DATU SUBJEKTA PIEKRIŠANA KĀ PERSONAS DATU APSTRĀDES PAMATS

Mg. iur. ***Māris Bomiņš,***
Biznesa augstskolas Turība studiju programmas "Juridiskā zinātne", doktorants, Latvija

Abstract

While the principles encompassed by the General Data Protection Regulation (GDPR) were mostly welcomed, one of them, namely the consent, caused prolonged controversy among privacy scholars, human rights advocates and business world due to their pivotal impact on the way personal data would be handled under the new legal provisions and the drastic consequences of enforcing these new requirements in the era of big data and internet of things. In this work, we firstly review all controversies around the new stringent definitions of consent in reference to their implementation impact on privacy and personal data protection, and secondly, we evaluate existing legislation in terms of fulfilling the practicalities for the implementation and effective integration of the new requirements.

For the reasons explained above, consent is far removed from an easy option under the GDPR. Greater specification around what is meant by consent has brought with it more detailed and onerous obligations. Additionally, sometimes may first wish to look closely at the other legal grounds available to establish whether there is an available alternative to the consent path. In addition, given the extensive lengths that a data controller now has to go to demonstrate a valid consent according new legislation, it is important to see what further steps may be needed to distinguish such a consent from one that is explicit. For this and other reasons, the arguments around what makes consent effective are unlikely to be put to bed by the GDPR and it remains a rough-edged concept to tackle.

Keywords: data protection law, data subject consent, the freely given consent under the GDPR, concent procedure.

 http://dx.doi.org/10.17770/acj.v3i84.3655

Ievads

Jau pašreiz tiesības uz personas datu aizsardzību nešaubīgi ir daļa no tiesībām uz privātās dzīves neaizskaramību un ir nostiprinātas gan nacionālajā, gan Eiropas Savienības līmenī. Taču ātrā tehnoloģiju izaugsme ir radījusi jaunas problēmas personas datu aizsardzības jomā. Datu apmaiņas un vākšanas apjoms ir dramatiski pieaudzis. Jaunākās tehnoloģijas ļauj gan privātām sabiedrībām, gan valsts iestādēm vēl nepieredzētā apjomā savas darbības mērķiem izmantot personas datus. Minētie priekšnoteikumi radīja nepieciešamību pārvērtēt Eiropas Savienībā eksistējošos personas datu aizsardzības noteikumus un radīt vispusīgu un saskaņotu regulējumu, kas garantētu indivīdu pamattiesību uz personas datu aizsardzību ievērošanu visā Eiropas Savienībā. 2016. gada 14. aprīlī beidzās vairāk kā četru gadu ilgais gaidīšanas periods, kas sākās 2012. gada janvārī ar Eiropas Komisijas iniciatīvu reorganizēt personas datu aizsardzības regulējumu un 2018. gada 25. maijā, noslēdzoties divu gadu pārejas periodam, stājās spēkā jaunā Eiropas Parlamenta un Padomes Regula 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (turpmāk – Regula), kas aizvietoja Fizisko personu datu aizsardzības likumu. Kaut gan Regulā ietvertais reglamentējums nav revolūcija datu aizsardzības jomā, taču viens no Regulas mērķiem ir būtiski paaugstināt indivīda personas datu aizsardzības līmeni.

Viens no personas datu apstrādes pamatprincipiem paredz, ka jebkurai fizisko personu datu apstrādei ir jābūt likumīgai[1]. Personu datu apstrādei jābūt tiesiski pamatotai, proti, jāizpilda vismaz viens no Regulas 6. pantā minētajiem 6 nosacījumiem, kas ļauj pārzinim likumīgi veikt datu apstrādi. Starp tiem ir arī datu subjekta piekrišana. Tomēr, lai datu subjekta piekrišana būtu spēkā esoša un būtu pietiekams pamats personas datu apstrādes veikšanai, Regula iezīmē vairākus datu subjekta piekrišanas nosacījumus, tāpēc raksta mērķis ir analizēt Regulā minētos likumīgas piekrišanas nosacījumus un ierobežojumus, kas jāievēro datu pārzinim, veicot personu datu apstrādi uz šī tiesiskā pamata. **Pētījuma objekts** – datu subjekta derīgas piekrišanas kā personu datu apstrādes pamata izpēte kopsakarā ar vispārīgiem datu apstrādes principiem, mērķiem, apstrādes nolūkiem un to nošķiršana no citiem likumīgiem datu apstrādes veidiem un pamatiem. **Pētījuma priekšmets** – datu

subjekta derīgas piekrišanas nosacījumi, juridiskie aspekti un to norobežošana no operatora datu apstrādes nolūkiem.

