16/LV
***WP* 242 rev. 01**

Pamatnostādnes par tiesībām uz datu pārnesamību

Pieņemtas 2016. gada 13. decembrī
Pēdējo reizi pārskatītas un pieņemtas 2017. gada 5. aprīlī

Šī Darba grupa tika izveidota saskaņā ar Direktīvas 95/46/EK 29. pantu. Tā ir neatkarīga Eiropas padomdevēja institūcija datu aizsardzības un privātās dzīves neaizskaramības 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 tiesiskums), B-1049 Brisele, Beļģija, birojs Nr. MO59 05/35.

Tīmekļa vietne: http://ec.europa.eu/justice/data-protection/index_en.htm

SATURS

Kopsavilkums

Ar VDAR 20. pantu rada jaunas tiesības uz datu pārnesamību, kas ir cieši saistītas ar piekļuves tiesībām, bet daudzējādā ziņā no tām atšķiras. Šīs tiesības ļauj datu subjektiem strukturētā, plaši izmantotā un mašīnlasāmā formātā saņemt personas datus, ko šie subjekti ir snieguši datu pārzinim, un nosūtīt minētos datus citam pārzinim. Šo jauno tiesību mērķis ir paplašināt datu subjekta iespējas un nodrošināt tam lielāku kontroli pār saviem personas datiem.

Tā kā saskaņā ar šīm tiesībām personas datus ir atļauts tieši nosūtīt no viena datu pārziņa citam pārzinim, datu pārnesamība ir arī svarīgs rīks, kas atbalstīs personas datu brīvu plūsmu ES un veicinās konkurenci starp pārziņiem. Tas atvieglos pāreju no viena pakalpojumu sniedzēja pie cita un tādējādi sekmēs jaunu pakalpojumu attīstību digitālā vienotā tirgus stratēģijas kontekstā.

Šajā atzinumā sniegtas norādes par to, kā interpretēt un īstenot tiesības uz datu pārnesamību, kas ieviestas ar VDAR. Atzinuma mērķis ir apspriest tiesības uz datu pārnesamību un to darbības jomu. Tajā precizēti nosacījumi, saskaņā ar kuriem ir piemērojamas šīs jaunās tiesības, ņemot vērā datu apstrādes juridisko pamatu (datu subjekta piekrišanu vai nepieciešamību izpildīt līgumu), un tas, ka šīs tiesības attiecas vienīgi uz personas datiem, ko sniedz datu subjekts. Lai paskaidrotu apstākļus, kādos šīs tiesības ir piemērojamas, atzinumā minēti arī konkrēti piemēri un kritēriji. Šajā sakarā 29. panta Darba grupa uzskata, ka tiesības uz datu pārnesamību attiecas uz datiem, ko apzināti un aktīvi sniedz datu subjekts. Šīs jaunās tiesības nevar apgrūtināt un ierobežot, attiecinot tās vienīgi uz personisku informāciju, ko tieši paziņo datu subjekts, piemēram, tiešsaistes veidlapā.

Īstenojot labu praksi, datu pārziņiem būtu jāsāk izstrādāt līdzekļus, kas sekmēs datu pārnesamības pieprasījumu izpildi, piemēram, datu lejupielādes rīkus un lietojumprogrammu saskarnes. Pārziņiem jānodrošina, ka personas dati tiek nosūtīti strukturētā, plaši izmantotā un mašīnlasāmā formātā, un viņi būtu jāmudina nodrošināt datu pārnesamības pieprasījumā izmantotā datu formāta sadarbspēju.

Atzinums arī palīdz datu pārziņiem skaidri saprast savus attiecīgos pienākumus, un tajā ir ieteikta paraugprakse un rīki, kas sekmē tiesību uz datu pārnesamību ievērošanu. Visbeidzot, atzinumā ieteikts nozares ieinteresētajām personām un arodasociācijām sadarboties un kopīgi strādāt, lai izveidotu savstarpēji izmantojamu standartu un formātu kopumu un izpildītu prasības, ko izvirza tiesības uz datu pārnesamību.

