



**29. panta darba grupas
Pamatnostādnes par piekrišanu saskaņā ar Regulu 2016/679**

Pieņemtas 2017. gada 28. novembrī

Pēdējoreiz pārskatītas un pieņemtas 2018. gada 10. aprīlī

DARBA GRUPA PERSONU AIZSARDZĪBAI ATTIECĪBĀ UZ

PERSONAS DATU APSTRĀDI,

kas izveidota ar Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvu 95/46/EK,

ņemot vērā tās 29. un 30. pantu,

ņemot vērā darba grupas reglamentu,

IR PIEŅĒMUSI ŠĪS PAMATNOSTĀDNES.

Šī darba grupa tika izveidota saskaņā ar Direktīvas 95/46/EK 29. pantu. Tā ir neatkarīga Eiropas padomdevēja institūcija datu aizsardzības un privātuma jautājumos. Tās uzdevumi ir aprakstīti Direktīvas 95/46/EK 30. pantā un Direktīvas 2002/58/EK 15. pantā.

Sekretariāta pakalpojumus nodrošina Eiropas Komisijas Tiesiskuma un patērētāju ģenerāldirektorāta C direktorāts (Pamattiesības un Savienības pilsonība), B-1049 Brisele, Beļģija, birojs Nr. MO-59 02/013.

Tīmekļa vietne: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

Satura rādītājs

1.	Ievads.....	3
2.	Piekrišana VDAR 4. panta 11. punktā	4
3.	Spēkā esošas piekrišanas elementi.....	5
3.1.	Brīva / brīvi sniegta	5
3.1.1.	Spēku nevienlīdzība	6
3.1.2.	Nosacījumi	7
3.1.3.	Detalizācija.....	9
3.1.4.	Kaitējums	10
3.2.	Konkrēta	11
3.3.	Apzināta	12
3.3.1.	Minimālās satura prasības, lai piekrišana būtu “apzināta”	12
3.3.2.	Kā sniegt informāciju	13
3.4.	Viennozīmīga norāde par vēlmēm	15
4.	Nepārprotama piekrišanas saņemšana	17
5.	Papildu nosacījumi spēkā esošas piekrišanas saņemšanai.....	19
5.1.	Piekrišanas parādīšana	20
5.2.	Piekrišanas atsaukšana	21
6.	Mijiedarbība starp piekrišanu un citiem VDAR 6. pantā noteiktajiem likumīgajiem pamatiem	22
7.	Konkrētas jomas VDAR, kuras rada bažas	23
7.1.	Bērni (8. pants)	23
7.1.1.	Informācijas sabiedrības pakalpojumi	24
7.1.2.	Tieša sniegšana bērnam	24
7.1.3.	Vecums	25
7.1.4.	Bērnu piekrišana un vecāku atbildība.....	25
7.2.	Zinātniskā pētniecība	27
7.3.	Datu subjekta tiesības	29
8.	Saskaņā ar Direktīvu 95/46/EK iegūta piekrišana.....	30

1. Ievads

Šajās pamatnostādnēs sniegta padziļināta piekrišanas jēdziena analīze Regulas 2016/679 jeb Vispārīgās datu aizsardzības regulas (turpmāk tekstā — VDAR) izpratnē. Līdz šim Datu aizsardzības direktīvā (turpmāk tekstā — Direktīva 95/46/EK) un E-privātuma direktīvā izmantotais piekrišanas jēdziens ir attīstījies. VDAR sīkāk paskaidrotas un precizētas prasības spēkā esošas piekrišanas saņemšanai un parādīšanai. Šajās pamatnostādnēs uzmanība ir pievērsta šīm izmaiņām, sniedzot praktiskus norādījumus atbilstības VDAR nodrošināšanai un balstoties uz Atzinumu 15/2011 par piekrišanu. Pārziņiem ir pienākums ieviest jauninājumus, lai rastu jaunus risinājumus, kas darbojas tiesību aktos noteikto parametru ietvaros, un labāk atbalsta personas datu aizsardzību un datu subjektu intereses.

Saskaņā ar VDAR 6. pantu piekrišana ir viens no sešiem personas datu apstrādes likumīgajiem pamatiem¹. Uzsākot darbības, kuras ietver personas datu apstrādi, pārzinis vienmēr jāapsver atbilstošu paredzētās apstrādes likumīgo pamatu.

Kopumā piekrišana var būt atbilstošs likumīgais pamats tikai tādā gadījumā, ja datu subjektam tiek piedāvāta kontrole un patiesa izvēle attiecībā uz piedāvāto nosacījumu pieņemšanu vai noraidīšanu vai iespēja noraidīt tos bez nelabvēlīgām sekām. 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 personas dati tiks vai netiks apstrādāti. Pretējā gadījumā datu subjektam nav faktiskas kontroles un piekrišana nav uzskatāma par derīgu apstrādes pamatu, tādējādi apstrādes darbības kļūst nelikumīgas².

Esošie 29. panta darba grupas (WP29) atzinumi par piekrišanu³ ir spēkā tiktāl, ciktāl tie atbilst jaunajam tiesiskajam regulējumam, jo VDAR kodificēti esošie WP29 norādījumi un vispārpieņemta labā prakse, un galvenie piekrišanas elementi saglabājas nemainīgi VDAR. Tādēļ šajā dokumentā WP29 drīzāk paplašina un pabeidz iepriekšējos atzinumus par konkrētiem tematiem, kuros ietverta atsauce uz piekrišanu Direktīvas 95/46/EK izpratnē, nevis tos aizstāj.

Kā noteikts Atzinumā 15/2011 par piekrišanas definīciju, aicinājumam personām piekrist datu apstrādes darbībai būtu jāpiemēro stingras prasības, jo tas attiecas uz datu subjektu pamattiesībām un pārzinis vēlas iesaistīties apstrādes darbībā, kas bez datu subjekta piekrišanas būtu nelikumīga⁴. Piekrišanas svarīgā loma uzsvēta arī Eiropas Savienības Pamattiesību hartas 7. un 8. pantā. Turklāt piekrišanas saņemšana neizslēdz un nekādā veidā nesamazina pārziņa pienākumus ievērot VDAR, jo īpaši tās 5. pantā, noteiktos apstrādes principus attiecībā uz godprātību, nepieciešamību un proporcionalitāti, kā arī attiecībā uz datu kvalitāti. Pat ja personas datu apstrādes pamatā ir datu

¹ VDAR 9. pantā ir sniegts saraksts ar iespējamie izņēmumiem no aizlieguma apstrādāt īpašu kategoriju datus. Viens no uzskaitījumiem ir datu subjekta nepārprotama piekrišana šo personas datu apstrādei.

² Skatīt arī Atzinumu 15/2011 par piekrišanas definīciju (WP 187), 6.-8. lpp., un/vai Atzinumu 06/2014 par datu pārziņa likumīgajām interesēm atbilstīgi Direktīvas 95/46/EK 7. pantam (WP 217), 9., 10., 13. un 14. lpp.

³ Jo īpaši Atzinums 15/2011 par piekrišanas definīciju (WP 187).

⁴ Atzinums 15/2011, lappuse par piekrišanas definīciju (WP 187), 8. lpp.

subjekta piekrišana, tā nevar kalpot par likumīgu pamatu tādu datu vākšanai, kas nav nepieciešami konkrētajam apstrādes nolūkam, un tādējādi būtu pašos pamatos negodīga⁵.

Tāpat DG29 ir informēta, ka tiek pārskatīta E-privātuma direktīva (2002/58/EK). Piekrišanas jēdziens E-privātuma regulas projektā joprojām ir saistīts ar VDAR ietverto piekrišanas jēdzienu⁶. Visticamāk, organizācijām vajadzēs saņemt piekrišanu E-privātuma instrumenta ietvaros lielākajai daļai tiešsaistes tirgvedības ziņojumiem vai zvaniem, kā arī tiešsaistes izsekošanas metodēm, tostarp sīkdatņu izmantošanai lietotnēs un citā programmatūrā. Attiecībā uz priekšlikumu E-privātuma regulai WP29 jau ir sniegusi ieteikumus un norādījumus Eiropas likumdevējam⁷.

Attiecībā uz pašreizējo E-privātuma direktīvu WP29 norāda, ka atsauces uz atcelto Direktīvu 95/46/EK interpretējamas kā atsauces uz VDAR⁸. Tas attiecas arī uz atsaucēm uz piekrišanu spēkā esošajā Direktīvā 2002/58/EK, jo E-privātuma regula (vēl) nebūs spēkā 2018. gada 25. maijā. Saskaņā ar VDAR 95. pantu attiecībā uz apstrādi saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu publiskos komunikāciju tīklos netiek uzlikti papildu pienākumi, ciktāl E-privātuma direktīva uzliek konkrētus pienākumus ar šādu pašu mērķi. WP29 norāda, ka piekrišanai piemērojamās prasības VDAR ietvaros netiek uzskatītas par “papildu pienākumu”, bet drīzāk par likumīgas apstrādes priekšnosacījumu. Tādēļ VDAR noteiktie spēkā esošas piekrišanas saņemšanas nosacījumi piemērojami situācijām, kuras ietilpst E-privātuma direktīvas darbības jomā.

2. Piekrišana VDAR 4. panta 11. punktā

Piekrišana VDAR 4. panta 11. punktā definēta šādi: *“jebkura brīvi sniegta, konkrēta, apzināta un viennozīmīga norāde uz datu subjekta vēlmēm, ar kuru viņš paziņojuma vai skaidri apstiprinošas darbības veidā sniedz piekrišanu savu personas datu apstrādei.”*

Piekrišanas pamata izpratne joprojām ir līdzīga Direktīvā 95/46/EK ietvertajai, un piekrišana ir viens no likumīgiem pamatiem, uz kā balstāma personas datu apstrāde atbilstīgi VDAR 6. pantam⁹. Papildus grozītajai definīcijai 4. panta 11. punktā VDAR 7. pantā un 32., 33., 42. un 43. apsvērumā sniegti papildu norādījumi par to, kā pārzinim jārikojas, lai nodrošinātu atbilstību galvenajiem piekrišanas prasību elementiem.

⁵ Skatīt arī Atzinumu 15/2011 par piekrišanas definīciju (WP 187) un VDAR 5. pantu.

⁶ Saskaņā ar E-privātuma regulas priekšlikuma 9. pantu piemēro VDAR 4. panta 11. punktā un 7. pantā sniegto piekrišanas definīciju un nosacījumus.

⁷ Skatīt Atzinumu 03/2016 par E-privātuma direktīvas novērtējumu un pārskatīšanu (WP 240).

⁸ Skatīt VDAR 94. pantu.

⁹ Direktīvā 95/46/EK piekrišana definēta kā *“jebkurš labprātīgi sniegts šīs personas vēlmju konkrēts un paziņots norādījums, ar kuru datu subjekts izsaka savu piekrišanu uz viņu attiecināmu personas datu apstrādei”*, un kuram jābūt *“nepārprotami” sniegtam*, lai personas datu apstrāde būtu likumīga (Direktīvas 95/46/EK 7. panta a) apakšpunkts). Skatīt piemērus piekrišanas kā likumīga pamata piemērotībai WP29 Atzinumā 15/2011 par piekrišanas definīciju (WP 187). Šajā atzinumā WP29 ir sniegusi norādījumus, kā atšķirt gadījumus, kad piekrišana ir atbilstošs likumīgais pamats, no gadījumiem, kad pietiek ar likumīgām interesēm kā juridisku pamatu (iespējams, piedāvājot iespēju atteikties) vai būtu ieteicamas līgumiskas attiecības. Skatīt arī WP29 Atzinumu 06/2014, III.1.2. punkts, 14. lpp. un turpmāk. Nepārprotama piekrišana ir arī viens no izņēmumiem aizliegumam apstrādāt īpašu kategoriju datus: skatīt VDAR 9. pantu.

Visbeidzot, tas, ka tiek ietvertas konkrētas normas un apsvērumi par piekrišanas atsaukšanu, apstiprina, ka piekrišanai vajadzētu būt atsaucamam lēmumam un ka saglabājas zināms kontroles līmenis no datu subjekta puses.

3. Spēkā esošas piekrišanas elementi

VDAR 4. panta 11. punktā noteikts, ka datu subjekta piekrišana ir jebkura:

- brīvi sniegta,
- konkrēta,
- apzināta un
- viennozīmīga norāde uz datu subjekta vēlmēm, ar kuru viņš paziņojuma vai skaidri apstiprinošas darbības veidā sniedz piekrišanu savu personas datu apstrādei.

Turpmākajā iedaļās analizēts, ciktāl 4. panta 11. punkta formulējums uzliek pārziņiem pienākumu veikt izmaiņas to piekrišanas pieprasījumos/veidlapās, lai nodrošinātu atbilstību VDAR¹⁰.

3.1. Brīva / brīvi sniegta¹¹

Elements “brīvi sniegta” norāda uz reālu izvēles iespēju un datu subjektu kontroli. Kopumā VDAR paredz, ka gadījumos, kad datu subjektam nav reālas izvēles, kad viņš jūt, ka piekrišana ir piespiedu vai tās nesniegšanas rezultātā iestāsies nelabvēlīgas sekas, piekrišana nebūs spēkā esoša¹². Ja piekrišana ir iekļauta kā neapspriežama nosacījumu daļa, tā nav uzskatāma par brīvi sniegtu. Attiecīgi piekrišana netiks uzskatīta par brīvi sniegtu, ja datu subjektam nespēj atteikties vai atsaukt savu piekrišanu bez nelabvēlīgām sekām¹³. VDAR ir ņemts vērā arī līdzsvara trūkums starp pārziņi un datu subjektu.

Izvērtējot, vai piekrišana ir brīvi sniegta, būtu arī jāņem vērā konkrētā situācija, kādā piekrišana piesaistīta līgumiem vai pakalpojumu sniegšanai, kā aprakstīts 7. panta 4. punktā. 7. panta 4. punkta formulējums ir neizsmeļošs, izmantojot vārdus “cita starpā”, kas nozīmē, ka šī norma var attiekties uz virkni citu situāciju. Vispārīgi runājot, piekrišana kļūst spēkā neesoša jebkāda nepiemērota spiediena vai ietekmes uz datu subjektu elementa (kas var izpausties dažādi) rezultātā, liedzot datu subjektam īstenot tā brīvu gribu.

¹⁰ Norādījumiem attiecībā uz pašreiz veiktajām apstrādes darbībām, pamatojoties uz piekrišanu Direktīvā 95/46, skatīt šī dokumenta 7. nodaļu un VDAR 171. apsvērumu.

¹¹ 29. panta darba grupa vairākos atzinumos ir apskatījusi piekrišanas robežas situācijās, kad tās brīva sniegšana nav iespējama. Tas jo īpaši attiecās uz Atzinumu 15/2011 par piekrišanas definīciju (WP 187), Darba dokumentu par personas veselības datu apstrādi elektroniskās veselības kartēs (WP 131), Atzinumu 8/2001 par personas datu apstrādi saistībā ar nodarbinātību (WP48) un Otro atzinumu 4/2009 par Pasaules Antidopinga aģentūras (WADA) veikto datu apstrādi, Starptautisko privātuma un personas datu aizsardzības standartu, saistītajiem WADA kodeksa noteikumiem un citiem privātuma jautājumiem saistībā ar WADA un (valstu) antidopinga organizāciju cīņu pret dopingu sportā (WP 162).

¹² Skatīt Atzinumu 15/2011 par piekrišanas definīciju (WP 187), 12. lpp.

¹³ Skatīt VDAR 42. un 43. apsvērumu un 2011. gada 13. jūlijā pieņemto WP29 Atzinumu 15/2011 par piekrišanas definīciju (WP 187), 12. lpp.

[1. piemērs]

Mobilā lietotne fotoattēlu rediģēšanai prasa tās lietotājiem, lai tie varētu izmantot pakalpojumu, aktivizēt viņu GPS atrašanās vietu. Lietotne arī informē savus lietotājus, ka ievāks datus uzvedībā balstītas reklāmas nolūkos. Ne ģeolokalizācija, ne tiešsaistes uzvedībā balstīta reklāma nav nepieciešamas fotoattēlu rediģēšanas pakalpojuma sniegšanai un pārsniedz pamatpakalpojumu sniegšanai nepieciešamo. Tā kā lietotāji nevar izmantot lietotni, nesniedzot savu piekrišanu šiem nolūkiem, piekrišana nevar tikt uzskatīta par brīvi sniegtu.

