumā, "*[š]ai direktīvai būtu jāattiecas tikai uz maksājumu pakalpojumu lietotāja un maksājumu pakalpojumu sniedzēja savstarpējām līgumsaistībām un pienākumiem*". Saskaņā ar VDAR galvenais juridiskais pamats persondatu apstrādei, lai sniegtu maksājumu pakalpojumus, ir VDAR 6. panta 1. punkta b) apakšpunkts, kas nozīmē, ka apstrāde ir nepieciešama, lai izpildītu līgumu, kurā viena no pusēm ir datu subjekts, vai lai veiktu attiecīgas darbības pēc datu subjekta pieprasījuma pirms līguma noslēgšanas.

15. *PSD2* noteiktie maksājumu pakalpojumi ir definēti *PSD2* 1. pielikumā. Šo pakalpojumu sniegšana, kā noteikts *PSD2*, ir prasība, lai izveidotu līgumu, kura ietvaros pusēm būtu piekļuve maksājumu pakalpojumu lietotāja maksājumu konta datiem. Šiem maksājumu pakalpojumu sniedzējiem jābūt arī licencētiem operatoriem. Attiecībā uz maksājumu iniciēšanas pakalpojumiem un konta informācijas pakalpojumiem saskaņā ar *PSD2* līgumos var iekļaut noteikumus, kas arī paredz nosacījumus par papildu pakalpojumiem, kurus nereglamentē *PSD2*. *EDAK Pamatnostādnēs 2/2019 par personas datu [persondatu] apstrādi saskaņā ar VDAR 6. panta 1. punkta b) apakšpunktu, sniedzot tiešsaistes pakalpojumus datu subjektiem*, ir skaidri norādīts, ka datu pārziņiem jāizvērtē, kāda persondatu apstrāde ir objektīvi nepieciešama līguma izpildei. Šajās pamatnostādnēs ir norādīts, ka nepieciešamības pamatojums ir atkarīgs no pakalpojuma

[13] Saskaņā ar 6. pantu persondatu apstrāde ir likumīga tikai tādā apmērā un tikai tad, ja ir piemērojams vismaz viens no turpmāk minētajiem nosacījumiem:

(a) datu subjekts ir devis piekrišanu savu persondatu apstrādei vienam vai vairākiem konkrētiem nolūkiem;

(b) apstrāde ir vajadzīga līguma, kura līgumslēdzēja puse ir datu subjekts, izpildei vai pasākumu veikšanai pēc datu subjekta pieprasījuma pirms līguma noslēgšanas;

(c) apstrāde ir vajadzīga, lai izpildītu uz pārzini attiecināmu juridisku pienākumu;

(d) apstrāde ir vajadzīga, lai aizsargātu datu subjekta vai citas fiziskas personas vitālas intereses;

(e) apstrāde ir vajadzīga, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot pārzinim likumīgi piešķirtās oficiālās pilnvaras;

(f) apstrāde ir vajadzīga pārziņa vai trešās personas leģitīmo interešu ievērošanai, izņemot, ja datu subjekta intereses vai pamattiesības un pamatbrīvības, kurām nepieciešama persondatu aizsardzība, ir svarīgākas par šādām interesēm, jo īpaši, ja datu subjekts ir bērns.

rakstura, līguma pušu savstarpējām perspektīvām un gaidām, līguma pamatojuma un līguma būtiskajiem elementiem.

16. EDAK Pamatnostādnēs 2/2019 ir arī skaidri norādīts, ka, ņemot vērā VDAR 7. panta 4. punktu, tiek nošķirti apstrādes pasākumi, kas vajadzīgi līguma izpildei, un noteikumi, ko piemēro attiecībā uz pakalpojumu nosacījumu par konkrētām apstrādes darbībām, kuras nav faktiski nepieciešamas līguma izpildei. "Vajadzīgs izpildei" ir nepārprotami kas vairāk par vienkāršu līguma noteikumu[14]. Pārzinim būtu jāspēj pierādīt, ka ar datu subjektu noslēgtā konkrētā līguma priekšmets faktiski nav izpildāms, ja nenotiek attiecīgo personatu konkrēta apstrāde. Ar vienkāršu atsauci uz datu apstrādi vai tās pieminēšanu līgumā nepietiek, lai apstrāde nokļūtu 6. panta 1. punkta b) apakšpunkta darbības jomā.

17. VDAR 5. panta 1. punkta b) apakšpunkts paredz nolūka ierobežojumu principu, kas nosaka, ka persondati jāvāc konkrētiem, skaidriem un leģitīmiem nolūkiem un tos nedrīkst turpmāk apstrādāt tādā veidā, kurš nav saderīgs ar šiem nolūkiem. Vērtējot, vai 6. panta 1. punkta b) apakšpunkts ir atbilstošs juridiskais pamats apstrādei, ko veic saistībā ar līgumisku tiešsaistes pakalpojumu, būtu jāņem vērā pakalpojuma konkrētais mērķis, nolūks vai pamats[15]. Apstrādes nolūki skaidri jānorāda un jāpaziņo datu subjektam saskaņā ar pārzinim noteikto nolūka ierobežojuma un pārredzamības nodrošināšanas pienākumu. Lai vērtētu, kas ir "vajadzīgs", ir jāveic kombinēts, ar faktiem pamatots novērtējums par apstrādi "sasniedzamajam nolūkam un to, vai tā ir mazāk aizskaroša par citiem rīcības variantiem tā paša mērķa sasniegšanai". 6. panta 1. punkta b) apakšpunkts neaptver apstrādi, kas ir noderīga, bet ne objektīvi vajadzīga līgumiskā pakalpojuma izpildei vai pasākumu veikšanai pirms līguma noslēgšanas pēc datu subjekta pieprasījuma, pat ja tā ir vajadzīga citiem pārziņa darījumdarbības nolūkiem[16].

18. EDAK Pamatnostādnēs 2/2019 ir skaidri norādīts, ka ar līgumu nevar mākslīgi paplašināt persondatu kategorijas vai apstrādes darbību veidus, kas pārzinim nepieciešami, lai izpildītu līgumu 6. panta 1. punkta b) apakšpunkta nozīmē[17]. Minētajās pamatnostādnēs arī iztirzāti gadījumi, kuros var rasties "visu vai neko" situācija attiecībā uz datu subjektiem, kurus, iespējams, interesē tikai viens no pakalpojumiem. Tā var notikt, ja pārzinis vēlas apvienot vienā līgumā atsevišķus pakalpojumus vai pakalpojumu elementus, kam ir atšķirīgi pamatnolūki, īpašības vai pamatojums. Ja līgumu veido vairāki dažādi pakalpojumi vai pakalpojuma elementi, kurus faktiski var pamatoti izpildīt neatkarīgi citu no cita, 6. panta 1. punkta b) apakšpunkta piemērojamība būtu jāvērtē saistībā ar katru no šiem pakalpojumiem atsevišķi, ņemot vērā, kas ir objektīvi vajadzīgs, lai sniegtu katru atsevišķo pakalpojumu, kuru aktīvi pieprasījis vai abonējis datu subjekts[18].

19. Saskaņā ar iepriekš minētajām pamatnostādnēm pārzinim jāizvērtē, kas ir objektīvi nepieciešams līguma izpildei. Ja pārziņi nevar pierādīt, ka personas maksājumu konta datu apstrāde ir objektīvi nepieciešama, lai katru no šiem pakalpojumiem sniegtu atsevišķi, VDAR 6. panta 1. punkta b) apakšpunkts nav uzskatāms par derīgu juridisko pamatu apstrādei. Šādos gadījumos pārzinim būtu jāapsver cits apstrādes juridiskais pamats.

[14] Pamatnostādnes 2/2019 par personas datu [persondatu] apstrādi saskaņā ar VDAR 6. panta 1. punkta b) apakšpunktu, sniedzot tiešsaistes pakalpojumus datu subjektiem, EDAK, 8. lpp.
[15] Turpat.
[16] Turpat, 7. lpp.
[17] Turpat, 10. lpp.
[18] Turpat, 11. lpp.

2.3 Krāpšanas novēršana

20. *PSD2* 94. panta 1. punkts paredz, ka dalībvalstīm jāatļauj maksājumu sistēmām un maksājumu pakalpojumu sniedzējiem apstrādāt persondatus, ja tas ir nepieciešams, lai nodrošinātu ar maksājumiem saistītas krāpniecības novēršanu, izmeklēšanu un atklāšanu. Persondatu apstrāde tikai tādā apjomā, kas vajadzīgs krāpšanas novēršanai, var būt attiecīgā maksājumu pakalpojumu sniedzēja leģitīmās interesēs, ja vien nepieciešamība aizsargāt datu subjekta intereses vai pamattiesības un brīvības nav svarīgāka par šādām leģitīmām interesēm[19]. Apstrādes darbībām krāpšanas novēršanas nolūkā vajadzētu būt pamatotām ar pārziņa veiktu rūpīgu novērtējumu katrā atsevišķā gadījumā saskaņā ar pārskatatbildības principu. Turklāt, lai novērstu krāpšanu, uz pārziņiem var attiekties arī īpaši juridiski pienākumi, kas nosaka obligātu persondatu apstrādi.