I. Ievads

Ar Vispārīgās datu aizsardzības regulas (VDAR) 20. pantu ievieš jaunas tiesības uz datu pārnesamību. Šīs tiesības ļauj datu subjektiem strukturētā, plaši izmantotā un mašīnlasāmā formātā saņemt personas datus, ko šie subjekti snieguši datu pārzinim, un bez šķēršļiem nosūtīt minētos datus citam datu pārzinim. Šīs tiesības, ko piemēro saskaņā ar konkrētiem nosacījumiem, atbalsta lietotāja izvēli, lietotāja kontroli un iespēju radīšanu lietotājam.

Personas, kas, sniedzot pieprasīto informāciju, izmantoja savas piekļuves tiesības, kuras paredzētas Datu aizsardzības direktīvā 95/46/EK, ierobežoja datu pārziņa izvēlētais formāts. **Jauno tiesību uz datu pārnesamību mērķis ir paplašināt datu subjektu iespējas attiecībā**

uz viņu personas datiem, jo tās veicina viņu spēju viegli pārvietot, kopēt un nosūtīt personas datus no vienas IT vides uz citu (neatkarīgi no tā, vai tās ir viņu pašu, uzticamu trešo personu vai jaunu datu pārziņu sistēmas).

Apstiprinot indivīdu privātās tiesības un kontroli pār viņu personas datiem, datu pārnesamība piedāvā arī iespēju "līdzsvarot" attiecības starp datu subjektiem un datu pārziņiem[1].

Lai gan tiesības uz personas datu pārnesamību var arī veicināt konkurenci starp pakalpojumiem (atvieglojot pāreju uz citu pakalpojumu), VDAR reglamentē personas datus, nevis konkurenci. Konkrēti, 20. pants nenosaka, ka pārnesamie dati var būt vienīgi dati, kas ir vajadzīgi vai noderīgi pārejai uz citu pakalpojumu[2].

Lai gan datu pārnesamība ir jaunas tiesības, citās tiesību aktu jomās jau pastāv vai tiek apspriesti citi pārnesamības veidi (piemēram, saistībā ar līgumu izbeigšanu, sakaru pakalpojumu viesabonēšanu un pārrobežu piekļuvi pakalpojumiem[3]). Lai gan pret analoģijām būtu jāattiecas piesardzīgi, dažādus pārnesamības veidus apvienojot kombinētā pieejā, starp tiem var rasties zināmas sinerģijas un pat priekšrocības indivīdiem.

Šajā atzinumā sniegtas norādes datu pārziņiem, lai tie varētu atjaunināt savu praksi, procesus un politikas virzienus, un precizēta termina "datu pārnesamība" nozīme, lai datu subjekti varētu efektīvi īstenot savas jaunās tiesības.

II. Kādi ir datu pārnesamības galvenie elementi?

Tiesības uz datu pārnesamību VDAR 20. panta 1. punktā definētas šādi.

> *Datu subjektam ir tiesības saņemt personas datus attiecībā uz sevi, kurus viņš sniedzis pārzinim, strukturētā, plaši izmantotā un mašīnlasāmā formātā, un ir tiesības minētos datus nosūtīt citam pārzinim, un pārzinis, kuram attiecīgie personas dati sniegti, tam nerada nekādus šķēršļus [..]*

- Tiesības saņemt personas datus

Pirmkārt, datu pārnesamība ir datu subjekta tiesības saņemt to personas datu apakškopu, kurus attiecībā uz viņu apstrādā datu pārzinis, un uzglabāt minētos datus turpmākai personīgai izmantošanai. Šādu glabāšanu var veikt uz privātas ierīces vai privātā mākonī, obligāti nenosūtot šos datus citam datu pārzinim.