3.1.1. Spēku nevienlīdzība

43. apsvērumā¹⁴ ir skaidri norādīts, ka ir maz ticams, ka **publiskas iestādes** var atsaukties uz piekrišanu apstrādei, jo ikreiz, kad pārzinis ir publiska iestāde, attiecībās starp datu pārzini un datu subjektu bieži vien pastāv spēku nevienlīdzība. Tāpat ir skaidrs, ka datu subjektam nebūs reālu alternatīvu šāda pārziņa apstrādes (nosacījumu) pieņemšanai. WP29 uzskata, ka pastāv citi, principā publisko iestāžu darbībai atbilstoši likumīgi pamati¹⁵.

Neskarot šos vispārīgos apsvērumus, VDAR tiesiskajā regulējumā nav pilnībā izslēgta piekrišanas izmantošana par publisko iestāžu veiktas datu apstrādes likumīgo pamatu. Turpmākajos piemēros redzams, ka piekrišanas izmantošana noteiktos apstākļos var būt atbilstoša.

[2. piemērs] Vietējā pašvaldība plāno veikt ceļu uzturēšanas darbus. Tā kā ceļu darbi var ilgstoši traucēt satiksmi, pašvaldība piedāvā saviem iedzīvotājiem iespēju parakstīties uz e-pasta abonentu sarakstu, lai saņemtu atjaunotu informāciju par darbu norisi un sagaidāmajiem kavējumiem. Pašvaldība skaidri norāda, ka dalība nav obligāta un lūdz piekrišanu izmantot e-pasta adreses (tikai) šim nolūkam. Iedzīvotāji, kuri tam nepiekrīt, nezaudēs iespēju izmantot kādu no pašvaldības pamatpakalpojumiem vai īstenot jebkādas savas tiesības, tāpēc viņi var brīvi izvēlēties sniegt vai nesniegt savu piekrišanu šādai datu izmantošanai. Visa informācija par ceļa darbiem būs pieejama arī pašvaldības tīmekļa vietnē.

[3. piemērs] Personai, kam pieder zeme, ir nepieciešamas noteiktas atļaujas gan no vietējās pašvaldības, gan no provinces valdības, kurā atrodas pašvaldība. Abām publiskajām struktūrām ir vajadzīga vienāda informācija atļaujas izsniegšanai, bet tām nav savstarpējas piekļuves otras struktūras datu bāzei. Tādēļ abas struktūras pieprasa vienādu informāciju, un zemes īpašniece nosūta savu informāciju abām publiskajām struktūrām. Pašvaldība un provinces valdība lūdz viņas piekrišanu apvienot lietas, lai izvairītos no dubultas procedūras un sarakstes. Abas publiskās struktūras apliecina, ka šī apvienošana ir izvēles un ka atļauju pieprasījumi joprojām tiks izskatīti atsevišķi, ja viņa nepiekrīt datu apvienošanai. Zemes īpašniece tādējādi var brīvi sniegt piekrišanu iestādēm lietu apvienošanas nolūkā.

[4. piemērs] Valsts skola lūdz skolēnus sniegt savu piekrišanu viņu fotoattēlu izmantošanai drukātā skolēnu žurnālā. Šādā situācijā pastāv patiesa izvēle attiecībā uz piekrišanu, kamēr skolēniem netiks liegta izglītība vai pakalpojumi un viņi varēs atteikties ļaut izmantot šīs fotogrāfijas bez nelabvēlīgām sekām.¹⁶

Spēku nevienlīdzība parādās arī **nodarbinātības** kontekstā¹⁷. Ņemot vērā atkarību, kas izriet no darba devēja / darba ņēmēja attiecībām, ir maz ticams, ka datu subjekts var atteikties sniegt savam

¹⁴ VDAR 43. apsvērumā noteikts: "Lai nodrošinātu, ka piekrišana ir sniegta brīvi, piekrišanai nevajadzētu kalpot par derīgu juridisko pamatu personas datu apstrādei konkrētā gadījumā, kad datu subjekta un pārziņa attiecībās pastāv skaidra nevienlīdzība, jo īpaši, ja pārzinis ir publiska iestāde un tāpēc ir maz ticams, ka piekrišana visos minētās konkrētās situācijas apstākļos bija sniegta brīvi. (..)"

¹⁵ Skatīt VDAR 6. pantu, jo īpaši 1. punkta c) un e) apakšpunktu.

¹⁶ Šajā piemērā valsts skola ir valsts finansēta skola vai jebkura izglītības iestāde, kas valsts tiesību aktos ir kvalificēta kā publiska iestāde vai struktūra.

darba devējam piekrišanu datu apstrādei bez bailēm vai nepastāvot reāliem nelabvēlīgu seku draudiem atteikuma gadījumā. Maz ticams, ka darbinieks varētu brīvi atbildēt uz darba devēja pieprasījumu sniegt piekrišanu, piemēram, lai aktivizētu tādas uzraudzības sistēmas kā videonovērošanu darbavietā vai aizpildītu vērtēšanas veidlapas, neizjūtot spiedienu piekrist¹⁸. Tādēļ WP29 uzskata, ka darba devējiem ir problemātiski apstrādāt esošo un nākotnes darbinieku personas datus uz piekrišanas pamata, jo maz ticams, ka šāda piekrišana varētu būt brīvi sniegta. Attiecībā uz lielāko daļu šādas datu apstrādes darbā darbinieku piekrišana nevar un nedrīkstētu būt likumīgais pamats (6. panta 1. punkta a) apakšpunkts) darba devēja un darba ņēmēja attiecību rakstura dēļ¹⁹.

Tomēr tas nenozīmē, ka darba devēji nekad nevar atsaukties uz piekrišanu kā apstrādes likumīgo pamatu. Var būt situācijas, kurās darba devējs var faktiski parādīt, ka piekrišana ir brīvi sniegta. Ņemot vērā spēku nevienlīdzību darba devēja un viņa personāla attiecībās, darbinieki var brīvi sniegt piekrišanu tikai izņēmuma gadījumos, kad neiestāsies negatīvas sekas, neatkarīgi no tā, vai viņi sniedz savu piekrišanu²⁰.

[5. piemērs]

Filmēšanas grupa filmēs noteiktā biroja daļā. Darba devējs lūdz darbiniekus, kuru darba vieta ir šajā zonā, sniegt piekrišanu filmēšanai, jo viņi var būt redzami videomateriāla fonā. Darbinieki, kuri nevēlas tikt filmēti, netiks nekādā veidā sodīti, un uz filmēšanas laiku viņiem tiek ierādīta līdzvērtīga darba vieta citā ēkas daļā.

Spēku nevienlīdzība neattiecas tikai uz publiskām iestādēm un darba devējiem, tā var parādīties arī citās situācijās. Kā WP29 ir norādījusi vairākos savos atzinumos, piekrišana var būt spēkā esoša tikai tad, ja datu subjektam ir patiesa izvēle, nepastāv maldināšana, iebiedēšana, piespiešana vai nozīmīgas nelabvēlīgas sekas (piemēram, būtiskas papildu izmaksas), ja viņš nesniedz piekrišanu. Piekrišana nebūs brīvi sniegta gadījumos, kad ir piespiešanas, spiediena vai nespējas īstenot brīvu gribu elements.

3.1.2. Nosacījumi

VDAR 7. panta 4. punktam ir svarīga nozīme, izvērtējot, vai piekrišana ir brīvi sniegta²¹.

VDAR 7. panta 4. punktā norādīts, ka, cita starpā, par ļoti nevēlamu tiek uzskatīta piekrišanas “saistīšana” ar nosacījumu pieņemšanu vai līguma vai pakalpojuma sniegšanas “piesaistīšana” pieprasījumam piekrišanai personas datu apstrādei, kas nav nepieciešama šā līguma vai pakalpojuma izpildei. Ja šādā situācijā tiek sniegta piekrišana, tiek uzskatīts, ka tā nav brīvi sniegta

¹⁷ Skatīt arī VDAR 88. pantu, kurā uzsvērta darbinieku konkrētu interešu aizstāvības nepieciešamība un tiek izveidota iespēja atkāpties no dalībvalsts tiesību aktiem. Skatīt arī 155. apsvērumu.

¹⁸ Skatīt Atzinuma 15/2011 par piekrišanas definīciju (WP 187) 12.-14. lpp., Atzinuma 8/2001 par personas datu apstrādi nodarbinātības jomā (WP 48) 10. nodaļu, Darba dokumenta par elektroniskās komunikācijas novērošanu darba vietā (WP 55) 4.2. punktu un Atzinuma 2/2017 par datu apstrādi darba vietā (WP 249) 6.2. punktu.

¹⁹ Skatīt Atzinumu 2/2017 par datu apstrādi darba vietā, 6.-7. lpp.

²⁰ Skatīt Atzinuma 2/2017 par datu apstrādi darba vietā (WP 249) 6.2. punktu.

²¹ VDAR 7. panta 4. punkts: “*Novērtējot to, vai piekrišana ir dota brīvi, maksimāli ņem vērā to, vai cita starpā līguma izpilde, tostarp pakalpojuma sniegšana, ir atkarīga no piekrišanas tādai personas datu apstrādei, kura nav nepieciešama minētā līguma izpildei.*” Skatīt arī VDAR 43. apsvērumu, kurā noteikts: “*(..) Uzskata, ka piekrišana nav sniegta brīvi, ja tā neparedz atsevišķu piekrišanu dažādām personas datu apstrādes darbībām, neraugoties uz to, ka tas ir atbilstīgi konkrētajam gadījumam, vai ja tiek noteikts, ka no šīs piekrišanas ir atkarīga līguma izpilde, tostarp pakalpojuma sniegšana, neraugoties uz to, ka minētā piekrišana nav noteikti nepieciešama šādai izpildei.*”

(43. apsvērumš). Ar 7. panta 4. punktu tiek mēģināts nodrošināt, ka personas datu apstrādes nolūks nav slēpts vai apvienots ar tāda pakalpojuma līguma nodrošināšanu, kuram šie personas dati nav nepieciešami. To darot, VDAR nodrošina, ka personas datu apstrāde, kurai tiek lūgta piekrišana, nevar tieši vai netieši kļūt par līguma pretlikumīgu izpildi. Divi likumīgie pamati personas datu likumīgai apstrādei, t. i., piekrišana un līgums, nevar tikt apvienoti un padarīti neskaidri.

Pienākums piekrist personas datu izmantošanai papildus noteikti nepieciešamajam ierobežo datu subjekta izvēli un kavē brīvi sniegt piekrišanu. Tā kā datu aizsardzības tiesību akti ir vērsti uz pamattiesību aizsardzību, ir svarīgi nodrošināt privātpersonas kontroli pār tās personas datiem, un pastāv spēcīgs pieņēmums, ka piekrišana personas datu apstrādei, kas nav nepieciešama, nevar tikt uzskatīta par obligātu apsvērumu apmaiņā pret līgumsaistību izpildi vai pakalpojuma sniegšanu.

Tādējādi, ja piekrišanas pieprasījums ir saistīts ar datu pārziņa līgumsaistību izpildi, datu subjekts, kurš nevēlas, lai personas dati pārzinim būtu pieejami apstrādei, riskē, ka viņam tiks atteikta pieprasīto pakalpojumu nodrošināšana.

Lai novērtētu, vai šādā situācijā rodas piesaiste vai sasaistīšana, ir svarīgi noteikt, kāda ir līguma darbības joma un kādi dati būs nepieciešami šā līguma izpildei.

Saskaņā ar WP29 Atzinumu 06/2014 termins “nepieciešams līguma izpildei” ir jāinterpretē šauri. Apstrādei ir jābūt nepieciešamai, lai izpildītu līgumu ar katru atsevišķu datu subjektu. Tas var ietvert, piemēram, datu subjekta adreses apstrādi, lai varētu piegādāt tiešsaistē iegādātās preces, vai kredītkaršu datu apstrādi, lai nodrošinātu maksājuma izpildi. Nodarbinātības kontekstā šis pamats var ļaut, piemēram, algu informācijas un bankas konta informācijas apstrādi, lai varētu izmaksāt algas²². Jābūt tiešai un objektīvai saiknei starp datu apstrādi un līgumsaistību izpildes mērķi.

Ja datu pārzinis vēlas apstrādāt personas datus, kas faktiski ir nepieciešami līguma izpildei, tad piekrišana nav atbilstošs likumīgais pamats²³.

Regulas 7. panta 4. punkts ir piemērojams tikai tad, ja pieprasītie dati **nav** nepieciešami līguma izpildei (tostarp pakalpojuma sniegšanai), un šo datu iegūšana uz piekrišanas pamata ir līgumsaistību izpildes nosacījums. Savukārt, ja apstrāde ir nepieciešama līguma izpildei (tostarp pakalpojuma sniegšanai), tad 7. panta 4. punktu nepiemēro.

[6. piemērs]

Banka lūdz klientiem piekrišanu ļaut trešām personām izmantot viņu maksājumu informāciju tiešās tirgvedības nolūkos. Šī apstrādes darbība nav nepieciešama, lai izpildītu līgumu ar klientu un nodrošinātu parastos bankas kontu pakalpojumus. Ja klienta atteikuma piekrist šim apstrādes nolūkam rezultātā tiks liegta bankas pakalpojumu sniegšana, slēgti bankas konti vai — atkarībā no gadījuma — pieaugs maksa, piekrišanu nevar brīvi sniegt.

²² Plašāku informāciju un piemērus skatīt Atzinumā 06/2014 par datu pārziņa likumīgo interešu jēdzienu saskaņā ar Direktīvas 95/46/EK 7. pantu, kuru WP29 pieņēma 2014. gada 9. aprīlī, 16.-17. lpp. (WP 217).

²³ Atbilstošs likumīgais pamats tad varētu būt 6. panta 1. punkta b) apakšpunkts (līgums).

Likumdevēja izvēle uzsvērt nosacījumus — cita starpā kā pieņemumu par brīvības sniegt piekrišanu neesību — parāda, ka nosacījumu iestāšanās ir rūpīgi jāpārbauda. Formulējums “maksimāli ņem vērā” 7. panta 4. punktā paredz, ka datu pārzinim īpaši jāuzmanās, ja līgumā (kas var ietvert pakalpojuma sniegšanu) ir iekļauts tam piesaistīts pieprasījums piekrist apstrādāt personas datus.

Tā kā 7. panta 4. punkta formulējums nav absolūts, var pastāvēt ļoti ierobežots gadījumu skaits, kad šādu nosacījumu rezultātā piekrišana nebūtu uzskatāma par spēkā neesošu. Tomēr vārds “uzskata” 43. apsvērumā skaidri norāda, ka šādi gadījumi būs ārkārtīgi reti.

Jebkurā gadījumā saskaņā ar 7. panta 4. punktu pierādīšanas pienākums ir pārzinim²⁴. Šis konkrētais noteikums atspoguļo visā VDAR klātesošo vispārīgo pārskatatbildības principu. Tomēr gadījumos, kad piemēro 7. panta 4. punktu, pārzinim būs grūtāk pierādīt, ka datu subjekts savu piekrišanu ir sniedzis brīvi²⁵.

Pārzinis varētu apgalvot, ka tā organizācija nodrošina datu subjektiem patiesu izvēli, ja viņi varētu izvēlēties starp pakalpojumu, kas ietver piekrišanu personas datu izmantošanai papildu nolūkiem, no vienas puses, un līdzvērtīgu pakalpojumu, ko piedāvā tas pats personas datu pārzinis, kur nav nepieciešama piekrišana datu izmantošanai papildu nolūkiem, no otras puses. Kamēr pastāv iespēja, ka līgumsaistības tiek izpildītas, vai šī datu pārziņa sniegto līgumisko pakalpojumu var izpildīt bez piekrišanas citu vai papildu datu izmantošanai, tas vairs nav uzskatāms par pakalpojumu ar nosacījumiem. Tomēr abiem pakalpojumiem jābūt patiesi līdzvērtīgiem.