2.4 Turpmāka apstrāde (*AISP* un *PISP*)

21. VDAR 6. panta 4. punkts paredz nosacījumus persondatu apstrādei citam nolūkam, nevis tam, kuram persondati ir vākti. Konkrētāk, šāda turpmāka apstrāde var tikt veikta, ja tā ir pamatota ar Savienības vai dalībvalsts tiesību aktiem, kuri par nepieciešamu un samērīgu pasākumu demokrātiskā sabiedrībā nosaka 23. panta 1. punktā minēto mērķu aizsardzību, ja datu subjekts ir devis savu piekrišanu vai ja apstrāde citam nolūkam, nevis tam, kuram persondati tika sākotnēji vākti, ir saderīga ar sākotnējo nolūku.

22. Rūpīgi jāņem vērā *PSD2* 66. panta 3. punkta g) apakšpunkts un 67. panta 2. punkta f) apakšpunkts. Kā minēts iepriekš, *PSD2* 66. panta 3. punkta g) apakšpunkts paredz, ka *PISP* neizmanto nekādus datus, nepiekļūst tiem vai neuzglabā tos nekādos citos nolūkos kā vienīgi, lai sniegtu maksājumu iniciēšanas pakalpojumu, kā to nepārprotami lūdzis maksātājs. *PSD2* 67. panta 2. punkta f) apakšpunktā noteikts, ka *AISP* neizmanto nekādus datus, nepiekļūst tiem vai neuzglabā tos nekādos citos nolūkos kā vienīgi, lai veiktu konta informācijas pakalpojumu, ko nepārprotami lūdzis maksājumu pakalpojumu lietotājs, saskaņā ar datu aizsardzības noteikumiem.

23. Tādējādi *PSD2* 66. panta 3. punkta g) apakšpunkts un 67. panta 2. punkta f) apakšpunkts ievērojami ierobežo apstrādes iespējas citiem nolūkiem, kas nozīmē, ka apstrāde citiem nolūkiem nav atļauta, ja vien datu subjekts nav devis piekrišanu saskaņā ar VDAR 6. panta 1. punkta a) apakšpunktu vai apstrāde nav noteikta Savienības tiesību aktos vai dalībvalsts tiesību aktos, kuri ir piemērojami pārzinim saskaņā ar VDAR 6. panta 4. punktu. Ja apstrāde citam nolūkam, nevis tam, kuram persondati ir vākti, nav pamatota ar datu subjekta piekrišanu vai Savienības vai dalībvalsts tiesību aktiem, *PSD2* 66. panta 3. punkta g) apakšpunktā un 67. panta 2. punkta f) apakšpunktā noteiktie ierobežojumi skaidri norāda, ka jebkurš cits nolūks nav saderīgs ar nolūku, kuram persondati tika sākotnēji vākti. VDAR 6. panta 4. punktā noteiktā saderības pārbaude nevar rezultātā radīt apstrādes juridisko pamatu.

24. VDAR 6. panta 4. punkts pieļauj turpmāku apstrādi, pamatojoties uz Savienības vai dalībvalsts tiesību aktiem. Piemēram, visi *PISP* un *AISP* ir atbildīgie subjekti saskaņā ar 3. panta 2. punkta a) apakšpunktu Eiropas Parlamenta un Padomes Direktīvā (ES) 2015/849 (2015. gada 20. maijs) par to, lai nepieļautu finanšu sistēmas izmantošanu nelikumīgi iegūtu līdzekļu legalizēšanai vai teroristu finansēšanai. Attiecīgi šiem atbildīgajiem subjektiem ir pienākums veikt klienta uzticamības pārbaudes pasākumus, kā noteikts direktīvā. Tāpēc persondatus, kas tiek apstrādāti

[19] VDAR 47. apsvērums.

saistībā ar *PSD2* minētu pakalpojumu, apstrādā turpmāk, pamatojoties uz vismaz vienu juridisku pienākumu, kas ir pakalpojumu sniedzējam[20].

25. Kā minēts 20. punktā, VDAR 6. panta 4. punktā norādīts, ka apstrāde citam nolūkam, nevis tam, kuram persondati ir vākti, var būt pamatota ar datu subjekta piekrišanu, ja ir izpildīti visi piekrišanas nosacījumi saskaņā ar VDAR. Kā izklāstīts iepriekš, pārzinim uzskatāmi jāparāda, ka ir iespējams atteikties vai atsaukt piekrišanu bez nelabvēlīgām sekām (VDAR 42. apsvērums).

2.5 Likumīgs pamats piekļuves piešķiršanai kontam (*ASPSP*)

26. Kā minēts 10. punktā, maksājumu pakalpojumu lietotāji var īstenot savas tiesības izmantot maksājumu iniciēšanas un konta informācijas pakalpojumus. Pienākumi, kuri dalībvalstīm noteikti *PSD2* 66. panta 1. punktā un 67. panta 1. punktā, būtu jāievieš valsts tiesību aktos, lai garantētu, ka tiek efektīvi piemērotas maksājumu pakalpojumu lietotāja tiesības gūt labumu no iepriekš minētajiem maksājumu pakalpojumiem. Šādu tiesību efektīva piemērošana nebūtu iespējama, ja *ASPSP*, parasti bankai, nebūtu atbilstoša pienākuma piešķirt maksājumu pakalpojumu sniedzējam piekļuvi kontam ar nosacījumu, ka tas ir izpildījis visas prasības, lai iegūtu piekļuvi maksājumu pakalpojumu lietotāja kontam. Turklāt *PSD2* 66. panta 5. punktā un 67. panta 4. punktā skaidri noteikts, ka maksājumu iniciēšanas pakalpojumus un konta informācijas pakalpojumus sniedz neatkarīgi no tā, vai pastāv līgumattiecības starp *PISP*/*AISP* un *ASPSP*.

27. *ASPSP* veiktā persondatu apstrāde, kas ietver piekļuves piešķiršanu *PISP* un *AISP* pieprasītajiem persondatiem, lai maksājumu pakalpojumu lietotājam sniegtu savu maksājumu pakalpojumu, ir pamatota ar juridisku pienākumu. Lai sasniegtu *PSD2* mērķus, *ASPSP* jāsniedz persondati *PISP* un *AISP* pakalpojumu vajadzībām, kas ir nepieciešams nosacījums, lai *PISP* un *AISP* varētu sniegt savus pakalpojumus un tādējādi nodrošināt *PSD2* 66. panta 1. punktā un 67. panta 1. punktā paredzētās tiesības. Tāpēc šajā gadījumā piemērojamais juridiskais pamats ir VDAR 6. panta 1. punkta c) apakšpunkts.

28. Tā kā VDAR ir precizēts, ka ar juridisku pienākumu pamatotai apstrādei vajadzētu būt skaidri noteiktai Savienības vai dalībvalsts tiesību aktos (skatīt VDAR 6. panta 3. punktu), *ASPSP* pienākumam piešķirt piekļuvi vajadzētu izrietēt no valsts tiesību aktiem, kuros ir transponēta *PSD2*.

[20] Jāņem vērā, ka rūpīga pārbaude par to, vai nelikumīgi iegūtu līdzekļu legalizācijas novēršanas direktīva atbilst VDAR 6. panta 4. punktam, neietilpst šā dokumenta darbības jomā.

3 NEPĀRPROTAMA PIEKRIŠANA

3.1 Piekrišana saskaņā ar VDAR

29. Saskaņā ar VDAR piekrišana ir viens no sešiem persondatu apstrādes likumības juridiskajiem pamatiem. VDAR 4. panta 11. punkts definē piekrišanu kā jebkuru brīvi sniegtu, konkrētu, apzinātu un vienozīmīgu norādi uz datu subjekta vēlmēm, ar kuru viņš paziņojuma vai skaidri apstiprinošas darbības veidā sniedz piekrišanu savu persondatu apstrādei. Šie četri nosacījumi — brīvi sniegta, konkrēta, apzināta un vienozīmīga — ir būtiski, lai piekrišana būtu derīga. Atbilstīgi EDAK Pamatnostādnēm 05/2020 par piekrišanu saskaņā ar Regulu 2016/679 piekrišana var būt piemērots likumīgs pamats tikai tad, ja datu subjektam tiek piedāvāta kontrole un patiesa izvēle attiecībā uz piedāvāto noteikumu pieņemšanu vai noraidīšanu vai to noraidīšanu bez kaitējuma. Lūdzot piekrišanu, pārzinim ir pienākums izvērtēt, vai tas izpildīs visas spēkā esošās piekrišanas saņemšanai piemērojamās prasības. Pilnībā ievērojot VDAR, saņemta piekrišana ir rīks, ar ko datu subjektam tiek nodrošināta kontrole attiecībā uz to, vai tā persondati tiks vai netiks apstrādāti. Pretējā gadījumā datu subjektam nav faktiskas kontroles un piekrišana nav uzskatāma par derīgu apstrādes juridisko pamatu, tādējādi apstrādes darbības kļūst nelikumīgas[21].