Raksta ietvaros veiktā pētījuma uzdevums ir analizēt Regulu, kopsakarā ar nacionālajiem normatīvajiem aktiem, lai nodrošinātu efektīvu Regulas piemērošanu. Uzdevuma veikšanai noskaidrosim pastāvošos ierobežojumus, tiesu prakses risinājumus un salīdzināsim Latvijas un citu valstu regulējumu, kas atbilstoši Regulai jāievieš obligāti vai ieviešams pēc dalībvalsts ieskatiem. Pētījuma rezultātā doti ierosinājumi tiesiskā regulējuma izpratnes pilnveidošanai.

Pētījuma bāze ir normatīvie akti, tiesu nolēmumi, statistikas dati, doktrīnas atziņu un viedokļu analīze. Raksta izstrādē izmantota analīzes un sintēzes metode, kā arī salīdzinošā un vēsturiskā metode.

Personas piekrišanas kritēriji datu apstrādes pamatojumā

Praksē var šķist, ka datu apstrādes tiesiskais pamats – subjekta piekrišana ir drošākais starp pamatojumiem, jo datu subjekts piekrīt savu datu apstrādei, taču šāds secinājums ne vienmēr atbilst patiesībai, jo bieži vien nav izprasti visi nosacījumi, lai piekrišana atbilstu Regulas prasībām. Turklāt jāatzīst, ka līdzšinējā regulējumā, kaut gan arī bija noteikti piekrišanas nosacījumi, tās robežas bija izplūdušas un veidojās situācija, ka dalībvalstis piekrišanu traktēja nepamatoti sašaurināti vai paplašināti. Saistībā ar šo "Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvas 95/46 EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti 29. panta datu aizsardzības darba grupa" (turpmāk – Darba grupa) 2011. gadā sniedza viedokli par datu apstrādes tiesisko pamatu – subjekta piekrišanu, vienlaicīgi atzīstot šī institūta sarežģīto dabu[2]. Uzsāktā datu aizsardzības reforma ļāva pārskatīt piekrišanas institūtu un Regulas ietvaros izveidot vienveidīgu un uz kopējiem principiem balstītu piekrišanas koncepciju, piekrišanu datu apstrādē definējot daudz precīzāk. Atbilstoši Regulas 4. panta 11. punktam 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***. Iepriekš piekrišana bija definēta kā – *datu subjekta brīvi, nepārprotami izteikts gribas apliecinājums, ar kuru datu subjekts atļauj apstrādāt savus personas datus atbilstoši pārziņa sniegtajai informācijai*[3]. Regulas ietvaros piekrišanai izvirzītas daudz plašākas prasības. Tādējādi,

lai datu subjekta piekrišana būtu spēkā esoša un būtu pietiekams pamats personas datu apstrādes veikšanai, Regula iezīmē vairākus nosacījumus un ierobežojumus, kas jāievēro datu pārzinim, veicot personu datu apstrādi uz šī tiesiskā pamata.

Brīvi sniegta piekrišana – kā priekšnoteikums likumīgai datu subjekta piekrišanai kontekstā ar Regulas prasībām, jākonstatē divi raksturīgi kritēriji:

1) datu subjekta reālā izvēle,

2) kontrole pār saviem datiem.

Datu subjekta izvēles realitāti raksturo tas, ka piekrišana, kas ietverta neapstrīdamajos nosacījumos, atbilstoši Regulas regulējumam netiek uzskatīta par brīvi sniegtu. Turklāt, piekrišana nav uzskatāma par brīvi izteiktu, ja datu subjekts nevar atteikties vai atsaukt savu izvēli bez nelabvēlīgām sekām[4]. Ikdienas mobilā tālruņa lietošanā itin bieži sastopamies ar nepieciešamību lejuplādēt dažādas lietotnes, informāciju utt. Piemēram, situācijā, kad fotogrāfiju apstrādei paredzētās mobilās lietotnes izstrādātājs, pieprasa mobilā tālruņa lietotājam aktivizēt GPS reklāmas saņemšanai, piekrišana nebūs uzskatāma par brīvi izteiktu. Piekrišanas izteikšana attiecībā uz datu apstrādi, kas neizriet no sākotnējā mērķa, apmaiņa pret, piemēram, efektivitāti vai pakalpojuma saņemšanu, šajā gadījuma neveido brīvu piekrišanu. Tādējādi, piekrišana netiek uzskatīta par brīvi sniegtu, ja datu subjektam ir nosacījums piekrist tikai vienlaikus visām datu apstrādes darbībām vai nevienai. Gadījumos, kad datu apstrāde ietver vairākas datu apstrādes darbības vai vairākus mērķus, datu pārzinim jādod iespēju datu subjektam izteikt brīvu piekrišanu atsevišķi par katru no izvēlēm. Ja datu pārzinis ir apvienojis piekrišanas izteikšanu par dažādiem apstrādes mērķiem un nav paredzējis atsevišķu piekrišanu dažādām personas datu apstrādes darbībām, piekrišana šajā gadījumā nav sniegta brīvi[5].