Šajā ziņā datu pārnesamība papildina piekļuves tiesības. Datu pārnesamības īpaša iezīme ir tāda, ka tā piedāvā iespēju datu subjektiem pašiem pārvaldīt un atkalizmantot savus personas datus. Personas dati būtu jāsaņem "*strukturētā, plaši izmantotā un mašīnlasāmā formātā*". Piemēram, datu subjekts varētu būt ieinteresēts izgūt no mūzikas straumēšanas pakalpojuma

[1] Datu pārnesamības galvenais mērķis ir pastiprināt indivīdu kontroli pār saviem personas datiem un nodrošināt tiem aktīvu lomu datu ekosistēmā.
[2] Piemēram, šīs tiesības var atļaut bankām lietotāja uzraudzībā sniegt papildu pakalpojumus, izmantojot personas datus, kas sākotnēji tika vākti energoapgādes pakalpojuma ietvaros.
[3] Sk. Eiropas Komisijas digitālā vienotā tirgus programmu https://ec.europa.eu/digital-agenda/en/digital-single-market, īpaši pirmo politikas pīlāru "Labāka tiešsaistes piekļuve digitālām precēm un pakalpojumiem".

savu pašreizējo atskaņošanas sarakstu (vai klausīto dziesmu vēsturi), lai uzzinātu, cik reizes viņš klausījies konkrētas dziesmas, vai arī lai pārbaudītu, kādus mūzikas ierakstus viņš vēlas nopirkt vai klausīties citā platformā. Tāpat arī viņš var vēlēties izgūt no tīmekļa pasta lietojumprogrammas savu kontaktu sarakstu, lai, piemēram, sagatavotu kāzu dāvanu sarakstu vai saņemtu informāciju par pirkumiem, kas veikti, izmantojot lojalitātes kartes, vai piekļūt savai oglekļa dioksīda pēdai[4].

- **Tiesības nosūtīt personas datus no viena datu pārziņa citam pārzinim**

Otrkārt, saskaņā ar 20. panta 1. punktu datu subjektiem tiek piešķirtas **tiesības personas datus nosūtīt no viena pārziņa citam pārzinim**, un pārzinis tam "nerada nekādus šķēršļus". Pēc datu subjekta pieprasījuma datus arī var nosūtīt tieši no viena pārziņa citam pārzinim, ja tas ir tehniski iespējams (20. panta 2. punkts). Šajā sakarā 68. apsvērumā datu pārziņi tiek mudināti izstrādāt savstarpēji izmantojamus formātus, kas nodrošina datu pārnešanu[5], tomēr neradot pārziņiem pienākumu ieviest vai uzturēt apstrādes sistēmas, kas ir tehniski saderīgas[6]. VDAR tomēr aizliedz pārziņiem radīt šķēršļus nosūtīšanai.

Būtībā šis datu pārnesamības elements sniedz iespēju datu subjektiem ne tikai vienkārši iegūt un atkalizmantot, bet arī nosūtīt datus, ko tie snieguši citam pakalpojumu sniedzējam (vai nu tās pašas, vai citas darījumdarbības nozares ietvaros). Papildus patērētāju iespēju nodrošināšanai, ko sniedz piesaistes novēršana vienam pakalpojumu sniedzējam, paredzams, ka tiesības uz datu pārnesamību sekmēs inovācijas iespējas un personas datu drošu un neapdraudētu apmaiņu starp datu pārziņiem datu subjekta uzraudzībā[7]. Datu pārnesamība var veicināt kontrolētu un ierobežotu personas datu apmaiņu starp organizācijām, ko veic lietotāji, tādējādi bagātinot pakalpojumus un klientu pieredzi[8]. Datu pārnesamība var sekmēt personas datu par lietotājiem nosūtīšanu un atkalizmantošanu starp dažādajiem pakalpojumiem, kas interesē lietotājus.

[4] Šādos gadījumos uz datu apstrādi, ko par datu subjektu veic datu subjekts, var attiekties mājsaimniecisku pasākumu darbības joma, kad visu apstrādi veic datu subjekta vienpersoniskā uzraudzībā, vai arī datu subjekta vārdā to var veikt cita persona. Pēdējā minētajā gadījumā šī cita persona būtu uzskatāma par datu pārzini kaut vai tikai personas datu uzglabāšanas nolūkā, un tai ir jāievēro VDAR noteiktie principi un pienākumi.