WP29 uzskata, ka piekrišanu nevar uzskatīt par brīvi sniegtu, ja pārzinis apgalvo, ka ir nodrošināta izvēle starp tā sniegtiem pakalpojumiem, kas ietver piekrišanu personas datu izmantošanai papildu nolūkiem, no vienas puses, un līdzvērtīgu pakalpojumu, ko piedāvā cits pārzinis, no otras puses. Šādā gadījumā izvēles brīvība būtu atkarīga no tā, ko dara citi tirgus dalībnieki, un vai atsevišķs datu subjekts uzskatītu, ka cita pārziņa sniegtie pakalpojumi patiešām ir līdzvērtīgi. Turklāt tas nozīmē, ka pārziņiem ir pienākums uzraudzīt tirgus attīstību, lai nodrošinātu piekrišanas to datu apstrādes darbībām nepārtrauktu spēkā esību, jo konkurents savus pakalpojumus var vēlāk mainīt. Tādējādi šī argumenta izmantošana nozīmē, ka piekrišana neatbilst VDAR prasībām.

3.1.3. Detalizācija

Pakalpojums var ietvert vairākas apstrādes darbības vairāk nekā vienam nolūkam. Šādos gadījumos datu subjektiem vajadzētu būt brīvai izvēlei, kuru nolūku viņi pieņem, nevis jāsniedz piekrišana apstrādes darbību kopumam. Konkrētajā gadījumā, pamatojoties uz VDAR, var būt nepieciešamas vairākas piekrišanas pakalpojuma sniegšanas uzsākšanai.

²⁴ Skatīt arī VDAR 7. panta 1. punktu, kurā noteikts, ka datu pārzinim ir jāpierāda, ka datu subjekta piekrišana ir brīvi sniegta.

²⁵ Daļēji šī punkta ieviešana ir spēkā esošo WP29 norādījumu kodifikācija. Kā aprakstīts Atzinumā 15/2011, ja datu subjekts ir atkarīgs no datu pārziņa attiecību rakstura vai īpašu apstākļu dēļ, var pastāvēt spēcīgs pieņemums, ka šādā kontekstā piekrišanas sniegšanas brīvība ir ierobežota (piemēram, darba attiecībās vai ja datu vākšanu veic publiska iestāde). Tomēr esot spēkā 7. panta 4. punktam, pārzinim būs grūtāk pierādīt, ka datu subjekts savu piekrišanu ir sniedzis brīvi. Skatīt: Atzinumu 15/2011 par piekrišanas definīciju (WP 187), 12.-17. lpp.

43. apsvērumā ir paskaidrots, ka piekrišana tiek uzskatīta par brīvi sniegtu, ja piekrišanas saņemšanas process/procedūra neļauj datu subjektam sniegt atsevišķu piekrišanu dažādām personas datu apstrādes darbībām (piemēram, tikai dažām apstrādes darbībām un ne citām), neskatoties uz to, ka tas konkrētajā gadījumā ir atbilstoši. 32. apsvērumā noteikts: *“Piekrišanai būtu jāattiecas uz visām apstrādes darbībām, ko veic vienā un tajā pašā nolūkā vai nolūkos. Ja apstrādei ir vairāki nolūki, piekrišana būtu jādod visiem nolūkiem”*.

Ja pārzinis ir apvienojis vairākus apstrādes nolūkus un nav centies saņemt atsevišķu piekrišanu katram nolūkam, nav piekrišanas brīvības. Šī detalizācija ir cieši saistīta ar nepieciešamību, ka piekrišanai jābūt konkrētai, kā aprakstīts turpmāk 3.2. iedaļā. Ja datu apstrāde tiek veikta, lai sasniegtu vairākus nolūkus, risinājums, lai nodrošinātu spēkā esošas piekrišanas nosacījumu izpildi, ir detalizācija, t. i., šo nolūku nodalīšana un piekrišanas sniegšana katram atsevišķam nolūkam.

[7. piemērs]

Vienā piekrišanas pieprasījumā mazumtirgotājs lūdz klientiem piekrišanu izmantot to datus, lai nosūtītu tirgvedības paziņojumus pa e-pastu, kā arī dalītos informācijā par tiem ar citiem grupas uzņēmumiem. Šāda piekrišana nav detalizēta, jo šiem diviem nolūkiem netiek pieprasīta atsevišķa piekrišana, līdz ar to tā nebūs spēkā. Šajā gadījumā būtu jāsaņem konkrēta piekrišana kontaktinformācijas pārsūtīšanai komerciālajiem partneriem. Šāda konkrēta piekrišana tiks uzskatīta par spēkā esošu katram partnerim (skatīt arī 3.3.1. iedaļu), kura identitāte datu subjektam ir bijusi pieejama laikā, kad viņš sniedz piekrišanu, ja vien tā ir sniegta vienam un tam pašam nolūkam (šajā piemērā: tirgvedības nolūkam).

3.1.4. Kaitējums

Pārzinim ir jāparāda, ka piekrišanu var atteikt vai atsaukt bez nelabvēlīgām sekām (42. apsvēruma). Piemēram, pārzinim ir jāpierāda, ka piekrišanas atsaukšanas rezultātā datu subjektam neradīsies jebkādas papildu izmaksas, līdz ar to piekrišanas atsaukšanai nav nekādu acīmredzamu trūkumu.

Citi kaitējuma piemēri ir maldināšana, iebiedēšana, piespiešana vai nozīmīgas nelabvēlīgas sekas, kas iestājas, ja datu subjekts nepiekrīt. Pārzinim vajadzētu spēt pierādīt, ka datu subjektam bijusi brīva vai patiesa izvēle sniegt piekrišanu un piekrišanu bija iespējams atsaukt bez nelabvēlīgām sekām.

Ja pārzinis var parādīt, ka pakalpojumam var atsaukt piekrišanu bez negatīvām sekām, piemēram, nesamazinot pakalpojuma sniegšanas kvalitāti, kas nelabvēlīgi ietekmētu lietotāju, tas var kalpot par pierādījumu, ka piekrišana sniegta brīvi. VDAR neizslēdz visus stimulus, bet pārzinim ir pienākums parādīt, ka visos apstākļos piekrišana ir brīvi sniegta.

[8. piemērs]

Lejupielādējot dzīvesveida mobilo lietotni, lietotne lūdz piekrišanu piekļūt tālruņa akselerometram. Informācija nav nepieciešama lietotnes darbības nodrošināšanai, bet tā ir noderīga pārzinim, kurš vēlas uzzināt vairāk par savu lietotāju pārvietošanos un aktivitātes līmeņiem. Kad lietotāja vēlāk šo piekrišanu atsauca, viņa uzzināja, ka lietotne tagad darbosies tikai ierobežotā apjomā. Šis ir 42. apsvērumā minētais kaitējuma piemērs, kas nozīmē, ka piekrišana nav bijusi likumīgi saņemta (un tādēļ pārzinim ir jāizdzēš visi šādā veidā iegūtie personas dati par lietotāju pārvietošanos).

[9. piemērs]

Datu subjekts piekrīt saņemt modes mazumtirgotāja biļetenu ar vispārējām atlaidēm. Mazumtirgotājs lūdz datu subjektam sniegt piekrišanu, lai ievāktu vairāk datu par iepirkšanās izvēlēm, lai pielāgotu piedāvājumus viņa vēlmēm, pamatojoties uz iepirkšanās vēsturi vai aptaujas anketu, kuras aizpildīšana ir brīvprātīga. Kad datu subjekts vēlāk atsauc piekrišanu, viņš vai viņa turpinās saņemt personīgi nepielāgotas modes atlaides. Tas nav uzskatāms par kaitējumu, jo ticis zaudēts tikai pieļaujamais stimulants.

[10. piemērs]

Modes žurnāls piedāvā lasītājiem iespēju iegādāties jaunus kosmētikas līdzekļus pirms to oficiālās izlaišanas. Produkti drīzumā būs pieejami pārdošanai, taču šī žurnāla lasītājiem tiek piedāvāta ekskluzīva iespēja šos produktus iegādāties agrāk. Lai izmantotu šo iespēju, cilvēkiem jāsniedz sava pasta adrese un jāpiekrīt pierakstīties žurnāla adresātu sarakstam. Pasta adrese ir nepieciešama nosūtīšanai un adresātu saraksts tiek izmantots šādu produktu, piemēram, kosmētikas vai t-kreklu, komerciālo piedāvājumu izsūtīšanai visa gada garumā.

Uzņēmums paskaidro, ka dati adresātu sarakstā tiks izmantoti tikai žurnāla preču un papīra reklāmas nosūtīšanai un tie netiks nodoti nevienai citai organizācijai.

Ja lasītājs nevēlas izpaust savu adresi šim nolūkam, kaitējums nav nodarīts, jo produkti lasītājiem ir jebkurā gadījumā pieejami.

3.2. Konkrēta

Regulas 6. panta 1. punkta a) apakšpunktā ir apstiprināts, ka datu subjekta piekrišana jāsniedz saistībā ar “vienu vai vairākiem konkrētiem” nolūkiem un ka datu subjekts var izvēlēties attiecībā uz katru no tiem²⁶. Prasības piekrišanai būt “konkrētai” mērķis ir nodrošināt datu subjektam zināmu lietotāja kontroli un pārredzamību. VDAR šo prasību nav mainījusi un tā joprojām ir cieši saistīta ar “apzinātas” piekrišanas prasību. Tajā pašā laikā tā jāinterpretē atbilstīgi “detalizētības” prasībai “brīvas” piekrišanas iegūšanai²⁷. Kopumā, lai ievērotu “konkrētības” elementa prasību, pārzinim jāpiemēro:

- (i) nolūka specifiskāciju kā aizsardzības pasākumu pret funkciju nesamērīgu pieaugumu;
- (ii) detalizētus piekrišanas pieprasījumus un
- (iii) skaidru informācijas nodalīšanu attiecībā uz piekrišanas saņemšanu datu apstrādes darbībām no citas informācijas.

Papildinājums i) punktam: Saskaņā ar VDAR 5. panta 1. punkta b) apakšpunktu, lai saņemtu spēkā esošu piekrišanu, paredzētajai apstrādes darbībai vienmēr ir jānosaka konkrēts, skaidrs un leģitīms nolūks.²⁸ Nepieciešamība pēc konkrētas piekrišanas apvienojumā ar nolūka ierobežojuma jēdzienu 5. panta 1. punkta b) apakšpunktā darbojas kā aizsardzības pasākums pret nolūku, kuriem dati tiek apstrādāti, pakāpenisku paplašināšanu vai sapludināšanu pēc tam, kad datu subjekts ir piekritis sākotnējai datu vākšanai. Šī parādība, kas zināma arī kā funkciju nesamērīgs pieaugums, ir risks datu subjektiem, jo tas var izraisīt neplānotu personas datu izmantošanu no pārziņa vai trešo personu puses un datu subjektu kontroles zaudēšanu.

²⁶ Turpmākie norādījumi par “nolūku” noteikšanu ir atrodamā Atzinumā 3/2013 par nolūka ierobežojumu (WP 203).

²⁷ VDAR 43. apsvērumā noteikts, ka visos atbilstošos gadījumos dažādām apstrādes darbībām būs nepieciešama atsevišķa piekrišana. Lai datu subjektiem nodrošinātu iespēju sniegt piekrišanu katram atsevišķam nolūkam, būtu jānodrošina detalizētas piekrišanas iespējas.

²⁸ Skatīt WP29 Atzinumu 3/2013 par nolūku ierobežošanu (WP 203), 16. lpp.: “Šo iemeslu dēļ mērķis, kas ir neskaidrs vai vispārīgs, piemēram, “lietotāju pieredzes uzlabošana”, “tirgvedības nolūkos”, “IT drošības nolūkos” vai “turpmākiem pētījumiem” bez sīkāka paskaidrojuma parasti neatbilst “konkrētuma” kritērijam.”

Ja pārzinis atsaucas uz 6. panta 1. punkta a) apakšpunktu, datu subjektiem vienmēr ir jāsniedz piekrišana konkrētam apstrādes nolūkam²⁹. Atbilstīgi nolūku ierobežošanas jēdzienam, 5. panta 1. punkta b) apakšpunktam un 32. apsvērumam, piekrišana var attiekties uz dažādām darbībām, ja šīs darbības kalpo vienam nolūkam. Pats par sevi saprotams, ka konkrētu piekrišanu var iegūt tikai tad, ja datu subjekti ir konkrēti informēti par paredzētajiem nolūkiem datu izmantošanai, kas skar viņus.

Neatkarīgi no nolūku saderības normām, piekrišanai jāattiecas uz konkrētu nolūku. Datu subjekti sniegs savu piekrišanu, apzinoties, ka viņi saglabā kontroli un viņu datus apstrādās tikai minētajiem konkrētajiem nolūkiem. Ja pārzinis apstrādā datus uz piekrišanas pamata un vēlas apstrādāt datus arī citam nolūkam, minētajam pārzinim jālūdz atsevišķa piekrišana šim citam nolūkam, ja vien nepastāv cits, attiecīgajai situācijai atbilstošāks likumīgais pamats.

[11. piemērs] Kabeļtelevīzijas tīkls apkopo abonentu personas datus uz viņu piekrišanas pamata, lai sniegtu viņiem personīgus ieteikumus par jaunām filmām, kuras varētu abonētus interesēt, pamatojoties uz viņu skatīšanās paradumiem. Pēc laika televīzijas tīkls nolemj, ka vēlas ļaut trešām personām nosūtīt (vai atainot) mērķtiecīgu reklāmu, pamatojoties uz abonenta skatīšanās paradumiem. Ņemot vērā šo jauno mērķi, ir nepieciešama jauna piekrišana.

Papildinājums ii) punktam: Piekrišanas mehānismiem jābūt detalizētiem ne tikai, lai apmierinātu “brīvas” piekrišanas prasību, bet arī lai atbilstu “konkrētības” elementam. Tas nozīmē, ka pārzinim, kurš vēlas saņemt piekrišanu dažādiem nolūkiem, būtu jānodrošina atsevišķa izvēle katram nolūkam, lai lietotāji varētu sniegt konkrētu piekrišanu konkrētiem nolūkiem.

Papildinājums iii) punktam: Visbeidzot, pārziniem būtu jāsniedz konkrēta informācija katrā atsevišķā piekrišanas pieprasījumā par datiem, kas tiek apstrādāti katram nolūkam, lai datu subjekti būtu informēti par viņu dažādo izvēļu ietekmi. Tādējādi datu subjekti var sniegt konkrētu piekrišanu. Šis jautājums pārklājas ar prasību, ka pārziniem jāsniedz skaidra informācija, kā aprakstīts turpmāk 3.3. punktā.

3.3. Apzināta

VDAR ieviesta prasība piekrišanai būt apzinātai. Pamatojoties uz VDAR 5. pantu, pārredzamības prasība ir viens no pamatprincipiem, kas cieši saistīts ar godprātības un likumības principiem. Informācijas nodrošināšana datu subjektiem pirms piekrišanas saņemšanas ir būtiska, lai varētu pieņemt apzinātus lēmumus, saprast, kam viņi piekrīt, un, piemēram, izmantot tiesības atsaukt savu piekrišanu. Ja pārzinis nesniedz pieejamu informāciju, lietotāja kontrole kļūst iluzora un piekrišana kļūst par spēkā neesošu juridisko pamatu.

Apzinātas piekrišanas prasības neievērošanas sekas ir tādas, ka piekrišana būs spēkā neesoša un pārzinis, iespējams, būs pārkāpis VDAR 6. pantu.

3.3.1. Minimālās satura prasības, lai piekrišana būtu “apzināta”

²⁹ Tas atbilst WP29 Atzinumam 15/2011 par piekrišanas definīciju (WP 187), piemēram, 17. lpp.

Lai piekrišana būtu apzināta, datu subjekts jāinformē par noteiktiem elementiem, kas ir būtiski, izdarot izvēli. Tādēļ WP29 uzskata, ka spēkā esošas izvēles saņemšanai ir nepieciešama vismaz šāda informācija:

- (i) pārziņa identitāte;³⁰
- (ii) katras apstrādes darbības, kurai tiek lūgta piekrišana, nolūks;³¹
- (iii) kādi (kāda veida) dati tiks vākti un izmantoti;³²
- (iv) tiesības atsaukt piekrišanu;³³
- (v) attiecīgos gadījumos informācija par datu izmantošanu automatizētu lēmumu pieņemšanā saskaņā ar 22. panta 2. punkta c) apakšpunktu³⁴; un
- (vi) Informācija par iespējamiem datu pārsūtīšanas riskiem atbilstības lēmuma un atbilstošu aizsardzības pasākumu neesamības gadījumā, kā aprakstīts 46. pantā³⁵.