Otrs brīvi sniegtas piekrišanas kritērijs ir datu subjekta kontrole pār saviem datiem. Saskaņā ar to datu subjektam ir tiesības atsaukt savu piekrišanu jebkurā laikā[6]. Piekrišanas atsaukums neietekmē to datu apstrādes likumību, kas veikta saskaņā ar piekrišanu pirms atsaukuma. Datu subjektam jābūt par to informētam, pirms viņš dod piekrišanu. Turklāt, šajā gadījumā pārzinim jānodrošina sekojoša principa ievērošana: *"atsaukt piekrišanu ir tikpat viegli kā to dot"*[7]. Svarīgi, ka šajā gadījumā tas nenozīmē, ka piekrišanas sniegšanai un atsaukšanai ir jānotiek vienādā veidā, tomēr abām darbībām

jābūt vienlīdz viegli veicamām. Piemēram, ja piekrišana dota, veicot atzīmi mājas lapā norādītā lauciņā, tad tās atsaukšana, zvanot pārzinim konkrētā darba laikā, nebūtu tikpat viegla.

Tomēr ne vienmēr datu subjekta piekrišana, kas pirmsšķietami satur brīvas piekrišanas pazīmes, par tādu tiks uzskatīta. Eiropas Parlamenta un Padomes darba grupa, kas ir izstrādājusi vadlīnijas arī vairāku Regulas normu piemērošanai, atzinumos Nr. 2/2017[8] un Nr .8/2001[9] par personas datu apstrādi nodarbinātības jomā atkāroti ir paudusi viedokli, ka maldīgs ir priekšstats par to, ka piekrišana ir galvenais un labākais tiesiskais pamats darbinieka personas datu apstrādei. Ņemot vērā atkarību, kas izriet no darba devēja/darba ņēmēja attiecībām, visbiežāk piekrišana var netikt uzskatīta par derīgu tiesisko pamatu darbinieka personas datu apstrādei, jo darbiniekam nav īstas vai brīvas izvēles to izteikt vai atsaukt bez iespējamām nelabvēlīgām sekām (t.i., bez bažām, ka tā varētu izraisīt nelabvēlīgu darba devēja reakciju un atsaukties uz darbinieka novērtējumu, atalgojumu, izaugsmi vai citiem ar darba tiesiskajām attiecībām saistītiem jautājumiem). Regulas preambulas 42. un 43. apsvērums atkarību interpretē kā *"skaidru nevienlīdzību"* datu subjekta un pārziņa (tostarp darbinieka un darba devēja) attiecībās, kas liek apšaubīt, vai piekrišana ir sniegta brīvi[10]. Regulas izpratnē nevienlīdzība starp pārzini un datu subjektu var veidoties ne vien tikai darba tiesiskajās attiecībās, bet jebkurā citā sfērā, kur pastāv izteikta datu subjekta tiesību nevienlīdzība. Piemēram, Regulas izpratnē aizliegts apstrādāt īpašo kategoriju personas datus (sensitīvie dati) izņemot gadījumus, kad datu subjekts ir devis nepārprotamu piekrišanu. Tomēr Savienības vai dalībvalstu tiesību aktos atļauts precizēt apstrādes darbības un apstrādes procedūras attiecībā uz personas datu apstrādi, ko veic kompetentas iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai lai sauktu pie atbildības par tiem[11]. Ņemot vērā iepriekš minēto un kopsakarā ar 2016. gada 27. aprīlī pieņemto Policijas direktīvu, kas paredz pienākumu dalībvalstīm pieņemt un publicēt normatīvos un administratīvos aktus, kas vajadzīgi, lai izpildītu šīs direktīvas prasības, šobrīd tiek izstrādāts "Personu datu apstrādes tiesībaizsardzības iestādēs likums"[12] un tajā attiecībā uz īpašu kategoriju personas datu apstrādi tiek noteikti stingrāki apstrādes nosacījumi. Ņemot vērā tiesībsargājošo iestāžu darba specifiku un to, ka tiek īstenota valsts sodošā funkcija, likumprojektā kā tiesiskais pamats īpašu kategoriju

personas datu apstrādei nav paredzēta personas piekrišana, jo pastāv bažas, ka saskarē ar tiesībsargājošām iestādēm persona neizdara patiesi brīvu izvēli. Tādējādi, visos gadījumos, kad pastāv pazīmes, ka datu subjekta un pārziņa attiecībās pastāv skaidra nevienlīdzība, piekrišanas datu apstrādei vietā atbilstošāk būtu izvēlēties citu tiesisko pamatu. Savukārt, datu apstrāde ir jāpārtrauc, ja nav cita tiesiskā pamata apstrādāt datus.