30. VDAR satur arī papildu drošības pasākumus, kas paredzēti 7. pantā un kas noteic, ka datu pārzinim jāspēj uzskatāmi parādīt, ka apstrādes brīdī bija sniegta derīga piekrišana. Arī piekrišanas pieprasījums jāiesniedz veidā, kas ir skaidri atšķirams no citiem jautājumiem, saprotamā un viegli pieejamā formātā, izmantojot skaidru un saprotamu valodu. Turklāt datu subjekts jāinformē par tiesībām jebkurā laikā atsaukt piekrišanu tikpat vienkāršā veidā, kādā tā piešķirta.

31. Saskaņā ar VDAR 9. pantu piekrišana ir viens no izņēmumiem no vispārējā aizlieguma apstrādāt īpašas persondatu kategorijas. Tomēr šādā gadījumā datu subjekta piekrišanai jābūt "nepārprotamai"[22].

32. Atbilstīgi EDAK Pamatnostādnēm 05/2020 par piekrišanu saskaņā ar Regulu 2016/679 VDAR minētā nepārprotamā piekrišana attiecas uz veidu, kādā datu subjekts izsaka piekrišanu. Tas nozīmē, ka datu subjektam būtu jāsniedz skaidrs piekrišanas paziņojums attiecībā uz konkrēto(-ajiem) apstrādes nolūku(-iem). Acīmredzams veids, kā pārliecināties, ka piekrišana ir nepārprotama, būtu skaidri apstiprināt piekrišanu rakstveida paziņojumā. Attiecīgā gadījumā pārzinis var pārliecināties, ka datu subjekts ir parakstījis rakstveida paziņojumu, lai nākotnē novērstu jebkādas iespējamās šaubas un iespējamo pierādījumu trūkumu.

33. Nekādā gadījumā piekrišanu nevar secināt no iespējami neskaidriem izteikumiem vai darbībām. Pārzinim arī jāuzmanās, lai šāda piekrišana nevarētu tikt iegūta vienlaicīgi ar piekrišanu līgumam vai pieņemot vispārīgos pakalpojuma sniegšanas noteikumus.

3.2 Piekrišana saskaņā ar *PSD2*

34. EDAK atzīmē, ka tiesiskais regulējums attiecībā uz nepārprotamu piekrišanu ir komplicēts, jo gan *PSD2*, gan VDAR ietver jēdzienu "nepārprotama piekrišana". Tas izraisa jautājumu, vai "nepārprotama piekrišana", kas minēta *PSD2* 94. panta 2. punktā, būtu jāinterpretē tāpat kā nepārprotama piekrišana saskaņā ar VDAR.

[21] Pamatnostādnes 05/2020 par piekrišanu saskaņā ar Regulu 2016/679, EDAK, 3. punkts.
[22] Skatīt arī Atzinumu 15/2011 par piekrišanas definīciju (WP 187), 6.–8. lpp., un/vai Atzinumu 06/2014 par datu pārziņa leģitīmajām interesēm atbilstīgi Direktīvas 95/46/EK 7. pantam (WP 217), 9., 10., 13. un 14. lpp.

3.2.1 Nepārprotama piekrišana saskaņā ar *PSD2* 94. panta 2. punktu

35. *PSD2* ietver vairākus īpašus noteikumus attiecībā uz persondatu apstrādi, jo īpaši *PSD2* 94. panta 1. punktā, kas nosaka, ka persondatu apstrādei, kas tiek veikta *PSD2* vajadzībām, jāatbilst ES datu aizsardzības tiesību aktiem. Turklāt *PSD2* 94. panta 2. punkts paredz, ka maksājumu pakalpojumu sniedzēji piekļūst persondatiem, kuri nepieciešami to maksājumu pakalpojumu sniegšanai, apstrādā un glabā tos tikai ar maksājumu pakalpojumu lietotāja nepārprotamu piekrišanu. Saskaņā ar *PSD2* 33. panta 2. punktu šī prasība par maksājumu pakalpojumu lietotāja nepārprotamu piekrišanu neattiecas uz *AISP*. Tomēr *PSD2* 67. panta 2. punkta a) apakšpunkts joprojām paredz, ka nepieciešama nepārprotama piekrišana *AISP* pakalpojumu sniegšanai.

36. Kā minēts iepriekš, likumīgo pamatu saraksts apstrādei saskaņā ar VDAR ir pilnīgs. Kā minēts 14. punktā, juridiskais pamats persondatu apstrādei, lai sniegtu maksājumu pakalpojumus, būtībā ir VDAR 6. panta 1. punkta b) apakšpunkts, kas nozīmē, ka apstrāde ir nepieciešama, lai izpildītu līgumu, kurā viena no pusēm ir datu subjekts, vai lai veiktu attiecīgas darbības pēc datu subjekta pieprasījuma pirms līguma noslēgšanas. No tā izriet, ka *PSD2* 94. panta 2. punktu nevar uzskatīt par papildu juridisko pamatu persondatu apstrādei. EDAK uzskata, ka, ņemot vērā iepriekš minēto, šis punkts būtu jāinterpretē, no vienas puses, saskaņā ar piemērojamo datu aizsardzības tiesisko regulējumu un, no otras puses, tādā veidā, lai saglabātu tā vēlamo ietekmi. Tāpēc nepārprotama piekrišana saskaņā ar *PSD2* 94. panta 2. punktu būtu jāuzskata par līgumiska rakstura papildu prasību[23] attiecībā uz piekļuvi persondatiem un turpmāku apstrādi un glabāšanu maksājumu pakalpojumu sniegšanas nolūkā, un tāpēc tā nav tāda pati kā (nepārprotama) piekrišana saskaņā ar VDAR.

37. Nepārprotama piekrišana, kas minēta *PSD2* 94. panta 2. punktā, ir līgumiska piekrišana. Tas nozīmē, ka *PSD2* 94. panta 2. punkts būtu jāinterpretē tādā izpratnē, ka, noslēdzot līgumu ar maksājumu pakalpojumu sniedzēju saskaņā ar *PSD2*, datu subjektiem pilnībā jāiepazīstas ar īpašajām apstrādājamo persondatu kategorijām. Turklāt datu subjekti jāinformē par konkrēto (maksājumu pakalpojumu) nolūku, kādam tiks apstrādāti viņu persondati, un viņiem nepārprotami jāpiekrīt attiecīgajiem noteikumiem. Šādiem noteikumiem vajadzētu būt skaidri nošķiramiem no citiem līgumā aplūkotajiem jautājumiem, un datu subjektam tie nepārprotami būtu jāakceptē.

38. Galvenais jēdziena "nepārprotama piekrišana" elements saskaņā ar *PSD2* 94. panta 2. punktu ir piekļuves ieguve persondatiem, lai pēc tam apstrādātu un uzglabātu šos datus maksājumu pakalpojumu sniegšanas nolūkā. Tas nozīmē, ka maksājumu pakalpojumu[24] sniedzējs vēl neapstrādā persondatus, bet viņam ir nepieciešama piekļuve persondatiem, kas ir apstrādāti kāda cita pārziņa pārraudzībā. Ja maksājumu pakalpojumu lietotājs noslēdz līgumu, piemēram, ar maksājumu iniciēšanas pakalpojumu sniedzēju, šim pakalpojumu sniedzējam jāiegūst piekļuve maksājumu pakalpojumu lietotāja persondatiem, kas tiek apstrādāti kontu apkalpojošā maksājumu pakalpojumu sniedzēja pārraudzībā. Saskaņā ar *PSD2* 94. panta 2. punktu nepārprotamas piekrišanas mērķis ir iegūt atļauju piekļuvei minētajiem persondatiem, lai varētu apstrādāt un uzglabāt šos persondatus, kas nepieciešami maksājumu pakalpojumu sniegšanai. Ja datu subjekts ir devis nepārprotamu piekrišanu, kontu apkalpojošajam maksājumu pakalpojumu sniedzējam jāpiešķir piekļuve norādītajiem persondatiem.

39. Kaut arī *PSD2* 94. panta 2. punktā minētā piekrišana nav juridisks pamats persondatu apstrādei, šī piekrišana īpaši attiecas uz persondatiem un datu aizsardzību un nodrošina pārredzamību, kā arī

[23] EDAK vēstule par *PSD2* direktīvu, 2018. gada 5. jūlijs, 4. lpp.
[24] Tas attiecas uz 1. līdz 7. pakalpojumu *PSD2* 1. pielikumā.

zināmas kontroles iespējas maksājumu pakalpojumu lietotājam[25]. Lai gan *PSD2* nav norādīti pamatnosacījumi piekrišanai saskaņā ar *PSD2* 94. panta 2. punktu, piekrišana, kā minēts iepriekš, būtu jāsaprot saskaņā ar piemērojamo datu aizsardzības tiesisko regulējumu un tādā veidā, kas saglabā tās vēlamo ietekmi.