Attiecībā uz i) un iii) apakšpunktu WP29 norāda, ka gadījumos, kad pieprasīto piekrišanu izmanto vairāki (kopīgi) pārziņi vai arī ja datus pārsūta vai apstrādā citi pārziņi, kuri vēlas atsaukties uz sākotnējo piekrišanu, šīs organizācijas būtu jāuzskaita. Apstrādātājiem nav jābūt nosauktiem piekrišanas prasību ietvaros, tomēr, lai izpildītu VDAR 13. un 14. pantu, pārziņiem būs jāsniedz pilns saņēmēju vai saņēmēju kategoriju, tostarp apstrādātāju, saraksts. Noslēgumā WP29 norāda, ka atkarībā no lietas apstākļiem un konteksta var būt nepieciešama plašāka informācija, kas ļauj datu subjektam patiesi izprast apstrādes darbības.

3.3.2. Kā sniegt informāciju

VDAR nav noteikta forma vai veids, kādā informācija sniedzama, lai izpildītu apzinātas piekrišanas prasību. Tas nozīmē, ka spēkā esošu informāciju var uzrādīt dažādos veidos, piemēram, rakstiskos vai mutiskos paziņojumos vai audio vai video ziņojumos. Tomēr VDAR izvirzītas vairākas prasības attiecībā uz apzinātu piekrišanu, galvenokārt 7. panta 2. punktā un 32. apsvērumā. Tā rezultātā rodas augstāks informācijas skaidrības un pieejamības standarts.

Pieprasot piekrišanu, pārziņiem būtu jānodrošina, ka visos gadījumos tiek izmantota skaidra un vienkārša valoda. Tas nozīmē, ka ziņojumam vajadzētu būt viegli saprotamam vidusmēra cilvēkam, ne tikai juristiem. Pārziņi nevar izmantot garas konfidencialitātes politikas, kuras ir grūti saprotamas, vai paziņojumus, kas satur juridisku žargonu. Piekrišanai jābūt skaidrai un nošķiramai no citiem jautājumiem, un tā jāsniedz saprotamā un viegli pieejamā veidā. Šī prasība būtībā nozīmē, ka informācija, kas ir būtiska, lai pieņemtu apzinātu lēmumu sniegt vai nesniegt piekrišanu, nedrīkst būt apslēpta vispārīgos nosacījumos³⁶.

³⁰ Skatīt arī VDAR 42. apsvērumu: “(..) *Lai piekrišanu būtu apzināta, datu subjektam vajadzētu būt informētam vismaz par pārziņa identitāti un paredzētās personas datu apstrādes nolūkiem (..)*.”

³¹ Atkal skatīt VDAR 42. apsvērumu.

³² Skatīt arī WP29 Atzinumu 15/2011 par piekrišanas definīciju (WP 187) un VDAR 19.-20. lpp.

³³ Skatīt VDAR 7. panta 3. punktu.

³⁴ Skatīt arī WP29 Pamatnostādnes par automatizētu individuālo lēmumu pieņemšanu un profilēšanu Regulas 2016/679 nolūkiem (WP251), IV.B. punkts, 20. lpp. un turpmāk.

³⁵ Saskaņā ar 49. panta 1. punkta a) apakšpunktu, prasot nepārprotamu piekrišanu, ir nepieciešama konkrēta informācija par 46. pantā aprakstīto aizsardzības pasākumu neesību. Skatīt arī Atzinumu 15/2011 par piekrišanas definīciju (WP 187), 19. lpp.

³⁶ Piekrišanas deklarācijai tā arī jābūt nosauktai. Formulējums, piemēram, “Es zinu, ka ...” neatbilst skaidras valodas prasībai.

Pārzinim jānodrošina, ka piekrišana tiek sniegta, pamatojoties uz informāciju, kas ļauj datu subjektiem viegli identificēt, kura persona ir pārzinis, un saprast, kam viņi piekrīt. Pārzinim ir skaidri jāapraksta datu apstrādes, kurai tiek pieprasīta piekrišana, nolūks³⁷.

Citi konkrēti norādījumi par pieejamību ir ietverti WP29 pamatnostādņēs par pārredzamību. Ja piekrišana jāsniedz elektroniskā formā, pieprasījumam jābūt skaidram un īsam. Vispusīgas un detalizētas informācijas sniegšana var būt atbilstošs veids, kā izpildīt divējādo pienākumu nodrošināt precizitāti un pilnīgumu, no vienas puses, un saprotamību, no otras puses.

Pārzinim ir jāizvērtē mērķauditorija, kas tā organizācijai iesniedz personas datus. Piemēram, ja mērķauditorijā ietilpst nepilngadīgas personas, pārzinim ir jānodrošina, ka informācija ir saprotama šai vecuma grupai³⁸. Kad ir identificēta mērķauditorija, pārziņiem jānosaka, kāda informācija tiem būtu jāsniedz un pēc tam — kā tie sniegs informāciju datu subjektiem.

Regulas 7. panta 2. punktā apskatīti iepriekš sagatavotas rakstiskas piekrišanas deklarācijas, kas skar arī citus jautājumus. Ja piekrišanu pieprasa līguma (papīra formā) ietvaros, piekrišanas pieprasījums būtu skaidri jānošķir no citiem jautājumiem. Ja līgumā papīra formā ir ietverti vairāki aspekti, kas nav saistīti ar piekrišanu personas datu izmantošanai, jautājums par piekrišanu būtu jāaplūko tā, lai tas būtu skaidri izcelts, vai atsevišķā dokumentā. Tāpat, ja piekrišana tiek pieprasīta elektroniskā formā, piekrišanas pieprasījumam jābūt atsevišķam un atšķirīgam, tā nevar tikt vienkārši iekļauta kā punkts nosacījumos saskaņā ar 32. apsvērumu³⁹. Lai pielāgotos maziem ekrāniem vai situācijām, kad informācijas telpa ir ierobežota, attiecīgā gadījumā var apsvērt vispusīgu informācijas sniegšanas veidu, lai izvairītos no pārmērīgiem lietotāju pieredzes vai produktu dizaina traucējumiem.

Pārzinim, kurš atsaucas uz datu subjekta piekrišanu, ir jāizpilda arī 13. un 14. pantā noteiktie atsevišķi sniegtas informācijas pienākumi, lai nodrošinātu atbilstību VDAR. Praksē informācijas prasību izpilde un apzinātas piekrišanas prasības ievērošana daudzos gadījumos var radīt integrētu pieeju. Tomēr šī iedaļa ir rakstīta, izprotot, ka spēkā esoša “apzināta” piekrišana var pastāvēt pat tad, ja piekrišanas procesā nav minēti visi 13. un/vai 14. panta elementi (protams, šos jautājumus vajadzētu minēt citās vietās, piemēram, uzņēmuma paziņojumā par konfidencialitāti). WP29 ir izsniegusi atsevišķas pamatnostādnes par pārredzamības prasībām.

[12. piemērs]

Uzņēmums X ir pārzinis, kurš saņēmis sūdzības, ka datu subjektiem nav skaidrs, kādiem datu izmantošanas nolūkiem tiek prasīta viņu piekrišana. Uzņēmums apzinās, ka ir jāpārbauda, vai tā piekrišanas pieprasījumā ietvertā informācija ir saprotama datu subjektiem. X organizē brīvprātīgu testa grupu konkrētām tā klientu īpašām kategorijām un sniedz šīm testa auditorijām atjauninātu piekrišanas informāciju pirms šādas

³⁷ Skatīt VDAR 4. panta 11. punktu un 7. panta 2. punktu.

³⁸ Skatīt arī 58. apsvērumu par informāciju, kas saprotama bērniem.

³⁹ Skatīt arī 42. apsvērumu un Direktīvu 93/13/EEK, jo īpaši 5. pantu (vienkārša saprotama valoda un šaubu gadījumā interpretācija būs labvēlīga patērētājam) un 6. pantu (negodīgu noteikumu spēkā esamība, līgums joprojām ir spēkā bez šiem noteikumiem tikai tad, ja tas joprojām ir saprātīgs, pretējā gadījumā viss līgums kļūst spēkā neesošs).

informācijas paziņošanas ārpus uzņēmuma. Grupas sastāva atlasē ir ievērots neatkarības princips un atlase tiek veikta, pamatojoties uz tādiem standartiem, kas nodrošina reprezentatīvu, objektīvu iznākumu. Grupa saņem aptaujas anketu un norāda tajā, ko tā ir sapratusi no informācijas, un savu vērtējumu par to, cik saprotama un atbilstoša ir informācija. Pārzinis turpina testēšanu, līdz grupas norāda, ka informācija ir saprotama. X sagatavo testa ziņojumu un saglabā to pieejamu turpmākai atsaucēi. Šis piemērs parāda iespējamo veidu, kā X var pierādīt, ka datu subjekti saņēma skaidru informāciju pirms personas piekrišanas X veiktai personas datu apstrādei.

[13. piemērs]

Uzņēmums veic datu apstrādi uz piekrišanas pamata. Uzņēmums izmanto vispusīgu privātuma paziņojumu, kurā ietverts piekrišanas pieprasījums. Uzņēmums norāda visu pamata informāciju par pārzini un paredzētajām datu apstrādes darbībām⁴⁰. Tomēr uzņēmums pirmajā paziņojuma slānī nav norādījis, kā var sazināties ar datu aizsardzības speciālistu. Lai būtu spēkā esošs likumīgais pamats, kā paredzēts 6. pantā, šis pārzinis saņēma spēkā esošu "apzinātu" piekrišanu arī tad, ja datu aizsardzības speciālista kontaktinformācija nav paziņota datu subjektam (pirmajā informācijas slānī) atbilstīgi VDAR 13. panta 1. punkta b) apakšpunktam vai 14. panta 1. punkta b) apakšpunktam.

3.4. Viennozīmīga norāde par vēlmēm

VDAR ir skaidri noteikts, ka piekrišanai ir nepieciešams datu subjekta paziņojums vai skaidra apstiprinoša darbība, kas nozīmē, ka tā vienmēr sniedzama aktīvā veidā vai, izmantojot deklarāciju. Ir jābūt acīmredzamam, ka datu subjekts ir piekritis konkrētajai apstrādei.

Direktīvas 95/46/EK 2. panta h) apakšpunktā aprakstīta piekrišana ir "vēlmju (..) norādījums, ar kuru datu subjekts izsaka savu piekrišanu uz viņu attiecināmu personas datu apstrādei". VDAR 4. panta 11. punkts balstās uz šo definīciju, precizējot, ka spēkā esošajai piekrišanai nepieciešama *viennozīmīga* norāde, izmantojot *paziņojumu vai ar skaidri apstiprinošu darbību*, saskaņā ar 29. darba grupas iepriekšējiem norādījumiem.

"Skaidri apstiprinoša darbība" nozīmē, ka datu subjekts ir apzināti piekritis konkrētai apstrādei⁴¹. 32. apsvērumā sniegti papildu norādījumi šajā sakarā. Piekrišanu var saņemt arī, izmantojot rakstisku vai (ierakstītu) mutisku apliecinājumu, tostarp elektroniskus līdzekļus.

⁴⁰ Ievērojiet, ka, ja pārziņa identitāte vai apstrādes mērķis nav redzams vispusīga privātuma paziņojuma pirmajā informācijas slānī (un tas atrodas turpmākajos apakšējos slāņos), datu pārzinim būs grūti pierādīt, ka datu subjekts ir sniedzis apzinātu piekrišanu, ja vien datu pārzinis nevar pierādīt, ka attiecīgais datu subjekts piekļuvis šai informācijai pirms piekrišanas saņemšanas.

⁴¹ Skatīt Komisijas darba dokumenta "Ietekmes novērtējums" 2. pielikumu, 20. lpp., kā arī 105.-106. lpp.: "Kā norādīts arī 29. panta darba grupas pieņemtajā atzinumā par piekrišanu, ir svarīgi precizēt, ka spēkā esoša piekrišana prasa izmantot mehānismus, kas novērš jebkādas šaubas par datu subjekta nodomu sniegt piekrišanu, vienlaikus skaidri norādot, ka attiecībā uz tiešsaistes vidi noklusējuma izvēļu izmantošana, kas datu subjektam ir jāmaina, lai noraidītu apstrādi ("piekrišana, pamatojoties uz klusēšanu"), pati par sevi nav viennozīmīga piekrišana. Tas sniegtu indivīdiem lielāku kontroli pār viņu datiem gadījumos, kad apstrāde notiek, pamatojoties uz piekrišanu. Attiecībā uz ietekmi uz datu pārziņiem nebūtu būtiskas ietekmes, jo tas vienīgi precizē un labāk izklāsta pašreizējās direktīvas radītās sekas attiecībā uz datu subjekta spēkā esošas un jēgpilnas piekrišanas nosacījumiem. It īpaši tiktāl, ciktāl "nepārprotama" piekrišana precizētu, aizstājot "nepārprotamu", piekrišanas kārtību un kvalitāti un to, ka tā nav paredzēta, lai paplašinātu gadījumus un situācijas, kad (nepārprotamu) piekrišanu vajadzētu izmantot kā pamatu, nav sagaidāms, ka šī pasākuma ietekme uz datu pārziņiem būs nozīmīga."

Iespējams, ka visburtiskākais veids, kā izpildīt “rakstveida paziņojuma” kritēriju, ir pārliecināties, ka datu subjekts vēstulē vai e-pastā datu pārzinim paskaidro, kam tieši viņš piekrīt. Tomēr tas bieži vien nav reāli izpildāms. VDAR atbilstīgi rakstveida paziņojumi var būt dažādi.

Neskarot spēkā esošās (valstu) līgumtiesības, piekrišanu var iegūt, ierakstot mutisku paziņojumu, lai gan pirms piekrišanas norādīšanas ir jādokumentē, kāda informācija ir pieejama datu subjektam. Iepriekš atzīmētu izvēles aiļu izmantošana VDAR nav derīga. Datu subjekta klusēšana vai neaktivitāte, kā arī tikai pakalpojumu izmantošanas turpināšana nevar tikt uzskatīta par aktīvu izvēles rādītāju.

[14. piemērs]

Uzstādot programmatūru, lietotne prasa datu subjekta piekrišanu izmantot neanonimizētus ziņojumus par negadījumiem programmatūras uzlabošanas nolūkā. Piekrišanas pieprasījumam tiek pievienots vispusīgs privātuma paziņojums ar nepieciešamo informāciju. Aktīvi atzīmējot izvēles aili, kurā norādīts “Es piekrītu”, lietotājs var likumīgi veikt “skaidri apstiprinošu darbību”, piekrītot apstrādei.

Pārzinim arī jāuzmanās, lai šādu piekrišanu nevarētu saņemt, vienlaikus piekrītot līgumam vai pieņemot vispārīgos pakalpojuma sniegšanas noteikumus. Vispārīgu noteikumu vispārēja pieņemšana nav uzskatāma par skaidri apstiprinošu darbību, ar ko piekrīt personas datu izmantošanai. VDAR neļauj pārziņiem piedāvāt iepriekš atzīmētas ailes vai atteikšanās konstrukcijas, kas pieprasa datu subjekta iejaukšanos, lai atteiktos no vienošanās (piemēram, “atteikšanās ailes”)⁴².

Ja piekrišana ir jādod pēc elektroniska pieprasījuma, pieprasījums nedrīkstētu *nevajadzīgi* pārtraukt tā pakalpojuma izmantošanu, kam tiek sniegta piekrišana⁴³. Aktīvi apstiprinoša darbība, ar ko datu subjekts norāda uz piekrišanu, var būt nepieciešama, ja mazāk ierobežojošs vai traucējošs režīms radītu neskaidrību. Tādējādi var būt nepieciešams piekrišanas pieprasījumam daļēji pārtraukt lietošanas pieredzi, lai šis pieprasījums būtu spēkā esošs.

Tomēr saskaņā ar VDAR prasībām pārzinim ir tiesības izstrādāt savas organizācijas vajadzībām atbilstošu piekrišanas plūsmu. Šajā sakarā fiziskās darbības var uzskatīt par skaidri apstiprinošu darbību VDAR izpratnē.