Regulā ir ietverti papildus nosacījumi, kas var ietekmēt izvērtējumu vai piekrišana sniegta brīvi, tas ir piekrišanas "apvienošana" ar nosacījumu pieņemšanu vai līguma, vai pakalpojuma sniegšanas "piesaistīšana" piekrišanai tādai personas datu apstrādei, kas nav nepieciešama šā līguma vai pakalpojuma izpildei[13]. Piekrišanas apvienošana varētu būt situācijā, kad persona vēlas iegādāties tiešsaistē lidmašīnas biļeti un pircējam jāpiekrīt ne tikai personu datu apstrādei, kas nepieciešama šim darījumam, bet arī jāatļauj izmantot savus datus mārketinga nolūkos. Pienākums piekrist personas datu izmantošanai papildus nepieciešamajam datu apstrādes apjomam, ierobežo datu subjekta izvēli un kavē brīvi sniegtu piekrišanu. Šajā gadījumā papildus apstrādes darbības mārketinga vajadzībām nav būtiskas, lai izpildītu līgumu un, padarot pirkumu atkarīgu no šādas piekrišanas, tā nebūs sniegta brīvi. Savukārt, ja piekrišanas pieprasījums ir saistīts ar datu pārziņa līgumsaistību izpildi, datu subjekts, kurš nevēlās, lai personas dati pārzinim būtu pieejami apstrādei, riskē, ka viņam tiks atteikts nepieciešamais pakalpojums. Tādējādi, izvērtējot brīvas piekrišanas sniegšanas nosacījumus attiecībā uz piekrišanas "sasaistīšanu" vai "apvienošanu", svarīgi noteikt, kāda ir līguma darbības joma un kādi dati būs nepieciešami līguma izpildei. Regulas 7. panta 4. punkta kontekstā, apstrādei ir jābūt nepieciešamai, lai izpildītu līgumu ar katru datu subjektu atsevišķi, tādējādi Regulas noteikums *"nepieciešams līguma izpildei"* ir jāinterpretē ļoti šauri[14]. Piemēram, attiecībā uz iepriekš minēto gadījumu, pieļaujama datu subjekta dzīves vietas adreses apstrāde, gadījumā ja būtu nepieciešamība piegādāt tiešsaistē iegādātās lidmašīnas biļetes. Tādējādi, Regulas 7. panta 4. punkts ir piemērojams tikai tad, ja pieprasītie dati nav nepieciešami līguma izpildei un šo datu iegūšana uz piekrišanas pamata ir līgumsaistību izpildes nosacījums. Savukārt, ja apstrāde ir nepieciešama līguma izpildei, tostarp pakalpojumu sniegšanai, tad 7. panta 4. punktu nepiemēro.

Ja datu subjekta piekrišana ir brīvi sniegta, likumīgas piekrišanas

konstatēšanai nepieciešams arī, lai piekrišana būtu **konkrēta.** Konkrētās piekrišanas mērķis ir datu subjekta datu apstrādes procesu un mērķu kontrole.

Izvērtējot konkrētas piekrišanas nosacījumus, nošķir trīs piekrišanas konkrētuma komponentes:

1) konkrētas piekrišanas aizsardzība pret tehnisko difūziju. Pakāpeniska tehnoloģijas vai sistēmas izmantošanas paplašināšana ārpus sākotnēji paredzētā mērķa, var radīt iespējamu sākotnējās piekrišanas mērķa paplašināšanu, un tas šajā gadījumā neveidos likumīgu datu subjekta piekrišanu;

2) konkrētas piekrišanas detalizētība. Ja datu apstrādes mērķis nav pietiekami konkrēts, datu subjekts var piekrist mērķiem, kuriem viņš nebūtu piekritis, ja mērķis būtu detalizētāks;

3*) ar konkrēto piekrišanu saņemtās informācijas precīzs atdalījums no citas informācijas*. Regulas kontekstā ir jāsaņem atsevišķa piekrišana katram mērķim, kuram dati tiek apstrādāti.[15] Jebkura datu apstrādes mērķu apvienošana rada brīvības trūkumu, kā rezultātā nav arī likumīgas datu subjekta piekrišanas. 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, jānodrošina atsevišķa izvēle katram nolūkam, lai lietotāji varētu sniegt konkrētu piekrišanu konkrētiem nolūkiem[16]. Turklāt šajā gadījumā svarīga pārziņa sniegtās informācijas pietiekamība, lai datu subjekts būtu spējīgs izvērtēt jauno datu apstrādes mērķu iespējamo ietekmi attiecībā uz citiem mērķiem, par kuriem datu subjekts jau sniedzis vai sniegs savu piekrišanu. Tādējādi, ja no datu subjekta tiek iegūta vispārīga piekrišana apstrādāt personas datus, nenodalot šos apstrādes mērķus, tad šādu piekrišanu nevar uzskatīt par konkrētu un tā nav izmantojama.