40. Attiecībā uz informāciju, kas pārziņiem jāsniedz, un pārredzamību 29. panta darba grupas Pārredzamības pamatnostādnēs ir noteikts, ka "*[g]alvenais apsvērums attiecībā uz šajos noteikumos izklāstīto pārredzamības principu ir tas, ka datu subjektam vajadzētu būt iespējai iepriekš noteikt, kāds ir apstrādes tvērums un sekas, un ka viņam vēlāk nevajadzētu būt pārsteigtam par viņa personas datu [persondatu] izmantošanas veidiem*"[26].

41. Turklāt, kā nosaka nolūka ierobežojumu princips, persondati jāvāc konkrētos, skaidros un leģitīmos nolūkos (VDAR 5. panta 1. punkta b) apakšpunkts). Gadījumos, kad persondati tiek vākti vairāk nekā vienam nolūkam, "*pārziņiem vajadzētu izvairīties identificēt tikai vienu plašu nolūku, lai pamatotu dažādas turpmākas apstrādes darbības, kas būtībā ir tikai attālināti saistītas ar faktisko sākotnējo nolūku*"[27]. EDAK pēdējā laikā saistībā ar tiešsaistes pakalpojumu līgumiem ir uzsvērusi risku, ka līgumos tiks iekļauti vispārīgi apstrādes noteikumi, un paziņojusi, ka skaidri un konkrēti būtu jānosaka vākšanas nolūks: Tam vajadzētu būt pietiekami detalizētam, lai noteiktu, kāda veida apstrāde ir vai nav iekļauta konkrētajā nolūkā, kā arī ļautu novērtēt tiesību aktu ievērošanu un piemērot datu aizsardzības pasākumus[28].

42. Aplūkojot iepriekšminēto saistībā ar papildu prasību par nepārprotamu piekrišanu saskaņā ar *PSD2* 94. panta 2. punktu, tas nozīmē, ka pārziņiem jāsniedz datu subjektiem konkrēta un skaidra informācija par īpašiem pārziņa noteiktiem nolūkiem, kādos tiek piekļūts subjektu persondatiem, tie tiek apstrādāti un saglabāti. Saskaņā ar *PSD2* 94. panta 2. punktu datu subjektiem skaidri jāakceptē šie konkrētie nolūki.

43. Turklāt, kā norādīts iepriekš 10. punktā, EDAK uzsver, ka maksājumu pakalpojumu lietotājam jābūt iespējai izvēlēties, vai izmantot pakalpojumu, un viņu nevar piespiest to darīt. Tāpēc piekrišanai saskaņā ar *PSD2* 94. panta 2. punktu jābūt arī brīvi dotai piekrišanai.

3.3 Secinājums

44. Nepārprotama piekrišana saskaņā ar *PSD2* atšķiras no (nepārprotamas) piekrišanas saskaņā ar VDAR. Nepārprotama piekrišana saskaņā ar *PSD2* 94. panta 2. punktu ir papildu līgumiska rakstura prasība. Ja maksājumu pakalpojumu sniedzējam jāpiekļūst persondatiem, lai sniegtu maksājumu pakalpojumu, vajadzīga maksājumu pakalpojumu lietotāja nepārprotama piekrišana saskaņā ar *PSD2* 94. panta 2. punktu.

[25] *PSD2* 94. panta 2. punkts ietilpst 4. nodaļā "Datu aizsardzība".
[26] 29. panta darba grupas Pārredzamības pamatnostādnes saskaņā ar Regulu 2016/679, 10. punkts (pieņemtas 2018. gada 11. aprīlī) — apstiprinājusi EDAK.
[27] 29. panta darba grupas Atzinums 03/2013 par nolūka ierobežošanu (WP203), 16. lpp.
[28] Pamatnostādnes 2/2019 par personas datu [persondatu] apstrādi saskaņā ar VDAR 6. panta 1. punkta b) apakšpunktu, sniedzot tiešsaistes pakalpojumus datu subjektiem, 16. punkts (sabiedriskās apspriešanas versija) un 29. panta darba grupas Atzinums 03/2013 par nolūka ierobežošanu (WP203), 15. un 16. lpp.

4 KLUSO PERSONU DATU APSTRĀDE

4.1 Kluso personu dati

45. Rūpīgi jāapsver tāds datu aizsardzības jautājums kā "kluso personu datu" apstrāde. Šā dokumenta kontekstā kluso personu dati ir persondati par datu subjektu, kurš nav konkrēta maksājumu pakalpojumu sniedzēja pakalpojumu lietotājs, bet kura persondatus šis konkrētais maksājumu pakalpojumu sniedzējs apstrādā, lai izpildītu līgumu starp pakalpojumu sniedzēju un maksājumu pakalpojumu lietotāju. Tā notiek, piemēram, gadījumā, kad maksājumu pakalpojumu lietotājs, datu subjekts A, izmanto *AISP* pakalpojumus, un datu subjekts B ir veicis virkni maksājumu datu subjekta A maksājumu kontā. Šajā gadījumā datu subjekts B tiek uzskatīts par "kluso personu", un persondati (piemēram, datu subjekta B konta numurs un šajos darījumos iesaistītā naudas summa), kas saistīti ar datu subjektu B, tiek uzskatīti par "klusās personas datiem".

4.2 Pārziņa leģitīmās intereses

46. VDAR 5. panta 1. punkta b) apakšpunkts paredz, ka persondati jāvāc tikai konkrētiem, skaidriem un leģitīmiem nolūkiem un tos nedrīkst papildus apstrādāt tādā veidā, kas nav saderīgs ar šiem nolūkiem. Turklāt VDAR noteikts, ka jebkāda veida persondatu apstrādei jābūt nepieciešamai un samērīgai, kā arī jāatbilst datu aizsardzības principiem, piemēram, nolūka ierobežošanas un datu minimizēšanas principiem.

47. VDAR var atļaut apstrādāt kluso personu datus, ja šī apstrāde ir nepieciešama pārziņa vai trešās personas leģitīmo interešu vajadzībām (VDAR 6. panta 1. punkta f) apakšpunkts). Tomēr šāda apstrāde var notikt tikai tad, ja "datu subjekta intereses vai pamattiesības un pamatbrīvības, kurām nepieciešama personas datu [persondatu] aizsardzība" nav svarīgākas par pārziņa leģitīmajām interesēm.

48. Tādējādi likumīgs pamats kluso personu datu apstrādei, ko veic *PISP* un *AISP*, saistībā ar maksājumu pakalpojumu sniegšanu saskaņā ar *PSD2* varētu būt pārziņa vai trešās personas leģitīmās intereses izpildīt līgumu ar maksājumu pakalpojumu lietotāju. Nepieciešamību apstrādāt klusās personas persondatus ierobežo un nosaka šo datu subjektu saprātīgas gaidas. Tādu maksājumu pakalpojumu sniegšanas kontekstā, uz kuriem attiecas *PSD2*, jānosaka efektīvi un atbilstoši pasākumi, lai nodrošinātu, ka netiek aizskartas kluso personu intereses vai pamattiesības un brīvības un ka tiek respektētas šo datu subjektu saprātīgās gaidas attiecībā uz viņu persondatu apstrādi. Šajā saistībā pārzinim (*AISP* vai *PISP*) jānosaka apstrādei nepieciešamie drošības pasākumi, lai aizsargātu datu subjektu tiesības. Tie ietver tehniskus pasākumus, lai nodrošinātu, ka kluso personu dati netiek apstrādāti citam nolūkam, izņemot nolūku, kādam persondatus sākotnēji vāca *PISP* un *AISP*. Ja iespējams, būtu jāpiemēro arī šifrēšana vai citas metodes, lai sasniegtu atbilstošu drošības un datu minimizēšanas līmeni.

4.3 Klusās personas datu turpmāka apstrāde

49. Kā norādīts 29. punktā, persondatus, kas apstrādāti saistībā ar maksājumu pakalpojumu, kuru reglamentē *PSD2*, var apstrādāt turpmāk, pamatojoties uz juridiskajiem pienākumiem, kas ir pakalpojumu sniedzējam. Šie juridiskie pienākumi varētu attiekties uz klusās personas datiem.