Pārziņiem būtu jāizstrādā piekrišanas mehānismi tādā veidā, kas ir saprotams datu subjektiem. Pārziņiem jāizvairās no neskaidrības un jānodrošina, ka darbības, ar kurām tiek sniegta piekrišana, var atšķirt no citām darbībām. Tādēļ tīmekļa vietnes parastās izmantošanas turpināšana nav uzskatāma par rīcību, no kuras var secināt, ka datu subjekts vēlas norādīt savu piekrišanu ierosinātajai apstrādes darbībai.

[15. piemērs]

Joslas novilkšana ekrānā, pamāšana viedās kameras priekšā, viedtālruna pagriešana pulksteņrādītāja virzienā vai astoņnieka uzzīmēšanas kustība var būt iespējas, ar ko norāda piekrišanu, ja vien ir sniegta skaidra

⁴² Skatīt 7. panta 2. punktu. Skatīt arī Darba dokumentu 02/2013 par piekrišanas saņemšanu attiecībā uz sīkdatnēm (WP 208), 3.-6. lpp.

⁴³ Skatīt VDAR 32. apsvērumu.

informācija, un ir skaidrs, ka attiecīgā kustība nozīmē piekrišanu konkrētam pieprasījumam (piemēram, velkot šo joslu pa kreisi, jūs piekrītat X informācijas lietošanai Y nolūkam. Atkārtojiet šo darbību, lai apstiprinātu). Pārzinim jāspēj pierādīt, ka piekrišana ir iegūta šādā veidā, un datu subjektiem jāspēj atcelt piekrišanu tikpat viegli, kā tā tikusi sniegta.

[16. piemērs]

Ritināšana uz leju vai tīmekļa vietnes pārlūkošana neatbilst prasībai par skaidri apstiprinošu darbību. Tas ir tādēļ, ka brīdinājums “ritināšanas turpināšana nozīmē piekrišanu” var būt grūti atšķirams un/vai to var neievērot, ja datu subjekts ātri pārlūko lielu teksta apjomu, un šāda rīcība nav pietiekami viennozīmīga.

Digitālajā kontekstā daudziem pakalpojumiem ir nepieciešami personas dati, tādēļ datu subjekti saņem daudzkārtējus piekrišanas pieprasījumus, uz kuriem katru dienu ir jāatbild, klikšķinot un velkot. Tas var zināmā mērā izraisīt nogurumu no klikšķiem: ja šādi brīdinājumi parādās pārāk bieži, samazinās piekrišanas mehānismu faktiskā brīdinošā ietekme.

Tādējādi rodas situācija, kad jautājumi, ar ko lūdz sniegt piekrišanu, vairs netiek izlasīti. Tas ir īpašs risks datu subjektiem, jo parasti piekrišana tiek pieprasīta darbībām, kas bez viņu piekrišanas principā ir nelikumīgas. VDAR uzliek pārzinim pienākumu izstrādāt šīs problēmas risināšanas veidus.

Bieži pieminēts piemērs, kā to izdarīt tiešsaistes kontekstā, ir interneta lietotāju piekrišana, izmantojot pārlūka iestatījumus. Šādi iestatījumi būtu jāizstrādā atbilstīgi VDAR spēkā esošas piekrišanas nosacījumiem, piemēram, ka piekrišana ir detalizēta attiecībā uz katru no paredzētajiem nolūkiem un sniegtajā informācijā uzrāda pārziņus.

Jebkurā gadījumā — pirms pārzinis sāk apstrādāt personas datus, kuriem nepieciešama piekrišana, vienmēr jāsaņem piekrišana. Iepriekšējos atzinumos WP29 konsekventi ir secinājuši, ka piekrišana būtu jādod pirms apstrādes darbības veikšanas⁴⁴. Lai gan VDAR 4. panta 11. punktā nav burtiski noteikts, ka piekrišana ir jāsniedz pirms apstrādes darbības, tas skaidri no tā izriet. Šo interpretāciju apstiprina 6. panta 1. punkta virsraksts un 6. panta 1. punkta a) apakšpunktā minētais formulējums “ir devis”. No 6. panta un 40. apsvēruma loģiski izriet, ka pirms datu apstrādes uzsākšanas ir jābūt spēkā esošam likumīgajam pamatam. Tādēļ piekrišana būtu jādod pirms apstrādes darbības uzsākšanas. Principā pietiek ar vienreiz sniegtu datu subjekta piekrišanu. Tomēr pārziņiem ir jāsaņem jauna un konkrēta piekrišana, ja datu apstrādes nolūki mainās pēc piekrišanas saņemšanas vai, ja ir paredzēts papildu nolūks.

4. Nepārprotama piekrišanas saņemšana

Nepārprotama piekrišana ir nepieciešama dažās situācijās, kad rodas nopietns datu aizsardzības risks, līdz ar to augsta līmeņa individuāla kontrole pār personas datiem tiek uzskatīta par atbilstošu. Saskaņā ar VDAR nepārprotama piekrišana ir svarīga 9. pantā par īpašu kategoriju datu apstrādi, noteikumiem par datu pārsūtīšanu uz trešām valstīm vai starptautiskām organizācijām, ja nav

⁴⁴ WP29 ir konsekventi atbalstījis šo pozīciju kopš Atzinuma 15/2011 par piekrišanas definīciju (WP 187), 30.-31. lpp.

49. pantā⁴⁵ paredzēto atbilstošo aizsardzības pasākumu, un 22. pantā par automatizētu individuālu lēmumu pieņemšanu, tostarp profilēšanu⁴⁶.

VDAR paredz, ka “paziņojums vai skaidri apstiprinoša darbība” ir priekšnoteikums “parastas” piekrišanas saņemšanai. Tā kā VDAR “parastas” piekrišanas prasībai jau ir piemērots augstāks standarts salīdzinājumā ar Direktīvā 95/46/EK paredzēto piekrišanas prasību, ir nepieciešams precizēt, kādi papildu centieni pārzinim būtu jāveic, lai saņemtu *nepārprotamu* datu subjekta piekrišanu saskaņā ar VDAR.

Termins *nepārprotams* attiecas uz veidu, kādā datu subjekts pauž piekrišanu. Tas nozīmē, ka datu subjektam jāsniedz skaidrs piekrišanas apliecinājums. Acīmredzams veids, kā pārliecināties, ka piekrišana ir nepārprotama, būtu skaidri apstiprināt piekrišanu rakstiskā paziņojumā. Attiecīgā gadījumā pārzinis var pārliecināties, ka datu subjekts ir parakstījis rakstisku paziņojumu, lai nākotnē novērstu jebkādas iespējamās šaubas un iespējamo pierādījumu trūkumu⁴⁷.

Tomēr šāds parakstīts paziņojums nav vienīgais veids, kā iegūt nepārprotamu piekrišanu, un nevar teikt, ka VDAR paredz rakstiskus un parakstītus paziņojumus visos apstākļos, kad nepieciešama nepārprotama piekrišana. Piemēram, digitālā vai tiešsaistes kontekstā datu subjekts var sniegt nepieciešamo paziņojumu, aizpildot elektronisku veidlapu, nosūtot e-pastu, augšupielādējot skenētu dokumentu ar datu subjekta parakstu vai izmantojot elektronisko parakstu. Teorētiski mutiska paziņojumu izmantošana var arī būt pietiekami skaidra, lai iegūtu spēkā esošu, nepārprotamu piekrišanu, tomēr pārzinim var būt grūti pierādīt, ka visi nosacījumi spēkā esošai, nepārprotamai piekrišanai ir izpildīti, reģistrējot paziņojumu.

Organizācija var arī iegūt nepārprotamu piekrišanu, izmantojot telefona sarunu, ja informācija par izvēli ir godprātīga, saprotama un skaidra un tiek lūgts konkrēts datu subjekta apstiprinājums (piemēram, nospiežot pogu vai sniedzot mutisku apstiprinājumu).

[17. piemērs] Datu pārzinis var arī iegūt savas tīmekļa vietnes apmeklētāja nepārprotamu piekrišanu, piedāvājot nepārprotami izteiktas piekrišanas ekrānu, kurā ir ailes “Jā” un “Nē”, ar nosacījumu, ka teksts skaidri norāda piekrišanu, piemēram: “Ar šo es piekrītu manu datu apstrādei” un nevis, piemēram, “Es saprotu, ka mani dati tiks apstrādāti”. Pats par sevi saprotams, ka būtu jāizpilda apzinātas piekrišanas nosacījumi, kā arī citi nosacījumi spēkā esošas piekrišanas iegūšanai.

⁴⁵ Saskaņā ar VDAR 49. panta 1. punkta a) apakšpunktu nepārprotama piekrišana var atcelt aizliegumu datu pārsūtīšanai uz valstīm, kurās datu aizsardzības tiesību akti nav pietiekami līmenī. Jāatzīmē arī darba dokuments par kopēju 1995. gada 24. oktobra Direktīvas 95/46/EK 26. panta 1. punkta Interpretāciju (WP 114), 11. lpp., kurā WP29 norādīja, ka piekrišana datu pārsūtīšanai, kas parādās periodiski un pastāvīgi, nav atbilstoša.

⁴⁶ VDAR 22. pantā ieviesti noteikumi, kas aizsargā datu subjektus tikai pret automatizētā apstrādē, tostarp profilēšanā, balsītu lēmumu pieņemšanu. Uz šāda pamata pieņemti lēmumi ir atļauti ar noteiktiem juridiskiem nosacījumiem. Piekrišanai ir nozīmīga loma šajā aizsardzības mehānismā, jo VDAR 22. panta 2. punkta c) apakšpunktā skaidri noteikts, ka pārzinis drīkst veikt automatizētu lēmumu pieņemšanu, tostarp profilēšanu, kas var būtiski ietekmēt personu, ar datu subjekta nepārprotamu piekrišanu. WP29 šajā sakarā ir izdevusi atsevišķas pamatnostādnes. WP29 Pamatnostādnes par automatizētu lēmumu pieņemšanu un profilēšanu Regulas 2016/679 nolūkiem, 2017. gada 3. oktobris (WP 251).

⁴⁷ Skatīt arī Atzinumu 15/2011 par piekrišanas definīciju (WP 187), 25. lpp.

[18. piemērs] Kosmētikas ķirurģijas klīnika lūdz pacienta nepārprotamu piekrišanu nodot viņa medicīnisko karti ekspertam, kuram tiek lūgts sniegt alternatīvu viedokli par pacienta stāvokli. Pacienta medicīniskā karte ir digitālā datne. Ņemot vērā attiecīgās informācijas īpašo raksturu, klīnika pieprasa datu subjekta elektronisko parakstu, lai saņemtu spēkā esošu, nepārprotamu piekrišanu un varētu pierādīt, ka ir saņemta nepārprotama piekrišana⁴⁸.

Tāpat nepārprotamas piekrišanas spēkā esības nodrošināšanai var izmantot divu pakāpju pārbaudi. Piemēram, datu subjekts saņem e-pastu, informējot viņu par pārziņa nolūku apstrādāt ierakstu, kas satur medicīniskus datus. Pārzinis e-pastā paskaidro, ka viņš lūdz piekrišanu konkrēta informācijas kopuma izmantošanai konkrētam nolūkam. Ja datu subjekti piekrīt šo datu izmantošanai, pārzinis lūdz viņam atbildēt uz e-pastu, iekļaujot apliecinājumu "Es piekrītu". Pēc atbildes nosūtīšanas datu subjekts saņem apstiprinājuma saiti, uz kuras jānoklikšķina, vai arī īsziņu ar verifikācijas kodu līguma apstiprināšanai.

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 nav piemērojams neviens no b) līdz j) apakšpunktā minētajiem izņēmumiem, nepārprotamas piekrišanas iegūšana saskaņā ar VDAR norādītajiem piekrišanas nosacījumiem ir vienīgais iespējamais likumīgais izņēmums attiecībā uz šādu datu apstrādi.

[19. piemērs]

Aviosabiedrība *Holiday Airways* piedāvā ceļojumu pakalpojumus pasažieriem, kuri nevar ceļot bez palīdzības, piemēram, invaliditātes dēļ. Klients rezervē lidojumu no Amsterdamas uz Budapeštu un pieprasa palīdzības sniegšanu iekāpšanai lidmašīnā. *Holiday Airways* pieprasa viņam sniegt informāciju par viņa veselības stāvokli, lai varētu noorganizēt atbilstošus pakalpojumus (tādējādi iespēju ir daudz, piemēram, ratiņkrēsls pie vārtiem vai palīgs, kurš kopā ar viņu ceļo no punkta A līdz punktam B.) *Holiday Airways* lūdz sniegt nepārprotamu piekrišanu šā klienta veselības datu apstrādei, lai organizētu pieprasīto palīdzību ceļojumā. Datiem, kas apstrādāti uz piekrišanas pamata, vajadzētu būt nepieciešamiem pieprasītā pakalpojuma sniegšanai. Turklāt lidojumi uz Budapeštu ir pieejami arī bez ceļojumu palīdzības. Lūdzu, ņemiet vērā, ka, tā kā šie dati ir nepieciešami pieprasītā pakalpojuma sniegšanai, 7. panta 4. punktu nepiemēro.

[20. piemērs]

Panākumiem bagāts uzņēmums ir specializējies pēc pasūtījuma izgatavotu slēpošanas un snovborda aizsargbrīļļu un citu veidu āra sporta veidiem pielāgotu brīļļu ražošanā. Ideja ir tāda, ka cilvēki tās valkā, neizmantojot savas brilles. Uzņēmums saņem pasūtījumus centrālajā punktā un piegādā produktus no vienas vietas visā ES. Lai varētu nodrošināt savus individuāli pielāgotos produktus klientiem, kuri ir tuvredzīgi, pārzinis pieprasa piekrišanu informācijas par klientu acu stāvokli izmantošanai. Klienti sniedz nepieciešamos veselības datus, piemēram, receptšu datus tiešsaistē, iesniedzot savu pasūtījumu. Bez tā nav iespējams nodrošināt pieprasītās individuāli pielāgotās brilles. Uzņēmums piedāvā arī dažādas aizsargbrilles ar standartizētām korekcijas vērtībām. Klienti, kuri nevēlas izpaust veselības datus, var izvēlēties standarta versijas. Tādēļ ir nepieciešama nepārprotama piekrišana atbilstīgi 9. pantam, un piekrišanu var uzskatīt par brīvi sniegtu.

5. Papildu nosacījumi spēkā esošas piekrišanas saņemšanai

⁴⁸ Šis piemērs neskar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 910/2014 (2014. gada 23. jūlijs) par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū.

Ar VDAR ieviestas prasības pārzinim veikt papildu pasākumus, lai nodrošinātu, ka viņš saņem, uztur un spēj parādīt spēkā esošu piekrišanu. VDAR 7. pantā ir izklāstīti šie papildu nosacījumi spēkā esošai piekrišanai, ietverot īpašus noteikumus par piekrišanas reģistrēšanu un tiesībām viegli atsaukt piekrišanu. 7. pants attiecas arī uz piekrišanu, kas minēta citos VDAR pantos, piemēram, 8. un 9. pantā. Turpmāk sniegti norādījumi attiecībā uz papildu prasībām, lai parādītu spēkā esošu piekrišanu, un piekrišanas atsaukšanu.

5.1. Piekrišanas parādīšana

VDAR 7. panta 1. punktā skaidri parādīts nepārprotams pārziņa pienākums parādīt datu subjekta piekrišanu. Saskaņā ar 7. panta 1. punktu pierādīšanas pienākums ir pārzinim.

42. apsvērumā noteikts: *“Ja apstrāde pamatojas uz datu subjekta piekrišanu, pārzinim būtu jāspēj uzskatāmi parādīt, ka datu subjekts ir devis piekrišanu apstrādes darbībai.”*

Pārziņi var brīvi izstrādāt metodes, lai izpildītu šo noteikumu veidā, kas atbilst to ikdienas darbībām. Tajā pašā laikā pienākums pierādīt, ka pārzinis ir ieguvis spēkā esošu piekrišanu, pats par sevi nedrīkst radīt pārmērīgu papildu datu apstrādi. Tas nozīmē, ka pārziņiem vajadzētu būt pietiekami daudz datu, lai parādītu saikni ar apstrādi (lai parādītu piekrišanas saņemšanu), bet tiem nevajadzētu vākt vairāk informācijas nekā nepieciešams.