Apzināta piekrišana saturiski pārklājas gan ar brīvi sniegtu, gan ar konkrētu piekrišanu, tomēr Regulas kontekstā tas ir atsevišķs kritērijs likumīgas piekrišanas konstatēšanai. Ja iepriekš konstatējām, ka piekrišanai jābūt brīvi sniegtai, konkrētai attiecībā uz apstrādes mērķi utt., kā arī jāatbilst visiem pārējiem piekrišanas elementiem, tad likumsakarīga ir datu subjekta informēšana. Datu subjekta informēšana daļēji attiecas uz brīvas piekrišanas elementu,

kad datu subjektam ir tiesības izdarīt patiesu izvēli, taču apzinātas piekrišanas kontekstā prevalē pārredzamības pamatprincips[17], kura pamatā ir prasība pārzinim apstrādāt personas datus tikai tad, ja viņš ir informējis datu subjektu[18] par pārziņa identitāti un paredzētās personas datu apstrādes nolūkiem[19], kā arī par Regulas 13, 14.pantos norādīto pieejamo informāciju, tas ir datu apstrādes apjomu, apstrādes nolūku, personas datu saņēmēju kategorijām, datu uzglabāšanas laiku, datu subjekta tiesībām utt. Informācijas sniegšana datu subjektam pirms piekrišanas saņemšanas ir būtiska, lai subjekts var pieņemt apzinātu lēmumu un saprast, kam viņš piekrīt. Savukārt, ja pārzinis nesniedz pietiekamu informāciju, lietotāja kontrole pār saviem datiem kļūst iluzora un piekrišana kļūst par spēkā neesošu juridisku fikciju. Regulas kontekstā nav noteikta informācijas sniegšanas forma vai veids, lai izpildītu prasību par apzinātu piekrišanu, taču pastāv vairāki nosacījumi. Viens no būtiskiem nosacījumiem attiecībā uz apzinātu piekrišanu ir tas, ka pārzinim visos gadījumos jānodrošina, ka tiek izmantota skaidra un vienkārša valoda[20]. Ņemot vērā datu subjektu iespējamo īpatsvaru, kopsakarā ar vairākām datu subjektu kategorijām attiecībā uz kurām var tikt veikta datu apstrāde, secināts, ka informēšanai vajadzētu būt viegli saprotamai ne tikai juristiem, advokātiem vai personām, kuras darbojas datu aizsardzības jomā, bet arī parastam/vidusmēra cilvēkam (angļu – *regular/average person*)[21]. Līdz ar to pārzinim ir jāizvērtē mērķauditorija, kuras dati tiks apstrādāti un ja, piemēram, mērķauditorijā ietilpst nepilngadīgas personas, pārzinim jānodrošina, ka informācija ir saprotama šai vecuma grupai[22]. Pēc mērķauditorijas identificēšanas, pārzinim jānosaka, kāda informācija būtu jāsniedz un kādā veidā informācija datu subjektiem tiks sniegta. Datu subjekta informētības izvērtēšanai, izšķiroša nozīme ir informācijas sniegšanas veidam (vienkāršs teksts, neizmantojot žargonu, saprotama, pamanāma), ka arī informācijai jābūt skaidri redzamai (fontu veids un izmērs), ievērojamai un visaptverošai[23]. Nepietiek ar norādi, ka informācija kaut kur ir pieejama[24]. Ja piekrišana tiek noformēta līgumā papīra formātā vai elektroniskā formā, piekrišanas pieprasījumam jābūt atsevišķam un atšķirīgam[25].

Lai izpildītu apzinātas piekrišanas prasību izpildi, piekrišana būtu jādod ar skaidru apstiprinošu darbību, tas nozīmē **viennozīmīgu norādi** par datu subjekta piekrišanu ar viņu saistīto personas datu apstrādei[26]. Arī attiecībā uz sensitīvo datu apstrādi, Regula paredz

datu apstrādi, ja datu subjekts ir devis nepārprotamu piekrišanu šo personas datu apstrādei.[27] Kaut gan abos gadījumos datu subjekta piekrišana sniedzama aktīvā apstiprinošā darbībā, ar ko datu subjekts norāda uz piekrišanu[28], datu subjekta subjektīvo pusi attiecībā uz vispārējo datu apstrādi nosaka *"viennozīmīga"*, bet uz sensitīvo datu apstrādi *"nepārprotama"* piekrišana. Ņemot vērā, ka abos gadījumos datu subjekts piekrišanu sniedz aktīvā veidā un jābūt acīmredzamam, ka datu subjekts ir piekritis konkrētai apstrādei, rodas jautājums vai šie jēdzieni interpretējami atšķirīgi. Vēsturiski datu subjekta piekrišanu formulēja, kā *"norādi par vēlmēm, ar kuru datu subjekts apliecina savu piekrišanu personas datiem, kas attiecas uz viņu, apstrādi"*[29]. Sākotnējais Eiropas Komisijas priekšlikums bija pievienot *"nepārprotamas"* piekrišanas kritēriju, lai izvairītos no maldinošas līdzības ar *"viennozīmīgu"* piekrišanu un lai iegūtu vienu, konsekventu piekrišanas definīciju, saskaņā ar kuru datu subjekts apzinās savu piekrišanu[30]. Tomēr 2015. gadā Eiropas Komisija nāca klajā ar visaptverošu datu aizsardzības priekšlikumu paketi, kas paredzēja līdzsvarot regulējumu attiecībā uz vispārīgo un sensitīvo datu apstrādi, nosakot, ka datu subjektu piekrišanas veids ir nepārprotams visai personas datu apstrādei, precizējot, ka tam ir vajadzīga "skaidra pozitīva rīcība", un šī piekrišana ir jādara "skaidri" attiecībā uz sensitīviem datiem[31]. Līdz ar to paziņojums vai skaidri apstiprinošā darbība ir priekšnoteikums "parastās" vai vispārīgās piekrišanas saņemšanai, savukārt termins "nepārprotams" attiecas uz veidu, kādā datu subjekts pauž piekrišanu.