50. Attiecībā uz kluso personu datu turpmāku apstrādi, pamatojoties uz leģitīmām interesēm, EDAK uzskata, ka šos datus nevar izmantot citiem nolūkiem, izņemot tos, kuriem persondati ir vākti, ja vien ES vai dalībvalsts tiesību akti nenosaka citu pamatu. Klusās personas piekrišana juridiski nav iespējama, jo, lai iegūtu piekrišanu, būtu jāvāc vai jāapstrādā klusās personas persondati, kam nav atrodams juridisks pamats saskaņā ar VDAR 6. pantu. Arī VDAR 6. panta 4. punkta saderības

pārbaude nevar būt pamats apstrādei citiem nolūkiem (piemēram, tiešās tirgvedības darbībām). Šo kluso personu datu subjektu tiesības un brīvības netiks ievērotas, ja jaunais datu pārzinis izmantos persondatus citiem nolūkiem, ņemot vērā kontekstu, kurā persondati ir vākti, jo īpaši gadījumos, kad nav nekādas saistības ar datu subjektiem, kuri ir klusās personas[29]; nav nekādas saiknes starp jebkādu citu nolūku un to nolūku, kādam sākotnēji tika vākti persondati (t. i. fakts, ka maksājumu pakalpojumu sniedzējiem ir nepieciešami tikai klusās personas dati, lai izpildītu līgumu ar otru līgumslēdzēju pusi); ņemot vērā iesaistīto persondatu būtību[30], apstākli, ka datu subjekti nevar pamatoti gaidīt turpmāku apstrādi vai pat apzināties, kurš pārzinis varētu apstrādāt viņu persondatus, un ņemot vērā juridiskos ierobežojumus, kas noteikti *PSD2* 66. panta 3. punkta g) apakšpunktā un 67. panta 2. punkta f) apakšpunktā.

[29] Kā norādīts *PSD2* 87. apsvērumā, šī direktīva attiecas tikai uz "maksājumu pakalpojumu lietotāja un maksājumu pakalpojumu sniedzēja savstarpējām līgumsaistībām un pienākumiem". Tāpēc kluso personu dati neietilpst *PSD2* darbības jomā.

[30] Apstrādājot personas finanšu datus, būtu jāievēro īpaša piesardzība, jo saskaņā ar Pamatnostādnēm novērtējuma par ietekmi uz datu aizsardzību veikšanai (*DPIA*) var uzskatīt, ka apstrāde palielina iespējamo risku personu tiesībām un brīvībām.

5 ĪPAŠU KATEGORIJU PERSONDATU APSTRĀDE SASKAŅĀ AR *PSD2*

5.1 Īpašu kategoriju persondati

51. Saskaņā ar VDAR 9. panta 1. punktu ir aizliegta "tādu personas datu [persondatu] apstrāde, kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās, un ģenētisko datu, biometrisko datu, lai veiktu fiziskas personas unikālu identifikāciju, veselības datu vai datu par fiziskas personas dzimumdzīvi vai seksuālo orientāciju apstrāde".

52. Būtu jāuzsver, ka dažās dalībvalstīs elektroniskie maksājumi jau ir pašsaprotami un daudzi cilvēki ikdienas darījumos dod priekšroku tiem, nevis skaidrai naudai. Tomēr finanšu darījumi var atklāt sensitīvu informāciju par atsevišķu datu subjektu, tostarp datu subjektiem, kuri saistīti ar īpašām persondatu kategorijām. Darījuma detaļas var norādīt uz politiskajiem uzskatiem un reliģisko pārliecību, piemēram, ziedojumi politiskajām partijām vai organizācijām, baznīcām vai draudzēm. Savukārt uz dalību arodbiedrībā var norādīt gada biedra naudas atskaitījumi no personas bankas konta. Persondatus par veselību var apkopot, analizējot medicīniskos rēķinus, ko datu subjekts apmaksājis profesionālam medicīnas darbiniekam (piemēram, psihiatram). Visbeidzot, informācija par konkrētiem pirkumiem var atklāt informāciju par personas seksuālo dzīvi vai dzimumorientāciju. Kā rāda šie piemēri, pat atsevišķi darījumi var saturēt īpašu kategoriju persondatus. Turklāt konta informācijas pakalpojumu sniedzēji var paļauties uz profilēšanu, kā noteikts VDAR 4. panta 4. punktā. Kā iepriekš minēts 29. panta darba grupas Pamatnostādnēs par automatizētu individuālu lēmumu pieņemšanu un profilēšanu Regulas 2016/679 nolūkiem un kā apstiprināja EDAK, "[p]rofilēšanas rezultātā var izveidot īpašo kategoriju datus, tos izsecinot no datiem, kas nav īpašo kategorijas dati, bet kļūst par tādiem apvienojumā ar citiem datiem"[31]. Tas nozīmē, ka, pamatojoties uz finanšu darījumu summu, var atklāt dažādu veidu rīcības modeļus, kas var ietvert īpašu kategoriju persondatus. Tāpēc pastāv liela iespēja, ka pakalpojumu sniedzējs, kas apstrādā informāciju par datu subjektu finanšu darījumiem, apstrādā arī īpašu kategoriju persondatus.

53. Attiecībā uz terminu "sensitīvi maksājumu dati" EDAK ir šāds viedoklis. *PSD2* sensitīvu maksājumu datu definīcija ievērojami atšķiras no tā, kā termins "sensitīvi persondati" parasti tiek izmantots VDAR un datu aizsardzības (tiesību aktu) kontekstā. Saskaņā ar *PSD2* "sensitīvi maksājumu dati" ir "dati, tostarp personalizēti drošības dati, ko var izmantot krāpnieciskā nolūkā", savukārt VDAR uzsver nepieciešamību nodrošināt specifisku aizsardzību īpašu kategoriju persondatiem, kuri saskaņā ar VDAR 9. pantu ir pēc būtības īpaši jutīgi saistībā a pamattiesībām un brīvībām, piemēram, īpašu kategoriju persondati[32]. Šajā saistībā ieteicams vismaz precīzi plānot un kategorizēt, kādi persondati tiks apstrādāti. Visticamāk, saskaņā ar VDAR 35. pantu būs nepieciešams novērtējums par ietekmi uz datu aizsardzību (*DPIA*), kas palīdzēs šajā plānošanas uzdevumā. Vairāk norādījumu par *DPIA* var skatīt 29. panta darba grupas Pamatnostādnēs novērtējuma par ietekmi uz datu aizsardzību (*DPIA*) veikšanai un noteikšanai, vai apstrāde "varētu radīt augstu risku" Regulas 2016/679 izpratnē — apstiprinājusi EDAK.

[31] 29. panta Datu aizsardzības darba grupa, Pamatnostādnes par automatizētu individuālu lēmumu pieņemšanu un profilēšanu Regulas 2016/679 nolūkiem, WP251rev.01, 15. lpp.
[32] Piemēram, VDAR 10. apsvērumā īpašu kategoriju persondati tiek dēvēti par "sensitīviem datiem".

5.2 Iespējamās atkāpes

54. VDAR 9. pantā noteiktais aizliegums nav absolūts. Proti, gadījumos, kad VDAR 9. panta 2. punkta b)–f) un h)–j) apakšpunktā noteiktās atkāpes acīmredzami nav piemērojamas persondatu apstrādei *PSD2* kontekstā, var apsvērt divas turpmāk minētās atkāpes, ko paredz VDAR 9. panta 2. punkts:

a) aizliegums nav piemērojams, ja datu subjekts ir devis nepārprotamu piekrišanu minēto persondatu apstrādei vienam vai vairākiem noteiktiem nolūkiem (VDAR 9. panta 2. punkta a) apakšpunkts);

b) aizliegums nav piemērojams, ja apstrāde ir nepieciešama būtisku sabiedrības interešu dēļ, pamatojoties uz Savienības vai dalībvalsts tiesību aktiem, kas ir samērīgi izvirzītajam mērķim, ievēro tiesību uz datu aizsardzību būtību un paredz piemērotus un konkrētus pasākumus datu subjekta pamattiesību un interešu aizsardzībai (VDAR 9. panta 2. punkta g) apakšpunkts).

55. Būtu jāatzīmē, ka VDAR 9. panta 2. punktā minēto izņēmumu saraksts ir pilnīgs. Pakalpojumu sniedzējam jāatzīst, ka pastāv iespēja, ka persondatos, kuri tiek apstrādāti, lai sniegtu kādu no *PSD2* aptvertajiem pakalpojumiem, tiek iekļauti īpašu kategoriju persondati. Tā kā uz minētajiem pakalpojumu sniedzējiem attiecas VDAR 9. panta 1. punktā noteiktais aizliegums, viņiem jānodrošina, ka tiek piemērots viens no VDAR 9. panta 2. punktā paredzētajiem izņēmumiem. Būtu jāuzsver, ka gadījumos, kad pakalpojumu sniedzējs nevar pierādīt, ka tas atbilst vienai no atkāpēm, ir piemērojams 9. panta 1. punktā noteiktais aizliegums.