Pārzinim ir jāpierāda, ka no datu subjekta ir saņemta spēkā esoša piekrišana. VDAR nav precīzi noteikts, kā tas darāms. Tomēr pārzinim ir jāspēj pierādīt, ka konkrētajā gadījumā datu subjekts ir sniedzis savu piekrišanu. Kamēr tiek veikta attiecīgā datu apstrādes darbība, pastāv pienākums pierādīt piekrišanu. Pēc apstrādes beigām saskaņā ar 17. panta 3. punkta b) un e) apakšpunktu piekrišanas pierādījumu nedrīkstētu uzglabāt ilgāk, nekā tas ir strikti nepieciešams, lai izpildītu juridiskās saistības vai celtu, īstenotu vai aizstāvētu juridiskās prasības.

Piemēram, pārzinis drīkst saglabāt saņemto piekrišanas paziņojumu protokolu, lai tas varētu parādīt, kā piekrišana tika saņemta, kad tā tika saņemta, kā arī attiecīgajam datu subjektam sniegto informāciju. Pārzinis spēj arī pierādīt, ka datu subjekts tika informēts, un pārziņa darbplūsma atbilda visiem attiecīgajiem spēkā esošas piekrišanas kritērijiem. Šī pienākuma loģiskais pamatojums VDAR ir tāds, ka pārziņiem ir jāuzņemas atbildība par datu subjektu spēkā esošas piekrišanas iegūšanu un pašu ieviestajiem piekrišanas mehānismiem. Piemēram, tiešsaistes kontekstā pārzinis var saglabāt informāciju par seansu, kurā tika izteikta piekrišana, kā arī dokumentāciju par piekrišanas darbplūsmu seansa laikā un informācijas, kas tajā laikā tika sniegta datu subjektam, kopiju. Nepietiks tikai ar atsauci uz attiecīgās vietnes pareizu konfigurāciju.

[21. piemērs] Slimnīca izveido zinātniskās pētniecības programmu, ko sauc par projektu X un kuram ir vajadzīgi reāli pacienti. Dalībnieki tiek atlasīti, zvanot pa tālruni pacientiem, kuri brīvprātīgi piekrituši būt to kandidātu sarakstā, pie kuriem var vērsties šim nolūkam. Pārzinis lūdz datu subjektu nepārprotamu piekrišanu viņu zobārstniecības datu izmantošanai. Piekrišana tiek saņemta pa tālruni, ierakstot datu subjekta mutisku paziņojumu, kurā datu subjekts apstiprina, ka piekritīs viņa datu izmantošanai projekta X nolūkiem.

VDAR nav noteikts konkrēts termiņš, cik ilgi piekrišana ir derīga. Tas, cik ilgi piekrišana ir derīga, ir atkarīgs no konteksta, sākotnējās piekrišanas tvēruma un tā, ko datu subjekts sagaida. Ja apstrādes

darbības ievērojami mainās vai attīstās, sākotnējā piekrišana vairs nebūs spēkā esoša. Tādā gadījumā ir jāsaņem jauna atļauja.

WP29 iesaka kā paraugpraksi atbilstošos intervālos atjaunot piekrišanu. Atkārtota visas informācijas sniegšana palīdz nodrošināt, ka datu subjekts ir pienācīgi informēts par to, kā tiek izmantoti viņa dati un kā īstenot savas tiesības⁴⁹.

5.2. Piekrišanas atsaukšana

Piekrišanas atsaukšanai VDAR ir atvēlēta nozīmīga vieta. VDAR normas un apsvērumus par piekrišanas atsaukšanu var uzskatīt par šī jautājuma WP29 atzinumos sniegtās pašreizējās interpretācijas kodifikāciju⁵⁰.

VDAR 7. panta 3. punktā noteikts, ka pārzinim jānodrošina, lai datu subjekts jebkurā laikā var atsaukt savu piekrišanu tikpat viegli, kā to sniedzis. VDAR nenosaka, ka piekrišanas sniegšana un atsaukšana vienmēr ir jāveic, izmantojot vienu un to pašu rīcību.

Tomēr, ja piekrišana tiek iegūta, izmantojot elektroniskus līdzekļus un tikai ar vienu peles klikšķi, pavilkšanas žestu vai taustiņsienu, datu subjektiem praksē ir jābūt iespējai tikpat viegli atsaukt šo piekrišanu. Ja piekrišana tiek iegūta, izmantojot pakalpojumu īpašo lietotāja saskarni (piemēram, izmantojot vietni, lietotni, pieteikšanās kontu, IoT ierīces saskarni vai e-pastu), nav šaubu, ka datu subjektam jāspēj atsaukt piekrišanu, izmantojot vienu un to pašu elektronisko saskarni, jo pāreja uz citu saskarni tikai tāpēc, ka jāatsauc piekrišana, būtu nepamatotas pūles. Turklāt datu subjektam vajadzētu būt iespējai atsaukt savu piekrišanu bez nelabvēlīgām sekām. Tas cita starpā nozīmē to, ka pārzinim ir jāparedz piekrišanas atsaukšana bez maksas vai bez sniedzamo pakalpojuma līmeņa samazināšanas⁵¹.

[22. piemērs] Mūzikas festivāls pārdod biļetes, izmantojot tiešsaistes biļešu tirdzniecības aģentu. Katrā biļešu pārdošanā tiešsaistē tiek pieprasīta piekrišana izmantot kontaktinformāciju tirgvedības nolūkos. Lai norādītu piekrišanu šim nolūkam, klienti var izvēlēties atzīmēt "Nē" vai "Jā". Pārzinis informē klientus, ka viņiem ir iespēja atsaukt piekrišanu. Lai to izdarītu, viņiem bez maksas jāsaazinās ar zvanu centru darba dienās no plkst. 8:00 līdz 17:00. Šajā piemērā pārzinis neizpilda VDAR 7. panta 3. punkta prasības. Piekrišanas atsaukšana šajā gadījumā prasa veikt tālruņa zvanu darba laikā, kas ir apgrūtinātāk nekā viens peles klikšķis, kas bija nepieciešams, lai sniegtu piekrišanu tiešsaistes biļešu pārdevējam, kurš ir atvērts visu diennakti.

Prasība par vienkāršu atsaukšanu VDAR tiek aprakstīta kā nepieciešams spēkā esošas piekrišanas aspekts. Ja atsaukšanas tiesības neatbilst VDAR prasībām, tad pārziņa piekrišanas mehānisms neatbilst VDAR. Kā minēts 3.1. iedaļā par *apzinātas* piekrišanas nosacījumu, pārzinim saskaņā ar

⁴⁹ Skatīt WP29 pamatnostādnes par pārredzamību. [Citāts tiks precizēts, tiklīdz tas būs pieejams]

⁵⁰ WP29 ir apspriedusi šo tematu savā Atzinumā par piekrišanu (skatīt Atzinumu 15/2011 par piekrišanas definīciju (WP 187), 9., 13., 20., 27. un 32.-33. lpp.) un cita starpā savā Atzinumā par atrašanās vietas datu izmantošanu. (skatīt Atzinumu 5/2005 par atrašanās vietas datu izmantošanu, lai nodrošinātu pievienotās vērtības pakalpojumus (WP 115), 7. lpp.).

⁵¹ Skatīt arī WP29 Atzinumu 4/2010 par Eiropas *FEDMA* rīcības kodeksu attiecībā uz personas datu izmantošanu tiešajā tirdzniecībā (WP 174) un atzinumu par atrašanās vietas datu izmantošanu, lai nodrošinātu pievienotās vērtības pakalpojumus (WP 115).

VDAR 7. panta 3. punktu jāinformē datu subjekts par atteikšanās tiesībām pirms faktiskās piekrišanas saņemšanas. Turklāt pārzinim pārskatāmības pienākuma ietvaros jāinformē datu subjekti par to, kā īstenot savas tiesības⁵².

Parasti, ja piekrišana tiek atsaukta, jebkādas datu apstrādes darbības, kas balstītas uz piekrišanu, veiktas pirms piekrišanas atsaukšanas un saskaņā ar VDAR, joprojām ir likumīgas, tomēr pārzinim ir jāpārtrauc attiecīgās apstrādes darbības. Ja nav cita likumīga pamata datu apstrādei (piemēram, turpmāka saglabāšana), pārzinim tā būtu jādzēs⁵³.

Kā minēts iepriekš šajās pamatnostādņēs, ir ļoti svarīgi, lai pārziņi pirms datu vākšanas novērtētu nolūkus, kādiem dati faktiski tiek apstrādāti, un likumīgos pamatus. Bieži vien uzņēmumiem personas dati ir nepieciešami vairākiem nolūkiem, un apstrāde ir balstīta uz vairāk nekā vienu likumīgu pamatu, piemēram, klientu dati var būt balstīti gan līgumā, gan piekrišanā. Tādējādi piekrišanas atsaukšana nenozīmē, ka personas datu apstrādātājam ir jādzēs dati, kas tiek apstrādāti nolūkam, kura pamatā ir līguma ar datu subjektu izpilde. Tādēļ pārziņiem jau no paša sākuma būtu skaidri jānorāda, kāds mērķis ir piemērojams katram datu elementam un uz kādu likumīgu pamatu atsaucas.

Pārzinim ir pienākums izdzēst datus, kas apstrādāti uz piekrišanas pamata, tiklīdz šī piekrišana ir atsaukta, pieņemot, ka nav citu iemeslu, kas attaisnotu pastāvīgu saglabāšanu⁵⁴.

Papildus šai situācijai, uz ko attiecas 17. panta 1. punkta b) apakšpunkts, katrs datu subjekts var pieprasīt dzēst citus ar viņu saistītus datus, kurus apstrādā uz cita likumīga pamata, piemēram, pamatojoties uz 6. panta 1. punkta b) apakšpunktu⁵⁵. Pārzinim ir pienākums novērtēt, vai datu apstrādes turpināšana ir atbilstoša, pat ja datu subjekts nav pieprasījis dzēst datus⁵⁶.

Gadījumos, kad datu subjekts atsauc savu piekrišanu un pārzinis vēlas turpināt apstrādāt personas datus uz cita likumīga pamata, viņš nevar neinformējot pāriet no piekrišanas (kas tiek atsaukta) kā juridiska pamata uz šo citu likumīgu pamatu. Jebkādas izmaiņas apstrādes likumīgajā pamatā jāpaziņo datu subjektam saskaņā ar 13. un 14. pantā noteiktajām paziņošanas prasībām un vispārējo pārredzamības principu.

6. Mijiedarbība starp piekrišanu un citiem VDAR 6. pantā noteiktajiem likumīgajiem pamatiem

⁵² VDAR 39. apsvērumā, kas atsaucas uz Regulas 13. un 14. pantu, noteikts, ka “*fiziskās personas būtu jāinformē par riskiem, noteikumiem, aizsardzības pasākumiem un tiesībām saistībā ar personas datu apstrādi un to, kā īstenot savas tiesības saistībā ar šādu apstrādi*”.

⁵³ Skatīt VDAR 17. panta 1. punkta b) apakšpunktu un 3. punktu.

⁵⁴ Šajā gadījumā otram apstrādes pamatā esošajam nolūkam ir jābūt savam atsevišķam juridiskajam pamatam. Tas nenozīmē, ka pārzinis var pārslēgties no piekrišanas uz citu likumīgu pamatu, skatiet tālāk 6. iedaļu.

⁵⁵ Skatīt 17. pantu, tostarp iespējamus izņēmumus, un VDAR 65. apsvērumu

⁵⁶ Skatīt arī VDAR 5. panta 1. punkta e) apakšpunktu.

Regulas 6. pantā ir noteikti personas datu likumīgas apstrādes nosacījumi un aprakstīti seši likumīgie pamati, uz kuriem pārzinis var atsaukties. Pirms apstrādes darbības uzsākšanas un saistībā ar konkrētu nolūku⁵⁷ ir jāpiemēro viens no šiem sešiem pamatiem.

Šeit ir svarīgi norādīt, ka gadījumā, kad pārzinis izvēlas atsaukties uz piekrišanu kādai apstrādes daļai, tam jābūt gatavam ievērot šo izvēli un pārtraukt šo apstrādes daļu, ja persona ir atsaukusi piekrišanu. Nosūtīt ziņojumu, ka dati tiks apstrādāti uz piekrišanas pamata, lai gan faktiski tiek izmantots kāds cits likumīgais pamats, būtu pašos pamatos negodīgi attiecībā pret indivīdiem.

Citiem vārdiem sakot, pārzinis nedrīkst mainīt piekrišanu pret citu likumīgu pamatu. Piemēram, nav atļauts retrospektīvi izmantot likumīgās intereses kā juridisko pamatu, lai pamatotu apstrādi, ja ir radušās problēmas ar piekrišanas spēkā esamību. Ņemot vērā prasību atklāt juridisko pamatu, uz kuru pārzinis atsaucas personas datu vākšanai, pārzinim jau pirms vākšanas ir jāizlemj, kāds ir piemērojamais likumīgais pamats.

7. Konkrētas jomas VDAR, kuras rada bažas

7.1. Bērni (8. pants)

Salīdzinot ar pašreizējo direktīvu, VDAR izveido papildu aizsardzības slāni attiecībā uz neaizsargāto fizisko personu, jo īpaši bērnu, personas datu apstrādi. Regulas 8. pantā ievieš papildu pienākumus, lai nodrošinātu pastiprinātu bērnu datu aizsardzību saistībā ar informācijas sabiedrības pakalpojumiem. Pastiprinātās aizsardzības iemesli ir norādīti 38. apsvērumā: *“(..) viņi var pietiekami neapzināties attiecīgos riskus, sekas un aizsardzības pasākumus un savas tiesības saistībā ar personas datu apstrādi (...)”* Tapat 38. apsvērumā noteikts, ka: *“Šāda īpaša aizsardzība jo īpaši būtu jāpiemēro bērnu personas datu izmantošanai tirgvedības vajadzībām vai tādēļ, lai veidotu personu vai lietotāju profilus, un uz bērnu personas datu vākšanu, kad tiek izmantoti bērnam tiešā veidā piedāvāti pakalpojumi.”* Vārdi “jo īpaši” norāda, ka īpašā aizsardzība neattiecas tikai ar tirgvedību vai profilēšanu, bet ietver plašāku “bērnu personas datu vākšanu”.

Regulas 8. panta 1. punktā noteikts, ka gadījumos, kad tiek izmantota piekrišana attiecībā uz informācijas sabiedrības pakalpojumu tiešu sniegšanu bērnam, bērna personas datu apstrāde ir likumīga, ja bērns ir vismaz 16 gadus vecs. Ja bērns ir jaunāks par 16 gadiem, šāda apstrāde ir likumīga tikai tad un tādā apmērā, ja piekrišanu ir devusi vai apstiprinājusi persona, kurai ir vecāku atbildība par bērnu⁵⁸. Attiecībā uz spēkā esošas piekrišanas vecuma ierobežojumu VDAR nodrošina zināmu elastību, jo dalībvalstis ar likumu var paredzēt jaunāku vecumu, taču šis vecums nedrīkst būt mazāks par 13 gadiem.

Kā minēts 3.1. iedaļā par apzinātu piekrišanu, informācijai ir jābūt saprotamai mērķauditorijai, pie kuras pārzinis vērsas, īpašu uzmanību pievēršot bērnu viedoklim. Lai saņemtu “apzinātu piekrišanu” no bērna, pārzinim ir jāpaskaidro bērniem skaidrā un vienkāršā valodā, kā tas plāno

⁵⁷ Saskaņā ar 13. panta 1. punkta c) apakšpunktu un/vai 14. panta 1. punkta c) apakšpunktu pārzinim ir jāinformē datu subjekts.

⁵⁸ Neskarot dalībvalstu tiesības atkāpties no vecuma ierobežojuma, skatīt 8. panta 1. punktu.

apstrādāt savāktos datus⁵⁹. Ja piekrišanu sniedz vecāks, tad var būt nepieciešams informācijas kopums, kas ļauj pieaugušajiem pieņemt apzinātu lēmumu.

No iepriekš minētā izriet, ka 8. pantu piemēro tikai tad, ja ir izpildīti šādi nosacījumi:

- apstrāde ir saistīta ar informācijas sabiedrības pakalpojumu piedāvājumu tieši bērnam^{60,61}
- apstrāde pamatojas uz piekrišanu.