Acīmredzams veids, kā pārliecināties, ka piekrišana ir nepārprotama, būtu skaidri apstiprināt piekrišanu rakstiskā paziņojumā. Pirms Regulas stāšanās spēkā Fizisko personu datu apstrādes likums sensitīvo datu apstrādei noteica tikai rakstveida piekrišanu[32], tomēr Regulas kontekstā, tas nav vienīgais veids, kā iegūt nepārprotamu piekrišanu. Teorētiski arī mutisks paziņojums var būt pietiekami skaidra, nepārprotama piekrišana, tomēr pārzinim var būt grūti pierādīt, ka ir izpildīti visi nosacījumi spēkā esošai, nepārprotamai piekrišanai. Ja apstrāde pamatojas uz datu subjekta piekrišanu, pārzinim būtu jāspēj uzskatāmi parādīt, ka datu subjekts ir devis piekrišanu apstrādes darbībai[33]. Regulā nav precīzi noteikts, kā tas darāms. Izvērtējot Regulas 7. panta 1. punktu, var šķist, ka pārzinim pietiek ar to, ka viņš spēj uzskatāmi pierādīt, ka datu subjekts ir piekritis savu personas datu apstrādei, tādējādi, brīvas,

apzinātas un viennozīmīgas piekrišanas kritēriji netiek papildus vērtēti un pierādīšanas pienākumam šajā gadījumā būtu vairāk deklaratīvs raksturs[34].

Vērtējot Pierādīšanas prezumpciju kopsakarā ar Regulas 43. apsvērumu un 17. panta 3. punkta b) un e) apakšpunktu, pastāv pienākums pierādīt piekrišanu, lai izpildītu saistības vai īstenotu vai aizstāvētu juridiskās tiesības. Tas nozīmē, ka pārzinim jābūt pietiekami daudz datu, lai parādītu saikni ar apstrādi (lai parādītu piekrišanas saņemšanu), bet tiem nevajadzētu vākt vairāk informācijas nekā nepieciešams[35]. Tādējādi, pārzinim ir jāpierāda, ka no datu subjekta ir saņemta spēkā esoša piekrišana un pierādīšanas pienākumam šajā gadījumā nav deklaratīvs raksturs, jo ikvienam pārzinim, kurš apgalvo, ka datu subjekts ir piekritis, tas ir skaidri jāpierāda[36]. Vērtējot pierādīšanas pienākumu, var atzīmēt, ka Regulas piekrišanas definīcijā nav konkrēti noteikts, ka piekrišana ir jāsniedz pirms apstrādes darbības, taču, vērtējot likumīgas datu apstrādes priekšnosacījumus attiecībā uz datu subjekta piekrišanu, ir lietots formulējums "ir devis"[37], no kā loģiski izriet, ka pirms datu apstrādes uzsākšanas ir jābūt spēkā esošam likumīgajam pamatam, tādējādi, piekrišana jādod pirms apstrādes darbības uzsākšanas.

Secinājumi un priekšlikumi

Lai datu subjekta piekrišana būtu spēkā esoša un būtu pietiekams pamats personas datu apstrādes veikšanai, Regula iezīmē vairākus nosacījumus un ierobežojumus, kas jāievēro datu pārzinim, veicot personu datu apstrādi.

Piekrišanai jābūt brīvi sniegtai, paredzot datu subjekta reālo izvēli un kontroli pār saviem datiem. Piekrišana, kas tiek ietverta neapstrīdamos nosacījumos vai datu subjekts nevar atteikties vai atsaukt savu izvēli bez nelabvēlīgām sekām, netiek uzskatīta par brīvi sniegtu. Ja ir skaidras pazīmes par nevienlīdzību datu subjekta un pārziņa attiecībās, datu apstrādei piekrišanas vietā atbilstošāk būtu izvēlēties citu tiesisko pamatu. Ja nav cita tiesiska pamata datu apstrādei, datu apstrāde jāpārtrauc. Novērtējot, vai piekrišana dota brīvi, maksimāli ievēro to, vai līguma izpilde ir atkarīga no piekrišanas tādai personas datu apstrādei, kura nav nepieciešama minētā līguma izpildei. Savukārt, ja apstrāde ir nepieciešama līguma izpildei, tad datu apstrādi nepiemēro uz piekrišanas pamata.