5.3 Būtiskas sabiedrības intereses

56. Maksājumu pakalpojumu sniedzēji var apstrādāt īpašu kategoriju persondatus būtisku sabiedrības interešu dēļ, bet tikai tad, ja ir izpildīti visi VDAR 9. panta 2. punkta g) apakšpunkta nosacījumi. Tas nozīmē, ka īpašo kategoriju persondatu apstrāde jārisina, iekļaujot konkrētu atkāpi no VDAR 9. panta 1. punkta Savienības vai dalībvalsts tiesību aktos. Šajā noteikumā jābūt aplūkotam samērīgumam attiecībā pret izvirzīto apstrādes nolūku un jāietver piemēroti un konkrēti pasākumi datu subjekta pamattiesību un interešu aizsardzībai. Turklāt šajā noteikumā saskaņā ar Savienības vai dalībvalsts tiesību aktiem būs jāņem vērā tiesību uz datu aizsardzību būtība. Visbeidzot, arī jāpierāda, ka īpašo kategoriju datu apstrāde ir nepieciešama būtisku sabiedrības interešu, tostarp sistēmiskas nozīmes interešu, dēļ. Tikai tad, kad ir pilnīgi izpildīti visi minētie nosacījumi, šo atkāpi var piemērot noteiktiem maksājumu pakalpojumu veidiem.

5.4 Nepārprotama piekrišana

57. Gadījumos, kad VDAR 9. panta 2. punkta g) apakšpunkta atkāpe nav piemērojama, šķiet, ka nepārprotamas piekrišanas iegūšana saskaņā ar VDAR derīgas piekrišanas nosacījumiem joprojām ir vienīgā iespējamā likumīgā atkāpe, lai *TPP* varētu apstrādāt īpašu kategoriju persondatus. EDAK Pamatnostādnēs 05/2020 par piekrišanu saskaņā ar Regulu 2016/679 noteikts[33]: "Regulas 9. panta 2. punkts neatzīst pamatojumu "vajadzīgs līguma izpildei" kā izņēmumu vispārējam aizliegumam apstrādāt īpašu kategoriju datus. Tādēļ pārziņiem un dalībvalstīm, kas saskaras šo situāciju, būtu jāizpēta 9. panta 2. punkta b) līdz j) apakšpunktā minētie īpaši izņēmumi." Ja pakalpojumu sniedzēji paļaujas uz VDAR 9. panta 2. punkta a) apakšpunktu, pakalpojumu sniedzējiem pirms apstrādes sākšanas jāpārliecinās, ka tiem ir dota nepārprotama piekrišana. VDAR 9. panta 2. punkta a) apakšpunktā noteiktajai nepārprotamajai piekrišanai jāatbilst visām VDAR prasībām.

[33] Pamatnostādnes 05/2020 par piekrišanu saskaņā ar Regulu 2016/679, EDAK, 99. punkts.

5.5 Nav piemērotas atkāpes

58. Kā minēts iepriekš, gadījumos, kad pakalpojumu sniedzējs nevar pierādīt, ka tas atbilst vienai no atkāpēm, ir piemērojams 9. panta 1. punktā noteiktais aizliegums. Šajā gadījumā varētu ieviest tehniskus pasākumus, lai novērstu īpašu kategoriju persondatu apstrādi, piemēram, novēršot konkrētu datu punktu apstrādi. Šajā saistībā maksājumu pakalpojumu sniedzēji var izpētīt tehniskās iespējas izslēgt īpašu kategoriju persondatus un nodrošināt izvēlētu piekļuvi, kas neļautu *TPP* apstrādāt īpašu kategoriju persondatus, kuri saistīti ar klusajām personām.

6 DATU MINIMIZĒŠANA, DROŠĪBA, PĀRREDZAMĪBA, PĀRSKATATBILDĪBA UN PROFILĒŠANA

6.1 Datu minimizēšana, integrētā datu aizsardzība un datu aizsardzība pēc noklusējuma

59. Datu minimizēšanas princips ir nostiprināts VDAR 5. panta 1. punkta c) apakšpunktā: "Personas dati [persondati] ir [..] adekvāti, atbilstīgi un ietver tikai to, kas nepieciešams to apstrādes nolūkos". Būtībā saskaņā ar datu minimizēšanas principu pārziņiem nevajadzētu apstrādāt vairāk persondatu, kā nepieciešams konkrētajam nolūkam. Kā norādīts 2. nodaļā, maksājumu pakalpojumu sniegšanai nepieciešamo persondatu apjomu un veidu nosaka objektīvais un abām pusēm saprotamais līguma nolūks[34]. Datu minimizēšana ir piemērojama jebkurai apstrādei (piemēram, ikvienam gadījumam, kad tiek vākti persondati, piekļūts tiem vai tie tiek pieprasīti). EDAK Pamatnostādnēs 4/2019 par 25. pantā paredzēto integrēto datu aizsardzību un datu aizsardzību pēc noklusējuma (*Data Protection by Design and by Default, DPbDD*) norādīts, ka "arī apstrādāji un tehnoloģiju nodrošinātāji tiek uzskatīti par galvenajiem *DPbDD* nodrošinātājiem, un viņiem arī vajadzētu būt informētiem, ka pārziņiem ir pienākums apstrādāt persondatus tikai ar sistēmām un tehnoloģijām, kurām ir iebūvēta datu aizsardzība"[35].

60. VDAR 25. pantā ir noteikti pienākumi piemērot integrēto datu aizsardzību un datu aizsardzību pēc noklusējuma. Šie pienākumi ir īpaši svarīgi saistībā ar datu minimizēšanas principu. Šis pants nosaka, ka pārziņiem gan apstrādes līdzekļu noteikšanas laikā, gan pašas apstrādes laikā jāīsteno atbilstoši tehniskie un organizatoriskie pasākumi, kas ir paredzēti datu aizsardzības principu efektīvai piemērošanai un nepieciešamo drošības pasākumu integrēšanai apstrādē, lai izpildītu VDAR prasības un aizsargātu datu subjektu tiesības. Pārzinis īsteno atbilstošus tehniskus un organizatoriskus pasākumus, lai nodrošinātu, ka pēc noklusējuma tiek apstrādāti tikai tādi persondati, kas ir nepieciešami katram konkrētajam apstrādes nolūkam. Minētais pienākums attiecas uz vākto persondatu apjomu, to apstrādes pakāpi, glabāšanas laikposmu un to pieejamību. Šie pasākumi var ietvert šifrēšanu, pseidonimizāciju un citus tehniskus pasākumus.

61. Ja tiek piemērots VDAR 25. pantā noteiktais pienākums, jāņem vērā tehnikas līmenis, ieviešanas izmaksas un apstrādes veids, joma, konteksts un nolūki, kā arī dažādu apstrādes radīto risku iespējamības un smaguma pakāpe attiecībā uz fizisko personu tiesībām un brīvībām. Papildu skaidrojumi par šo pienākumu ir sniegti iepriekš minētajās EDAK Pamatnostādnēs 4/2019 par 25. pantā paredzēto integrēto datu aizsardzību un datu aizsardzību pēc noklusējuma.

6.2 Datu minimizēšanas pasākumi

62. *TPP*, piekļūstot maksājumu konta datiem, lai sniegtu pieprasītos pakalpojumus, jāņem vērā arī datu minimizēšanas princips un jāvāc tikai persondati, kas nepieciešami, lai sniegtu konkrētos maksājumu pakalpojumus, kurus pieprasījis maksājumu pakalpojumu lietotājs. Principā piekļuvei persondatiem vajadzētu būt tikai tādā mērā, kas nepieciešams maksājumu pakalpojumu sniegšanai. Kā atspoguļots 2. nodaļā, *PSD2* nosaka, ka *ASPSP* pēc maksājumu pakalpojumu lietotāja pieprasījuma apmainās ar maksājumu pakalpojumu lietotāju informāciju, ja maksājumu

[34] Pamatnostādnes 2/2019 par personas datu [persondatu] apstrādi saskaņā ar VDAR 6. panta 1. punkta b) apakšpunktu, sniedzot tiešsaistes pakalpojumus datu subjektiem, EDAK, 32. punkts.
[35] Pamatnostādnes 4/2019 par 25. pantā paredzēto integrēto datu aizsardzību un datu aizsardzību pēc noklusējuma, 29. lpp.

pakalpojumu lietotājs vēlas izmantot maksājuma iniciēšanas pakalpojumu vai konta informācijas pakalpojumu.

63. Ja līguma izpildei nav nepieciešami visi maksājumu konta dati, pirms datu vākšanas *AISP* būtu jāizvēlas attiecīgās datu kategorijas. Piemēram, datu kategorijas, kas var nebūt vajadzīgas, var ietvert klusās personas identitāti un darījuma pazīmes. Turklāt, ja vien to neprasa dalībvalsts vai ES tiesību akti, var nebūt nepieciešams norādīt klusās personas bankas konta IBAN.