7.1.1. Informācijas sabiedrības pakalpojumi

Lai noteiktu VDAR termina “informācijas sabiedrības pakalpojums” piemērošanas jomu, VDAR 4. panta 25. punktā ir atsauce uz Direktīvu 2015/1535.

Vērtējot šīs definīcijas tvērumu, WP29 atsaucas arī uz EST judikatūru⁶². EST sprieda, ka *informācijas sabiedrības pakalpojumi* aptver līgumus un citus pakalpojumus, kas ir noslēgti vai nosūtīti tiešsaistē. Ja pakalpojumam ir divas ekonomiski neatkarīgas sastāvdaļas, no kurām viena ir tiešsaistes sastāvdaļa, piemēram, piedāvājums un piedāvājuma pieņemšana saistībā ar līguma slēgšanu vai informācija par produktiem vai pakalpojumiem, tostarp tirgvedības darbības, šī sastāvdaļa tiek definēta kā informācijas sabiedrības pakalpojums, savukārt otra sastāvdaļa ir preču fiziska piegāde vai izplatīšana, kas neietilpst informācijas sabiedrības pakalpojuma jēdzienā. Pakalpojuma sniegšana tiešsaistē ietilpst VDAR 8. pantā iekļautā termina “informācijas sabiedrības pakalpojums” piemērošanas jomā.

7.1.2. Tieša sniegšana bērnam

Formulējuma “tieša sniegšana bērnam” iekļaušana norāda, ka 8. pantu paredzēts piemērot dažiem, bet ne visiem informācijas sabiedrības pakalpojumiem. Šajā ziņā, ja informācijas sabiedrības pakalpojumu sniedzējs potenciālajiem lietotājiem skaidri norāda, ka piedāvā pakalpojumus tikai personām, kuras ir vismaz 18 gadus vecas, un šo apgalvojumu neapstrīd citi pierādījumi (piemēram,

⁵⁹ VDAR 58. apsvērumā atkārtoti apstiprināts šis pienākums, norādot, ka attiecīgā gadījumā pārzinim būtu jāpārliciecinās, vai sniegtā informācija ir saprotama bērniem.

⁶⁰ Saskaņā ar VDAR 4. panta 25. punktu “informācijas sabiedrības pakalpojums” ir pakalpojums, kā definēts Direktīvas 2015/1535 1. panta 1. punkta c) apakšpunktā: “b) *“pakalpojums” ir jebkāds Informācijas sabiedrības pakalpojums, tas ir, jebkāds pakalpojums, ko parasti sniedz par atlīdzību no attāluma, ar elektroniskiem līdzekļiem un pēc pakalpojumu saņēmēja individuāla pieprasījuma. Šajā definīcijā: i) “no attāluma” nozīmē, ka pakalpojumu sniedz bez vienlaicīgas pušu klātbūtnes; ii) “ar elektroniskiem līdzekļiem” nozīmē, ka pakalpojumu nosūta un galamērķī saņem ar elektroniskas apstrādes (ietverot digitālu kompresiju) un datu uzglabāšanas aparātūras palīdzību un ka to pilnībā pārraida, nosūta un saņem pa vadiem, pa radio ar optiskiem vai citiem elektromagnētiskiem līdzekļiem; iii) “pēc pakalpojumu saņēmēja individuāla pieprasījuma” nozīmē, ka pakalpojumu sniedz, pārraidot datus pēc individuāla pieprasījuma.” Orientējošs to pakalpojumu saraksts, uz kuriem neattiecas šī definīcija, ietverts minētās Direktīvas I pielikumā. Skatīt Direktīvas 2000/31/EK 18. apsvērumu.*

⁶¹ Saskaņā ar ANO Konvencijas par bērna aizsardzību 1. pantu: “(..) par bērnu tiek uzskatīts ikviens cilvēks, kas nav sasniedzis 18 gadu vecumu, ja vien saskaņā ar attiecīgiem tiesību aktiem pilngadība neiestājas agrāk”, skatīt Apvienoto Nāciju Organizācijas Vispārējās asamblejas 1989. gada 20. novembra Rezolūciju 44/25 (Bērnu tiesību konvencija).

⁶² Skatīt Eiropas Savienības Tiesas 2010. gada 2. decembra spriedumu lietā C-108/09 (*Ker-Optika*), 22. un 28. punkts. Saistībā ar “jauktajiem pakalpojumiem” WP29 atsaucas arī uz lietas C-434/15 (*Asociacion Profesional Elite Taxi pret Uber Systems Spain SL*) 40. punktu, kas nosaka, ka informācijas sabiedrības pakalpojumu, kas ir neatņemama tāda kopējā pakalpojuma sastāvdaļa, kura galvenā sastāvdaļa nav informācijas sabiedrības pakalpojums (šajā gadījumā transporta pakalpojums), nedrīkst kvalificēt kā “informācijas sabiedrības pakalpojumu”.

vietnes saturs vai tirgvedības plāni), tad pakalpojums netiks uzskatīts par “tieši sniegtu bērnam” un 8. pants netiks piemērots.

7.1.3. Vecums

VDAR noteikts, ka “*dalībvalstis minētajiem nolūkiem ar likumu var paredzēt jaunāku vecumu, ar noteikumu, ka šāds jaunāks vecums nav mazāks par 13 gadiem*”. Pārzinim jāzina minētie dažādie valsts tiesību akti, ņemot vērā sabiedrību, uz ko attiecas tā pakalpojumi. Jo īpaši jānorāda, ka pārzinis, kurš sniedz pārrobežu pakalpojumus, ne vienmēr var atsaukties tikai uz tās dalībvalsts tiesību aktiem, kurā atrodas tā galvenā mītne, bet, iespējams, tam ir jāievēro katras attiecīgās dalībvalsts valsts tiesību akti, kurā tas piedāvā informācijas sabiedrības pakalpojumu (-us). Tas ir atkarīgs no tā, vai dalībvalsts izvēlas izmantot pārziņa galvenās mītnes vietu kā atsauces punktu valsts tiesību aktos vai arī datu subjekta dzīvesvietu. Vispirms visām dalībvalstīm, izdarot šādu izvēli, ir jāņem vērā bērna intereses. Darba grupa aicina dalībvalstis rast saskaņotu risinājumu šajā jautājumā.

Ja informācijas sabiedrības pakalpojumi tiek sniegti bērniem uz piekrišanas pamata, sagaidāms, ka pārziņi pieliks saprātīgas pūles, lai pārliecinātos, ka lietotājs ir sasniedzis digitāli sniegtās piekrišanas obligāto vecumu, un šiem pasākumiem vajadzētu būt samērīgiem attiecībā uz apstrādes darbību veidu un risku.

Ja lietotāji apgalvo, ka viņi ir vecāki par digitāli sniegtās piekrišanas obligāto vecumu, pārzinis var veikt atbilstošas pārbaudes, lai pārliecinātos, ka šis apgalvojums ir patiess. Kaut arī VDAR nav viennozīmīgi noteikts pienākums pielikt saprātīgas pūles, lai pārliecinātos par vecumu, tas ir netieši izteikts, jo datu apstrāde kļūs nelikumīga gadījumā, kad bērns sniedz piekrišanu, bet nav sasniedzis attiecīgo vecumu, lai sniegtu spēkā esošu piekrišanu savā vārdā.

Ja lietotājs norāda, ka nav sasniedzis digitālās piekrišanas sniegšanai obligāto vecumu, pārzinis šo apgalvojumu var pieņemt, neveicot turpmākas pārbaudes, taču tam ir jāsaņem vecāku piekrišana un jāpārbauda, ka personai, kura sniedz šo piekrišanu, ir vecāku atbildība.

Vecuma pārbaudes nedrīkstētu novest pie pārmērīgas datu apstrādes. Mehānismam, kas izvēlēts, lai pārbaudītu datu subjekta vecumu, būtu jāietver paredzamās apstrādes riska novērtējums. Dažās zema riska situācijās var būt atbilstoši pieprasīt pakalpojuma jaunajam abonentam atklāt savu dzimšanas gadu vai aizpildīt veidlapu, kurā norādīts, ka viņš ir (nav) nepilngadīgs⁶³. Ja rodas šaubas, pārzinim konkrētajā gadījumā būtu jāpārskata savi vecuma pārbaudes mehānismi un jāapsver, vai ir nepieciešamas alternatīvas pārbaudes⁶⁴.

7.1.4. Bērnu piekrišana un vecāku atbildība

⁶³ Lai gan tas var nebūt pilnīgi drošs risinājums visos gadījumos, tas ir piemērs iespējamai rīcībai saistībā ar šo normu.

⁶⁴ Skatīt WP29 Atzinumu Nr. 5/2009 par sociālo tīklu pakalpojumiem (WP 163).

Attiecībā uz personu, kurai ir vecāku atbildība, VDAR nenosaka praktiskus veidus, kā saņemt vecāka piekrišanu vai konstatēt, ka persona ir tiesīga šādi rīkoties⁶⁵. Tādēļ WP29 iesaka izmantot proporcionālu pieeju atbilstīgi VDAR 8. panta 2. punktam un 5. panta 1. punkta c) apakšpunktam (datu minimizācija). Proporcionāla pieeja var būt vērsta uz to, lai iegūtu ierobežotu informācijas daudzumu, piemēram, vecāku vai aizbildņa kontaktinformāciju.

Kas ir saprātīgi gan attiecībā uz pārbaudēm, vai lietotājs ir pietiekami vecs, lai sniegtu savu piekrišanu, gan attiecībā uz to, vai personai, kura sniedz bērna piekrišanu bērna vārdā, ir vecāku atbildība, var būt atkarīgs no apstrādei raksturīgiem riskiem, kā arī pieejamajām tehnoloģijām. Zema riska gadījumos var pietikt ar vecāku atbildības pārbaudi pa e-pastu. Turpretim augsta riska gadījumos var būt atbilstoši pieprasīt papildu pierādījumus, lai pārzinis varētu pārbaudīt un saglabāt informāciju atbilstīgi VDAR 7. panta 1. punktam⁶⁶. Uzticamu trešo personu pārbaudes pakalpojumi var ietvert risinājumus, kas samazina personas datu apjomu, kādu pārzinis pats apstrādā.

[23. piemērs] Interneta spēļu platforma vēlas pārliecināties, ka nepilngadīgi klienti abonē tās sniegtos pakalpojumus tikai ar savu vecāku vai aizbildņu piekrišanu. Pārzinis veic šādas darbības:

1. solis — lūdz lietotājiem norādīt, vai viņi ir jaunāki par 16 gadiem (vai alternatīvs vecums digitālās piekrišanas sniegšanai).

Ja lietotājs norāda, ka ir jaunāks par digitālās piekrišanas sniegšanas obligāto vecumu, seko

2. solis — pakalpojuma sniedzējs informē bērnu, ka vecākam vai aizbildnim ir jāpiekrīt vai jāpilnvaro apstrāde, pirms bērnam tiek sniegts pakalpojums. Lietotājam tiek lūgts norādīt vecāka vai aizbildņa e-pasta adresi.

3. solis — pakalpojuma sniedzējs sazinās ar vecāku vai aizbildni un iegūst viņa piekrišanu apstrādei pa e-pastu, un veic atbilstošus pasākumus, lai pārliecinātos, ka pieaugušajam ir vecāku atbildība.

4. solis — sūdzību gadījumā platforma veic papildu pasākumus abonenta vecuma pārbaudei.

Ja platforma ir izpildījusi citas piekrišanas saņemšanai nepieciešamās prasības, platforma, veicot šīs darbības, var izpildīt VDAR 8. pantā noteiktos papildu kritērijus.

Piemērā ir redzams, ka pārzinis var pierādīt, ka viņš ir spējis pielikt saprātīgas pūles, lai nodrošinātu, ka ir iegūta spēkā esoša piekrišana saistībā ar bērnam sniegtajiem pakalpojumiem. Jo īpaši 8. panta 2. punktā papildus nosaka, ka: *“Pārzinis pieliek saprātīgas pūles, lai šādos gadījumos pārbaudītu, vai piekrišanu ir devusi vai apstiprinājusi persona, kurai ir vecāku atbildība par bērnu, ņemot vērā pieejamās tehnoloģijas”*.

Pārziņa pienākums ir noteikt, vai pasākumi konkrētajā gadījumā ir atbilstoši. Parasti pārziņiem vajadzētu izvairīties no pārbaudes risinājumiem, kas paši par sevi ietver pārmērīgu personas datu vākšanu.

WP29 atzīst, ka var būt gadījumi, kad pārbaude ir apgrūtināša (piemēram, ja bērni, kas sniedz savu piekrišanu, vēl nav izveidojuši “identitātes pēdas nospiedumu” vai arī ir sarežģīti pārbaudīt vecāku

⁶⁵ WP29 norāda, ka ne vienmēr persona, kurai ir vecāku atbildība, ir bērna bioloģiskais vecāks un ka vecāku atbildība var būt vairākām personām, kuras var būt gan juridiskas, gan fiziskas personas.

⁶⁶ Piemēram, no vecākiem vai aizbildņiem var pieprasīt veikt pārzinim maksājumu EUR 0,01 apmērā, izmantojot bankas darījumu, tostarp īsu apstiprinājumu darījuma aprakstā, ka bankas konta turētājam ir vecāku atbildība pār lietotāju. Attiecīgā gadījumā būtu jāparedz alternatīva pārbaudes metode, lai novērstu nepamatoti diskriminējošu attieksmi pret personām, kurām nav bankas konta.

atbildību. To var ņemt vērā, lemjot, kādi centieni ir saprātīgi, bet pārziņiem ir jāturpina pastāvīgi pārskatīt savas ieviestās procedūras un pieejamās tehnoloģijas.

Attiecībā uz datu subjekta tiesībām neatkarīgi sniegt piekrišanu savu personas datu apstrādei un pilnībā kontrolēt apstrādi, tiklīdz datu subjekts ir sasniedzis digitālās piekrišanas sniegšanai nepieciešamo vecumu, personas, kurai ir vecāku atbildība, piekrišanu vai pilnvarojumu bērna personas datu apstrādei var apstiprināt, grozīt vai atsaukt.

Praksē tas nozīmē, ka, ja bērns neveic nekādas darbības, personas, kurai ir vecāku atbildība, piekrišana vai pilnvarojums personas datu apstrādei, kas sniegts, pirms bērns ir sasniedzis digitālās piekrišanas sniegšanai nepieciešamo vecumu, joprojām būs spēkā esošs apstrādes pamatojums.

Pēc digitālās piekrišanas sniegšanas obligātā vecuma sasniegšanas bērnam būs iespēja pašam atsaukt piekrišanu saskaņā ar 7. panta 3. punktu. Saskaņā ar godprātības un pārskatatbildības principiem, pārzinim bērns ir jāinformē par šo iespēju⁶⁷.

Ir svarīgi norādīt, ka saskaņā ar 38. apsvērumu vecāka vai aizbildņa piekrišana nav nepieciešama bērnam tieši sniegtu profilaktisku vai konsultāciju pakalpojumu kontekstā. Piemēram, bērnu aizsardzības pakalpojumu sniegšanai bērnam tiešsaistē, izmantojot tiešsaistes tērzēšanas pakalpojumu, nav nepieciešama iepriekšēja vecāku atļauja.

Visbeidzot, VDAR noteikts, ka noteikumi par vecāku pilnvaru izsniegšanu attiecībā uz nepilngadīgajiem neietekmē “dalībvalstu vispārējās līgumtiesības, piemēram, noteikumus par attiecībā uz bērnu noslēgta līguma spēkā esību, noslēgšanu vai sekām”. Tādēļ prasības attiecībā uz spēkā esošu piekrišanu datu par bērniem izmantošanai ir daļa no tiesiskā regulējuma, kas jāskata atsevišķi no valstu līgumtiesībām. Tādēļ šajās pamatnostādnēs nav aplūkots jautājums, vai tiešsaistes līgumu noslēgšana ar nepilngadīgo ir likumīga. Abus tiesiskos režīmus var piemērot vienlaicīgi, un VDAR piemērošanas joma neietver valstu līgumtiesību noteikumu saskaņošanu.