Pārzinim, kurš vēlas saņemt piekrišanu dažādiem nolūkiem,

jānodrošina atsevišķa izvēle katram nolūkam, lai lietotājs var sniegt konkrētu piekrišanu konkrētam nolūkam.

Lai datu subjekts izdarītu patiesu izvēli piekrišanas kontekstā prevalē pārredzamības pamatprincips, proti, prasība pārzinim apstrādāt personas datus tikai tad, ja viņi ir informējuši datu subjektu par viņa tiesībām un viņam pieejamo informāciju. Piekrišanas mehānismiem jābūt detalizētiem un visos gadījumos jānodrošina, ka tiek izmantota skaidra un vienkārša valoda, ka arī izvērtēta mērķauditorija, kuras dati tiks apstrādāti. Ja piekrišanu pieprasa līguma (papīra formātā) vai elektroniskā formā, piekrišanas pieprasījumam jābūt atsevišķam un atšķirīgam. Visos gadījumos, kad apstrāde pamatojas uz datu subjekta piekrišanu, pārzinim jāspēj uzskatāmi parādīt un pierādīt, ka no datu subjekta ir saņemta spēkā esoša piekrišana, taču ievērojot datu minimizēšanas principu, neievācot vairāk informācijas nekā nepieciešams.

Ar Regulas stāšanos spēkā pārziņiem būtu rūpīgi jāpārskata pašreizējie datu apstrādes procesi, jo praksē Regula ievieš augstāku standartu attiecībā uz piekrišanas mehānismu ieviešanu un nosaka vairākas jaunas prasības. Pārziņiem jāatceras, ka personas datu aizsardzības principi vienmēr ir pārāki par pārziņa ekonomiskajām interesēm, ja vien piekļuve šai informācijai ir nepieciešama saskaņā ar likumiskām sabiedrības interesēm[38].

Atsauces

1 Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula), Eiropas Savienības Oficiālais Vēstnesis, L 119/1, 04.05.2016., 33. apsvērums.

2 29. panta datu aizsardzības darba grupas viedoklis 15/2011, 13.07.2011. Pieejams: https://www.pdpjournals.com/docs/88081.pdf., 34.-35. lpp., (skatīts 22.10.2018).

3 Fizisko personu datu aizsardzības likuma 6. pants (zaudējis spēku). 05.07.2018) Pieejams: https://likumi.lv/doc.php?id=4042

4 Regulas (ES) 2016/679 42. apsvērums.

5 Regulas (ES) 2016/679 43. apsvērums un 7. panta 4. punkts.

6 Regulas (ES) 2016/679 7. panta 3. punkts.

7 Regulas (ES) 2016/679 7. panta trešā daļa.

8 29. panta datu aizsardzības darba grupas viedoklis 2/2017, 23.06.2017. Pieejams: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169 (skatīts 22.10.2018).Pieejams: http://ec.europa.eu/newsroom/

article29/item-detail.cfm?item_id=610169 (skatīts 22.10.2018).

[9] 29. panta datu aizsardzības darba grupas viedoklis 8/2001,16.12.2001. Pieejams: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=629492 (skatīts 24.10.2018).

[10] Regulas (ES) 2016/679 43. apsvērums.

[11] Regulas (ES) 2016/679 19. apsvērums.

[12] "Personu datu apstrādes tiesībaizsardzības iestādēs likums" izstrādes procesā (redakcija uz 2017. gada 27. septembri). Pieejams: https://www.tm.gov.lv/lv/cits/pazinojums-par-lidzdalibas-iespejam-likumprojekta-personu-datu-apstrades-tiesibaizsardzibas-iestades (skatīts 22.10.2018).

[13] Regulas (ES) 2016/679 7. panta 4. punkts.

[14] 29. panta datu aizsardzības darba grupas viedoklis 6/2014, 09.04.2014. Pieejams: http://www.dataprotection.ro/servlet/ViewDocument?id=1086, 16.-17. lpp., (skatīts 25.10.2018).

[15] Regulas (ES) 2016/679 32. apsvērums.

[16] 29. panta datu aizsardzības darba grupas viedoklis 15/2011, 13.07.2011. Pieejams: https://www.pdpjournals.com/docs/88081.pdf, 17. lpp. (skatīts 25.10.2018).

[17] Regulas (ES) 2016/679 5. panta 1. punkta a) daļa.

[18] Regulas (ES) 2016/679 39. apsvērums.

[19] Regulas (ES) 2016/679 42. apsvērums.

[20] Regulas (ES) 2016/679 32. apsvērums un 7. panta 2. punkts.