64. Šajā saistībā saskaņā ar VDAR 24. panta 2. punktu var apsvērt piemērotas datu aizsardzības politikas ietvaros īstenot tehniskos pasākumus, kas palīdz vai atbalsta *TPP* viņu pienākumā piekļūt tikai pakalpojumu sniegšanai nepieciešamajiem persondatiem un izgūt tos. Šādā nolūkā EDAK iesaka izmantot digitālos rīkus, lai atbalstītu *AISP* pienākumā vākt tikai tādus persondatus, kas nepieciešami nolūkiem, kuriem tie tiek apstrādāti. Piemēram, ja pakalpojumu sniedzējam pakalpojumu sniegšanai nav nepieciešami darījuma raksturlielumi (darījuma informācijas aprakstošajā laukā), digitālās atlases rīks varētu darboties kā līdzeklis *TPP* vajadzībām, lai *TPP* varētu izslēgt šo lauku no kopējām apstrādes darbībām.

2. piemērs.

HappyPayments, konta informācijas pakalpojuma sniedzējs, kas minēts 1. piemērā, vēlas nodrošināt, ka tas apstrādā tikai tādus personas maksājumu konta datus, kuros ir ieinteresēti pakalpojuma lietotāji. Pakalpojuma sniegšanai nebūtu nepieciešama piekļuve vairākiem maksājumu konta datiem. Tāpēc tas ļauj lietotājiem izvēlēties konkrētus interesējošās informācijas veidus.

Lietotājs A vēlas pārskatīt savus izdevumus par pēdējiem diviem mēnešiem. Attiecīgi tas pieprasa no saviem diviem bankas kontiem, kas atrodas divu dažādu *ASPSP* turējumā, informāciju par visiem pēdējo divu mēnešu darījumiem, darījuma summu, izpildes datumu un saņēmēja vārdu un atzīmē attiecīgās rūtiņas *HappyPayments* lietotāja saskarnē.

Tad *HappyPayments* sāk pieprasīt no attiecīgajiem *ASPSP* tikai informāciju, kas atbilst lietotāja A iestatītajiem laukiem, un tikai par pēdējo divu mēnešu periodu. Tāda informācija kā paziņojums par pārskaitījumu vai pat IBAN nav nepieciešama, jo lietotājs A šo informāciju nav prasījis.

Lai *HappyPayments* varētu pildīt savus datu minimizēšanas pienākumus, *ASPSP* ļauj uzņēmumam pieprasīt noteiktus laukus datumu diapazona norādīšanai.

65. Šajā saistībā arī būtu jāatzīmē, ka atbilstīgi *PSD2 ASPSP* ir atļauts nodrošināt piekļuvi tikai maksājumu kontu informācijai. Saskaņā ar *PSD2* nav juridiska pamata nodrošināt piekļuvi persondatiem, ko satur citi konti, piemēram, uzkrājumu, hipotēkas vai ieguldījumu konti. Attiecīgi saskaņā ar *PSD2* jāīsteno tehniski pasākumi, lai nodrošinātu, ka piekļuve aprobežojas ar nepieciešamo maksājumu konta informāciju.

66. Papildus tam, lai vāktu pēc iespējas mazāk datu, pakalpojumu sniedzējam jāievieš arī ierobežoti glabāšanas periodi. Pakalpojumu sniedzējam persondati nebūtu jāuzglabā ilgāk, kā nepieciešams maksājumu pakalpojumu lietotāja pieprasītajiem nolūkiem.

67. Ja līgums starp datu subjektu un *AISP* pieprasa persondatu pārsūtīšanu trešām personām, tad var nosūtīt tikai tādus persondatus, kuri nepieciešami līguma izpildei. Datu subjekti arī būtu īpaši jāinformē par nosūtīšanu un to, kādi persondati tiks nosūtīti šai trešai pusei.

6.3 Drošība

68. EDAK jau uzsvēra, ka personas finanšu datu pārkāpums "*nepārprotami rada nopietnu ietekmi uz datu subjekta ikdienas dzīvi*", un kā piemēru min ar maksājumiem saistītas krāpšanas riskus[36].

69. Ja datu pārkāpums ir saistīts ar finanšu datiem, datu subjekts var būt pakļauts būtiskam riskam. Atkarībā no nopludinātās informācijas datu subjekti var tikt pakļauti identitātes zādzības, viņu kontos esošo līdzekļu un citu aktīvu zādzības riskam. Turklāt pastāv iespēja, ka darījumu dati ir pakļauti ievērojamam privātuma riskam, jotie var saturēt atsauces uz visiem datu subjekta privātās dzīves aspektiem. Turklāt finanšu dati ir acīmredzami vērtīgi noziedzniekiem un tādējādi ir pievilcīgs mērķis.

70. Maksājumu pakalpojumu sniedzējiem kā datu pārziņiem ir pienākums veikt pietiekamus pasākumus, lai aizsargātu datu subjektu persondatus (VDAR 24. panta 1. punkts). Jo augstāki riski ir saistīti ar pārziņa veiktajām apstrādes darbībām, jo augstāki drošības standarti jāpiemēro. Tā kā finanšu datu apstrāde ir saistīta ar dažādiem nopietniem riskiem, drošības pasākumu līmenim vajadzētu būt attiecīgi augstam.

71. Pakalpojumu sniedzējiem būtu jāatbilst augstiem standartiem, tostarp jāizmanto stingri klientu autentifikācijas mehānismi un jāpiemēro augsti tehniskā aprīkojuma drošības standarti[37]. Svarīgas ir arī citas procedūras, piemēram, apstrādātāju pārbaude attiecībā uz drošības standartiem un procedūru ieviešana pret nesankcionētu piekļuvi.

6.4 Pārredzamība un pārskatatbildība

72. Pārredzamība un pārskatatbildība ir divi VDAR pamatprincipi.

73. Attiecībā uz pārredzamību (VDAR 5. panta 1. punkta a) apakšpunkts) VDAR 12. pants nosaka, ka pārziņi veic attiecīgus pasākumus, lai sniegtu jebkādu VDAR 13. un 14. pantā minēto informāciju. Turklāt tas paredz, ka informācijai vai paziņojumam par persondatu apstrādi jābūt kodolīgam, pārredzamam, saprotamam un viegli pieejamam. Informācijai jābūt skaidrā un saprotamā valodā un rakstveidā "vai citā veidā, tostarp – vajadzības gadījumā – elektroniskā formā". EDAK apstiprinātajās 29. panta darba grupas Pārredzamības pamatnostādnēs saskaņā ar Regulu 2016/679 sniegti īpaši norādījumi par pārredzamības principa ievērošanu digitālajās vidēs.

74. Atbilstīgi Pārredzamības pamatnostādnēm saskaņā ar Regulu 2016/679 VDAR 11. pants būtu jāinterpretē kā veids, kā īstenot patiesu datu minimizēšanu, netraucējot datu subjektu tiesību izmantošanu, un datu subjektu tiesību izmantošana būtu jāpadara iespējama ar datu subjekta sniegtas papildu informācijas palīdzību. Var būt situācijas, kurās datu pārzinis apstrādā persondatus, kam nav nepieciešama datu subjekta identifikācija (piemēram, pseidonimizētus datus). Šādos gadījumos 11. panta 1. punkts var būt būtisks arī tāpēc, ka tajā noteikts, ka datu pārzinim nav pienākuma uzturēt, iegūt vai apstrādāt papildu informāciju, lai identificētu datu subjektu tikai nolūkā ievērot VDAR.

75. Attiecībā uz pakalpojumiem saskaņā ar *PSD2* no datu subjekta savāktajiem persondatiem jāpiemēro VDAR 13. pants, bet 14. pants ir piemērojams, ja persondati nav iegūti no datu subjekta.

76. Datu subjekts īpaši jāinformē par to, cik ilgu periodu persondati tiks glabāti, vai, ja tas nav iespējams, par kritērijiem, kas izmantoti šā perioda noteikšanai, un attiecīgā gadījumā par

[36] 29. panta darba grupas Pamatnostādnes novērtējuma par ietekmi uz datu aizsardzību (*DPIA*) veikšanai un noteikšanai, vai apstrāde "varētu radīt augstu risku" Regulas 2016/679 izpratnē (WP248rev.01) — apstiprinājusi EDAK.

[37] Skatīt *RTS*.

leģitīmām interesēm, kuras jāīsteno pārzinim vai iespējamajai trešai pusei. Ja apstrādes pamatā ir VDAR 6. panta 1. punkta a) apakšpunktā minētā piekrišana vai nepārprotama piekrišana saskaņā ar VDAR 9. panta 2. punkta a) apakšpunktu, datu subjekts jāinformē par tiesībām atsaukt piekrišanu jebkurā laikā.

77. Pārzinis sniedz informāciju datu subjektam, ņemot vērā īpašos apstākļus, kādos persondati tiek apstrādāti. Ja persondatus paredzēts izmantot saziņai ar datu subjektu[38], kā tas, iespējams, būs *AISP* gadījumā, informācija jāsniedz, vēlākais, brīdī, kad notiek pirmā saziņa ar šo datu subjektu. Ja persondati jāatklāj citam saņēmējam, informācija jāsniedz, vēlākais, tad, kad persondati pirmo reizi tiek atklāti.