7.2. Zinātniskā pētniecība

Zinātniskās pētniecības nolūku definēšanai ir būtiska ietekme uz datu apstrādes darbību klāstu, ko var veikt pārzinis. Termins “zinātniskā pētniecība” VDAR nav definēts. 159. apsvērumā noteikts: “(..) Šajā regulā personas datu apstrāde zinātniskās pētniecības nolūkos būtu jāinterpretē plaši.” (..)”, tomēr WP29 uzskata, ka šis jēdziens nevar būt plašāks nekā tā vispārējā nozīme, un “zinātniskā pētniecība” šajā kontekstā nozīmē pētniecības projektu, kas saskaņā ar labo praksi izveidots atbilstīgi attiecīgajiem ar nozari saistītajiem metodoloģiskajiem un ētikas standartiem.

Ja piekrišana ir pētniecības veikšanas juridiskais pamats saskaņā ar VDAR, šī piekrišana personas datu izmantošanai būtu jānošķir no citām piekrišanas prasībām, kas kalpo par ētikas standartu vai procesuālajām pienākumiem. Piemērs šādam procesuālajam pienākumam, ja apstrāde ir balstīta nevis uz piekrišanu, bet gan uz citu juridisku pamatu, ir atrodams Klīnisko pārbaužu regulā. Datu aizsardzības tiesību kontekstā pēdējo minēto piekrišanas veidu var uzskatīt par papildu aizsardzības

⁶⁷ Turklāt datu subjektiem vajadzētu būt informētiem par tiesībām tikt aizmirstam, kā noteikts 17. pantā, kas jo īpaši attiecas uz piekrišanu, kas sniegta laikā, kad datu subjekts vēl bija bērns; skatīt 63. apsvērumu.

pasākumu⁶⁸. Tajā pašā laikā VDAR neierobežo 6. panta piemērošanu attiecībā tikai uz datu apstrādi pētniecības nolūkiem. Kamēr pastāv atbilstoši aizsardzības pasākumi, piemēram, prasības saskaņā ar 89. panta 1. punktu, un apstrāde ir godprātīga, likumīga, pārredzama un atbilst datu minimizācijas standartiem un individuālajām tiesībām, var izmantot citus juridiskos pamatus, piemēram, 6. panta 1. punkta e) vai f) apakšpunktā noteiktos⁶⁹. Tas attiecas arī uz īpašu kategoriju datiem saskaņā ar atkāpi no 9. panta 2. punkta j) apakšpunkta⁷⁰.

Šķiet, ka 33. apsvēruma nodrošina zināmu elastīgumu attiecībā uz piekrišanas konkrētības un detalizācijas pakāpi zinātniskās pētniecības kontekstā. Proti, 33. apsvērumā noteikts: *“Bieži vien datu vākšanas laikā, kad dati tiek vākti zinātniskās pētniecības nolūkos, nav iespējams pilnībā identificēt personas datu apstrādes nolūku. Tāpēc būtu jāļauj datu subjektiem dot savu piekrišanu attiecībā uz dažām zinātniskās pētniecības jomām, ja tiek ievēroti atzīti zinātniskās pētniecības ētiskie standarti. Datu subjektiem vajadzētu būt iespējai dot piekrišanu tikai konkrētām pētniecības jomām vai pētniecības projektu daļām, ciktāl to ļauj paredzētais nolūks.”*

Pirmkārt, būtu jānorāda, ka 33. apsvēruma neatceļ pienākumus attiecībā uz konkrētas piekrišanas prasību. Tas nozīmē, ka principā zinātniskās pētniecības projekti var ietvert personas datus uz piekrišanas pamata tikai tad, ja tiem ir labi aprakstīts nolūks. Gadījumos, kad datu apstrādes nolūkus zinātniskās pētniecības projekta sākumā nav iespējams precizēt, 33. apsvērumā kā izņēmums ir paredzēts, ka nolūku var aprakstīt vispārīgākā līmenī.

Ņemot vērā VDAR 9. pantā noteiktos striktos nosacījumus attiecībā uz īpašu kategoriju datu apstrādi, WP29 norāda, ka tad, kad tiek apstrādāti īpašu kategoriju dati uz nepārprotamas piekrišanas pamata, izmantojot 33. apsvēruma elastīgo pieeju, tiks piemērota stingrāka interpretācija un pieprasīta rūpīgāka pārbaude.

Skatot kopumā, VDAR nevar interpretēt tā, ka pārzinis drīkstētu atkāpties no pamatprincipa norādīt nolūkus, kādiem tiek prasīta datu subjekta piekrišana.

Ja pētniecības mērķus nevar pilnībā precizēt, pārzinim ir jāmeklē citi veidi, kā nodrošināt atbilstību piekrišanas prasību būtībai, piemēram, ļaujot datu subjektiem sniegt piekrišanu vispārīgāk formulētam pētnieciskajam mērķim un konkrētiem pētījuma projekta posmiem, kuri ir zināmi jau pašā sākumā. Pētniecības projekta gaitā pirms nākamā posma sākuma var saņemt piekrišanu projekta turpmākajām darbībām. Tomēr šādai piekrišanai būtu jāatbilst piemērojamiem zinātnisko pētījumu ētikas standartiem.

Turklāt pārzinis šādos gadījumos var piemērot papildu drošības pasākumus. Piemēram, 89. panta 1. punktā ir uzsvērtā nepieciešamība pēc aizsardzības pasākumiem datu apstrādes darbībās zinātniskās vai vēstures pētniecības vai statistikas nolūkiem. Uz šiem nolūkiem *“attiecas*

⁶⁸ Skatīt arī VDAR 161. apsvērumu.

⁶⁹ Regulas 6. panta 1. punkta c) apakšpunkts var tikt piemērots arī tādām apstrādes darbībām, kas ir īpaši paredzētas tiesību aktos, piemēram, uzticamu un stabilu datu vākšanai pēc protokola, ko dalībvalsts apstiprinājusi saskaņā ar Klīnisko pārbaužu regulu.

⁷⁰ Konkrēta zāļu pārbaude var tikt veikta, pamatojoties uz ES vai valsts tiesību aktiem saskaņā ar 9. panta 2. punkta i) apakšpunktu.

atbilstošas garantijas datu subjekta tiesībām un brīvībām”. Kā iespējamie aizsardzības pasākumi minēta datu minimizācija, anonimizācija un datu drošība⁷¹. Anonimizācija ir vēlmais risinājums, tiklīdz pētījuma mērķi var sasniegt bez personas datu apstrādes.

Pārredzamība ir papildu aizsardzības pasākums, ja pētījuma apstākļi nepieļauj konkrētu piekrišanu. Nolūka konkrētības trūkumu var atsvērt ar pārziņa regulāri sniegtu informāciju par nolūka attīstību pētniecības projekta gaitā, lai vēlāk piekrišana būtu iespējami konkrēta. Tādējādi datu subjektam ir vismaz pamata izpratne par situāciju, ļaujot viņam novērtēt, vai izmantot, piemēram, tiesības atsaukt piekrišanu saskaņā ar 7. panta 3. punktu⁷².

Turklāt, ja datu subjektiem ir pieejams visaptverošs pētījuma plāns, pirms tie sniedz piekrišanu, tas varētu palīdzēt kompensēt nolūka konkrētības trūkumu⁷³. Šajā pētījuma plānā pēc iespējas skaidri būtu jānorāda pētāmie jautājumi un darba metodes. Pētījuma plāns varētu veicināt arī atbilstību 7. panta 1. punktam, jo pārziņiem, lai varētu parādīt, ka piekrišana ir spēkā esoša, ir jānorāda, kāda informācija datu subjektiem bija pieejama piekrišanas brīdī, .

Ir svarīgi atcerēties, ka gadījumos, kad piekrišana tiek izmantota kā apstrādes likumīgais pamats, datu subjektam ir jābūt iespējai atsaukt šo piekrišanu. WP29 norāda, ka piekrišanas atsaukšana varētu apdraudēt tādus zinātniskos pētījumus, kuriem nepieciešami dati, ko var saistīt ar privātpersonām, tomēr VDAR ir skaidri noteikts, ka piekrišanu var atsaukt un ka pārziņiem šajā sakarā ir jārīkojas — šai prasībai netiek piemērots izņēmums zinātniskās pētniecības nolūkos. Ja pārzinis saņem piekrišanas atsaukšanas pieprasījumu, tam faktiski nekavējoties ir jādzēš personas dati, ja tas vēlas turpināt izmantot datus pētījuma nolūkos⁷⁴.

7.3. Datu subjekta tiesības

Ja datu apstrādes darbība pamatojas uz datu subjekta piekrišanu, tas ietekmēs minētās personas tiesības. Datu subjektiem var būt tiesības uz datu pārnesamību (20. pants), ja apstrāde pamatojas uz piekrišanu. Tajā pašā laikā tiesības iebilst (21. pants) nepiemēro, ja apstrāde pamatojas uz piekrišanu, lai gan tiesības atsaukt piekrišanu jebkurā laikā var nodrošināt līdzīgu rezultātu.

⁷¹ Skatīt, piemēram, 156. apsvērumu. Personas datu apstrādei zinātniskos nolūkos būtu jāatbilst arī citiem attiecīgajiem tiesību aktiem, piemēram, attiecībā uz klīniskiem izmēģinājumiem, skatīt 156. apsvērumu, kas atsaucas uz Eiropas Parlamenta un Padomes 2014. gada 16. aprīļa Regulu (ES) Nr. 536/2014 par cilvēkiem paredzētu zāļu klīniskajām pārbaudēm. Skatīt arī Atzinumu 15/2011 par piekrišanas definīciju (WP 187), 7. lpp.: “Turklāt piekrišanas saņemšana neatceļ pārziņa pienākumus saskaņā ar 6. pantu attiecībā uz godprātību, nepieciešamību un proporcionalitāti, kā arī datu kvalitāti. Piemēram, pat ja personas datu apstrāde ir balstīta uz lietotāja piekrišanu, tas nepadara likumīgu tādu datu vākšanu, kas ir pārmērīgi attiecībā uz konkrēto nolūku.” (..) Principā piekrišanu nevajadzētu uzskatīt par atbrīvojumu no citiem datu aizsardzības principiem, bet gan par garantiju. Tā galvenokārt ir pamats rīcības likumībai, un tas neatceļ citu principu piemērošanu.”

⁷² Var būt piemēroti arī citi pārredzamības pasākumi. Kad pārziņi iesaistās datu apstrādē zinātniskiem nolūkiem, kamēr sākumā nav iespējams sniegt pilnīgu informāciju, viņi varētu norīkot konkrētu kontaktpersonu, pie kuras datu subjekti var vērsties ar jautājumiem.

⁷³ Šāda iespēja ir rodama Somijas pašreizējā Datu aizsardzības likuma 14. panta 1. punktā (*Henkilötietolaki*, 523/1999)

⁷⁴ Skatīt arī WP29 Atzinumu 05/2014 par anonimizācijas metodēm (WP216).

VDAR 16. līdz 20. pantā norādīts, ka (gadījumos, kad datu apstrādes pamatā ir piekrišana) datu subjektiem ir tiesības uz dzēšanu, ja piekrišana ir atsaukta, un tiesības uz ierobežošanu, labojumu veikšanu un piekļuvi⁷⁵.

8. Saskaņā ar Direktīvu 95/46/EK iegūta piekrišana

Pārziņiem, kuri patlaban apstrādā datus uz piekrišanas pamata, kas atbilst valstu datu aizsardzības tiesību aktiem, gatavojoties VDAR, nav automātiski pilnībā jāatjauno visas līdzšinējās piekrišanas attiecības ar datu subjektiem. Līdz šim iegūtā piekrišana joprojām ir spēkā, ciktāl tā atbilst VDAR noteiktajiem nosacījumiem.

Pārzinim būtu rūpīgi jāpārskata pašreizējie darba procesi un ieraksti pirms 2018. gada 25. maija, lai pārliecinātos, ka esošās piekrišanas atbilst VDAR standartam (skatīt VDAR 171. apsvērumu⁷⁶). Praksē VDAR ievieš augstāku standartu attiecībā uz piekrišanas mehānismu ieviešanu un vairākas jaunas prasības, kas pārziņiem liek mainīt piekrišanas mehānismus, ne tikai pārrakstīt privātuma politiku⁷⁷.

Piemēram, tā kā VDAR pieprasa, lai pārzinis varētu parādīt, ka ir iegūta spēkā esoša piekrišana, visi iespējamie piekrišanas gadījumi, par kuriem nav saglabātas atsauces, automātiski tiks uzskatīti par neatbilstošiem VDAR piekrišanas standartiem un būs jāatjauno. Tāpat, tā kā VDAR pieprasīts “paziņojums vai skaidri apstiprinoša darbība”, visi iespējamie piekrišanas gadījumi, kas balstīti uz datu subjekta netiešāku darbību (piemēram, iepriekš atzīmēta izvēles aile), arī nebūs atbilstoši VDAR piekrišanas standartiem.

Turklāt, lai varētu pierādīt, ka piekrišana ir saņemta, vai lai dotu iespēju sīkāk norādīt datu subjekta vēlmes, var būt nepieciešams pārskatīt darbību un IT sistēmas. Turklāt ir jābūt pieejamiem mehānismiem, kas datu subjektiem ļauj vienkārši atsaukt savu piekrišanu, un jāsniedz informācija par to, kā atsaukt piekrišanu. Ja spēkā esošās piekrišanas iegūšanas un pārvaldības procedūras neatbilst VDAR standartiem, pārziņiem būs jāsaņem jauna, VDAR prasībām atbilstoša piekrišana.

No otras puses, tā kā nosacījumam par apzinātu piekrišanu ne vienmēr ir nepieciešami visi 13. un 14. pantā minētie elementi, VDAR paplašinātie informēšanas pienākumi ne vienmēr ir pretrunā tādas piekrišanas nepārtrauktībai, kas piešķirta pirms VDAR stāšanās spēkā (skatīt 15. lpp. iepriekš). Direktīvā 95/46/EK nepastāvēja prasība informēt datu subjektus par datu apstrādes pamatu.

⁷⁵ Gadījumos, kad saskaņā ar VDAR 18. pantu noteiktas datu apstrādes darbības tiek ierobežotas, ierobežojumu atcelšanai var būt nepieciešama datu subjekta piekrišana.

⁷⁶ VDAR 171. apsvērumā noteikts: “Ar šo regulu būtu jāatceļ Direktīva 95/46/EK. Apstrāde, kas jau tiek veikta dienā, kad šo regulu sāk piemērot, būtu jāpārskatīta ar šo regulu divos gados pēc šīs regulas spēkā stāšanās dienas. Ja apstrāde pamatojas uz piekrišanu, ievērojot Direktīvu 95/46/EK, datu subjektam nav vēlreiz jānodrošina piekrišana, ja veids, kādā piekrišana ir sniegta, atbilst šīs regulas nosacījumiem, lai tādējādi ļautu pārzinim turpināt šādu apstrādi pēc šīs regulas piemērošanas dienas. Saskaņā ar Direktīvu 95/46/EK pieņemtie Komisijas lēmumi un uzraudzības iestāžu izsniegtās atļaujas paliek spēkā līdz brīdim, kad tās tiek grozītas, aizstātas vai atceltas.”

⁷⁷ Kā norādīts ievadā, VDAR sīkāk paskaidrotas un precizētas prasības spēkā esošās piekrišanas saņemšanai un parādīšanai. Daudzas no jaunajām prasībām ir balstītas Atzinumā 15/2011 par piekrišanu.

Ja pārzinis konstatē, ka saskaņā ar iepriekšējo tiesību aktu iegūtā piekrišana neatbilst VDAR piekrišanas standartam, tad pārzinim ir jāveic pasākumi, lai nodrošinātu atbilstību šiem standartiem, piemēram, atjaunojot piekrišanu VDAR prasībām atbilstošā veidā. Saskaņā ar VDAR nav iespējams mainīt vienu likumīgo pamatu pret citu. Ja pārzinis nevar atjaunot piekrišanu atbilstošā veidā, kā arī nespēj (vienreizējā situācijā) pāriet uz VDAR atbilstības nodrošināšanu, datu apstrādi pamatojot ar citu likumīgo pamatu un vienlaikus nodrošinot, ka nepārtraukta apstrāde ir godprātīga un pārskatatbildīga, viņam apstrādes darbības ir jāpārtrauc. Jebkurā gadījumā pārzinim ir jāievēro likumīgas, godprātīgas un pārredzamas apstrādes principi.

._*._*._*._*._*._*._*._*._***DOKUMENTA BEIGAS***._*._*._*._*._*._*._*._*._*._*._*._*._*._*._*