[21] 29. panta datu aizsardzības darba grupas viedoklis 15/2011, 13.07.2011. Pieejams: https://www.pdpjournals.com/docs/88081.pdf, 20. lpp. (skatīts 25.10.2018).

[22] Regulas (ES) 2016/679 58. apsvērums.

[23] 29. panta datu aizsardzības darba grupas viedoklis 15/2011, 13.07.2011. Pieejams: https://www.pdpjournals.com/docs/88081.pdf, 20. lpp. (skatīts 25.10.2018).

[24] Eiropas Savienības Tiesas Lielās Palātas 05.10.2004. spriedums lietā Nr.C 397/01 – C 403/01 Bernhard Pfeiffer u.c. pret Deutsches Rotes Kreuz, Kreisverband Waldshut eV. Pieejams: https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:62001CJ0397 (skatīts 25.10.2018).

[25] Regulas (ES) 2016/679 32, 42. apsvērums.

[26] Regulas (ES) 2016/679 32. apsvērums.

[27] Regulas (ES) 2016/679 9. panta 2. punkts, a) apakšpunkts.

[28] Regula (ES) 2016/679 7. panta 2. punkts.

[29] Eiropas Parlamenta un Padomes Direktīva 95/46/EK, 24.10.1995, "Par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti" 2. pants, h) daļa. Pieejams: https://eur-lex.europa.eu/eli/dir/1995/46/oj/?locale=LV

[30] Eiropas komisijas priekšlikums Eiropas Parlamenta un Padomes regulai par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti, 25.01.2012., 3.4. punkts. Pieejams: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A52012PC0011.

[31] Eiropas komisijas priekšlikums Eiropas Parlamenta un Padomes regulai par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu

brīvu apriti, 15.12.2015. Pieejams: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf, 7. punkts.

[32] Fizisko personu datu aizsardzības likums 11. pants, 1) apakšpunkts.

[33] Regulas (ES) 2016/679 42. apsvērums, ka arī 7. pants, 1. punkts.

[34] Eiropas komisijas tiesas spriedums lietā Nr. C 54/07 Firma Feryn NV pret Eiropas Kopienu Komisiju „Direktīva 2000/43/EK – Diskriminējoši personāla atlases kritēriji – Pierādīšanas pienākums – Sankcijas". Pieejams: http://curia.europa.eu/juris/document/document_print.jsf;jsessionid=9ea7d2dc30dbabf76c1db5af42e5abfaec19ae54bf89.

[35] Regulas (ES) 2016/679 5. panta 1. punkta c) apakšnodaļa.

[36] Eiropas kopienas tiesas spriedums SpA Eiropas Kopienu Komisija pret Anic Partecipazioni, 08.07.1999, Pieejams: https://eur-lex.europa.eu/legal-content/LV/ALL/?uri=CELEX:61992CJ0049, 95., 96. punkti.

[37] Regulas (ES) 2016/679 6. panta 1. punkta a) apakšpunkts.

[38] Eiropas Savienības Tiesas Lielās Palātas 13.05.2014 spriedums Nr. C-131/12 Spānijas personas datu aizsardzības institūcijas pret Google. Pieejams: http://curia.europa.eu/juris/document/document.

Аннотация

В мае 2018 года вступили в силу обновлённые правила обработки персональных данных, установленные Общим регламентом по защите данных (Регламент ЕС 2016/679 от 27 апреля 2016 г.). Новый регламент GDPR (GDPR – General Data Protection Regulation) устанавливает высокие требования в отношении формы получения согласия на обработку данных. Основной проблемой в области обработки данных на основании согласия субъекта является сложная формулировка законодателя, так как основополагающие принципы применения согласия субъекта остались практически неизменными, а форма их реализации и границы применения существенно изменились, что делает этот способ правовой обработки данных одним из сложных на данный момент. В данной статье дан анализ юридической формы согласия субъекта с основополагающими принципами обработки данных на основании последних исследований рабочей группы, которая разрабатывала вышеупомянутый регламент.

Также проанализированы возможные недостатки в работе оператора данных и изучены необходимые условия и предпосылки в отношении соблюдения прав субъекта данных. Согласие субъекта на обработку его персональных данных может выражаться в разной форме, но презумпция доказывания

наличия такого согласия, а также отнесение обрабатываемых общедоступных персональных данных к соответствующей категории возлагаются на оператора. Отдельно в статье анализируется целевой характер, а именно, что цели обработки персональных данных должны соответствовать целям их сбора, полномочиям оператора, объему обрабатываемых персональных данных, рассматривается принцип запрещения объединения разных целей обработки данных, несовместимые цели и т. д.

Ввиду того, что институт согласия субъекта на обработку данных только формируется и какая-либо судебная практика, основанная на новых положениях, еще отсутствует, данная тема очень актуальна как для любого субъекта данных, так и для операторов, обрабатывающих или собирающихся обрабатывать данные субъекта, полагаясь на его согласие.