78. Attiecībā uz tiešsaistes maksājumu pakalpojumiem iepriekš minētajās pamatnostādnēs ir paskaidrots, ka datu pārziņi var ievērot vairāku līmeņu pieeju, ja viņi izvēlas izmantot metožu kombināciju, lai nodrošinātu pārredzamību. Lai izvairītos no informācijas pārslodzes un vienlaikus nodrošinātu tās efektivitāti, īpaši būtu ieteicams izmantot vairāku līmeņu paziņojumus par privātumu, tādējādi izveidojot saikni ar dažādu kategoriju informāciju, kas jāsniedz datu subjektam, nevis parādīt šādu informāciju ekrānā vienā paziņojumā.

79. Iepriekš minētajās pamatnostādnēs arī paskaidrots, ka pārziņi var izvēlēties izmantot papildu rīkus, lai sniegtu informāciju atsevišķam datu subjektam, piemēram, privātuma informācijas paneļus. Privātuma informācijas panelis ir vienots punkts, kurā datu subjekti var skatīt "informāciju par privātumu" un pārvaldīt savas privātuma vēlmes, atļaujot vai aizliedzot pārziņiem attiecīgajā pakalpojumā izmantot savus datus konkrētajā veidā[39]. Privātuma informācijas panelis varētu sniegt pārskatu par *TPP*, kuri ir saņēmuši datu subjektu nepārprotamu piekrišanu, kā arī varētu piedāvāt būtisku informāciju par to persondatu veidu un apjomu, kuriem *TPP* piekļuvuši. Būtībā *ASPSP* ar pārskata starpniecību var piedāvāt lietotājam iespēju atsaukt konkrētu *PSD2* paredzētu nepārprotamu piekrišanu[40], kā rezultātā tiktu liegta piekļuve lietotāja maksājumu kontiem vienam vai vairākiem *TPP*. Lietotājs varētu arī lūgt *ASPSP* atteikt piekļuvi lietotāja maksājumu kontam(-iem) vienam vai vairākiem konkrētiem *TPP*[41], jo lietotājam ir tiesības gan izmantot, gan neizmantot konta informācijas pakalpojumu. Ja privātuma informācijas paneļi tiek izmantoti, lai sniegtu vai atsauktu nepārprotamu piekrišanu, tie būtu jāizstrādā un jāpiemēro likumīgā veidā, jo īpaši jānovērš šķēršļu radīšana *TPP* tiesībām sniegt pakalpojumus saskaņā ar *PSD2*. Šajā saistībā un saskaņā ar piemērojamiem *PSD2* noteikumiem *TPP* ir iespēja pēc piekrišanas atsaukšanas vēlreiz saņemt atkārtotu lietotāja piekrišanu.

80. Pārskatatbildības principi nosaka, ka pārzinim jāievieš atbilstoši tehniskie un organizatoriskie pasākumi, lai nodrošinātu un spētu pierādīt, ka apstrāde tiek veikta saskaņā ar VDAR, jo īpaši galvenajiem datu aizsardzības principiem, kas paredzēti 5. panta 1. punktā. Šajos pasākumos būtu jāņem vērā apstrādes veids, joma, konteksts un nolūki, kā arī risks fizisko personu tiesībām un brīvībām, un pasākumi vajadzības gadījumā jāpārskata un jāatjaunina[42].

---

[38] VDAR 14. panta 3. punkta b) apakšpunkts.

[39] Atbilstīgi 29. panta darba grupas Pārredzamības pamatnostādnēm saskaņā ar Regulu 2016/679, kuras apstiprinājusi EDAK, privātuma informācijas paneļi ir īpaši noderīgi, ja vienu un to pašu pakalpojumu datu subjekti izmanto dažādās ierīcēs, jo tas nodrošina viņiem piekļuvi saviem persondatiem un to kontroli neatkarīgi no tā, kā viņi izmanto šo pakalpojumu. Ļaujot datu subjektiem manuāli pielāgot savus privātuma iestatījumus, izmantojot privātuma informācijas paneli, var arī atvieglot paziņojuma par persondatu aizsardzību personalizēšanu, atspoguļojot tikai tos apstrādes veidus, kas skar konkrēto datu subjektu.

[40] Skatīt, piemēram, "nepārprotamo piekrišanu", kas minēta *PSD2* 67. panta 2. punkta a) apakšpunktā.

[41] Skatīt arī dokumenta EBA/OP/2020/10 45. punktu.

[42] VDAR 5. panta 2. punkts un 24. pants.

6.5 Profilēšana

81. Maksājumu pakalpojumu sniedzēju veiktā persondatu apstrāde var ietvert "profilēšanu", kā paredz VDAR 4. panta 4. punkts. Piemēram, *AISP* varētu paļauties uz automatizētu persondatu apstrādi, lai novērtētu noteiktus personiskos aspektus saistībā ar fizisku personu. Datu subjekta personisko finansiālo stāvokli varētu novērtēt atkarībā no pakalpojuma specifikas. Konta informācijas pakalpojumi, kas sniedzami pēc lietotāju pieprasījuma, var ietvert plašu personīgo maksājumu kontu datu novērtēšanu.

82. Pārzinim arī jānodrošina, ka automatizētu lēmumu pieņemšana, tostarp profilēšana, notiek datu subjektiem pārredzamā veidā. Šādos gadījumos pārzinim jāsniedz nozīmīga informācija par pamatā esošo loģiku, kā arī šādas apstrādes nozīmi un paredzamajām sekām datu subjektam (13. panta 2. punkta f) apakšpunkts, 14. panta 2. punkta g) apakšpunkts un 60. apsvērums)[43]. Tāpat saskaņā ar VDAR 15. pantu datu subjektam ir tiesības pieprasīt un iegūt informāciju no pārziņa par to, ka pastāv automatizēta lēmumu pieņemšana, tostarp profilēšana, par tajā ietverto loģiku un sekām attiecībā uz datu subjektu, kā arī — noteiktos apstākļos — par tiesībām iebilst pret profilēšanu neatkarīgi no tā, vai tiek īstenota automatizēta individuālu lēmumu pieņemšana, pamatojoties uz profilēšanu[44].

83. Turklāt šajā kontekstā būtiskas ir datu subjekta tiesības nebūt tāda lēmuma subjektam, kura pamatā ir tikai automatizēta apstrāde, tostarp profilēšana, kas attiecībā uz datu subjektu rada tiesiskās sekas vai kas līdzīgā veidā ievērojami ietekmē datu subjektu, kā paredz VDAR 22. pants. Noteiktos apstākļos šī norma ietver arī nepieciešamību datu pārziņiem īstenot piemērotus pasākumus, lai aizsargātu datu subjekta tiesības, piemēram, attiecībā uz konkrētas informācijas sniegšanu datu subjektam, tiesības pieprasīt cilvēka līdzdalību lēmumu pieņemšanā un izteikt savu viedokli un apstrīdēt lēmumu. Kā arī norādīts VDAR 71. apsvērumā, tas cita starpā nozīmē, ka datu subjektam ir tiesības nebūt tāda lēmuma subjektam, kas pieņemts bez cilvēka līdzdalības, piemēram, tiešsaistē iesniegta kredītpieteikuma automātiskam noraidījumam[45].

84. Automatizēta lēmumu pieņemšana, tostarp profilēšana, kas ietver īpašas persondatu kategorijas, ir atļauta tikai saskaņā ar VDAR 22. panta 4. punkta kumulatīvajiem nosacījumiem:

- ir piemērojams 22. panta 2. punktā paredzētais atbrīvojums
- un tiek piemērots VDAR 9. panta 2. punkta a) vai g) apakšpunkts. Abos gadījumos pārzinis ievieš piemērotus pasākumus, lai aizsargātu datu subjekta tiesības un brīvības, kā arī leģitīmās intereses[46].

85. Būtu jāievēro arī turpmākās apstrādes prasības, kā noteikts šajās pamatnostādnēs. Maksājumu pakalpojumu kontekstā ļoti aktuāli ir skaidrojumi un norādījumi par automatizētu individuālu lēmumu pieņemšanu un profilēšanu, kas sniegti EDAK apstiprinātajās 29. panta darba grupas

[43] Pārredzamības pamatnostādnes saskaņā ar Regulu 2016/679, WP260rev.01 — apstiprinājusi EDAK.
[44] 29. panta darba grupas Pamatnostādnes par automatizētu individuālu lēmumu pieņemšanu un profilēšanu Regulas 2016/679 nolūkiem, WP251rev.01.
[45] VDAR 71. apsvērums.
[46] 29. panta darba grupas Pamatnostādnes par automatizētu individuālu lēmumu pieņemšanu un profilēšanu Regulas 2016/679 nolūkiem, WP251rev.01, 24. lpp.

Pamatnostādnēs par automatizētu individuālu lēmumu pieņemšanu un profilēšanu Regulas 2016/679 nolūkiem, tāpēc tie būtu pienācīgi jāņem vērā.

Eiropas Datu aizsardzības kolēģijas vārdā

priekšsēdētāja

(Andrea Jelinek)