[5] Sk. arī V iedaļu

[6] Tādējādi īpaša uzmanība būtu jāpievērš nosūtīto datu formātam, lai nodrošinātu, ka, pieliekot nelielas pūles, datus var atkalizmantot datu subjekts vai cits datu pārzinis. Sk. arī V iedaļu.

[7] Sk. vairākas eksperimentālas lietojumprogrammas Eiropā, piemēram, MiData Apvienotajā Karalistē, *FING* izstrādāto MesInfos / SelfData Francijā.

[8] Tā dēvētās pašmērīšanas un *IoT* nozares ir parādījušas priekšrocības (un riskus), ko sniedz tādu personas datu sasaistīšana, kas iegūti no indivīda dzīves dažādiem aspektiem, tādiem kā veselība, aktivitāte un kaloriju uzņemšana, lai vienā datnē gūtu pilnīgāku ainu par personas dzīvi.

- **Kontrole**

Datu pārnesamība garantē tiesības saņemt personas datus un tos apstrādāt atbilstoši datu subjekta vēlmēm[9].

Datu pārziņi, kas atbild uz datu pārnesamības pieprasījumiem, saskaņā ar 20. pantā paredzētajiem nosacījumiem nav atbildīgi par apstrādi, ko veic datu subjekts vai cits uzņēmums, kas saņem personas datus. Viņi rīkojas datu subjekta vārdā, tostarp arī tad, ja personas datus tieši nosūta citam datu pārzinim. Šajā sakarā datu pārzinis nav atbildīgs par to, vai saņēmējs datu pārzinis ievēro datu aizsardzības tiesību aktus, jo sūtītājs datu pārzinis saņēmēju neizvēlas. Tai pat laikā pārzinim būtu jāsniedz garantijas, lai nodrošinātu, ka viņš patiesi rīkojas datu subjekta interesēs. Piemēram, pārziņi varētu izveidot procedūras, lai nodrošinātu, ka nosūtīto personas datu veids patiesi ir tāds, kādu datu subjekts vēlas nosūtīt. To varētu izdarīt, vai nu saņemot datu subjekta apstiprinājumu pirms nosūtīšanas, vai arī agrāk, kad tiek sniegta sākotnējā piekrišana apstrādei vai pabeigta līguma izstrāde.

Datu pārzinim, kas atbild uz datu pārnesamības pieprasījumu, nav īpaša pienākuma pirms nosūtīšanas pārbaudīt datu kvalitāti un pārliecināties par to. Šiem datiem, protams, jau vajadzētu būt precīziem un atjauninātiem atbilstoši VDAR 5. panta 1. punktā noteiktajiem principiem. Turklāt datu pārnesamība neuzliek pienākumu datu pārzinim glabāt personas datus ilgāk, nekā tas ir nepieciešams, vai pēc konkrēta glabāšanas termiņa beigām[10]. Svarīgi ir tas, ka nepastāv papildu prasība glabāt datus ilgāk par citādi piemērojamiem glabāšanas laikposmiem, lai vienkārši izpildītu iespējamos turpmākos datu pārnesamības pieprasījumus.

Ja pieprasītos personas datus apstrādā datu apstrādātājs, līgumā, kas noslēgts saskaņā ar VDAR 28. pantu, ir jāiekļauj prasība palīdzēt "pārzinim ar atbilstīgiem tehniskiem un organizatoriskiem pasākumiem [..] atbildēt uz pieprasījumiem par [..] datu subjekta tiesību īstenošanu". Tāpēc, lai atbildētu uz datu pārnesamības pieprasījumiem, datu pārzinim sadarbībā ar datu apstrādātājiem vajadzētu ieviest īpašas procedūras. Kopīgu pārbaudes tiesību gadījumā līgumā jau agrīnā posmā būtu skaidri jānosaka katra datu pārziņa pienākumi attiecībā uz datu pārnesamības pieprasījumiem.

Turklāt saņēmējs datu pārzinis[11] ir atbildīgs par to, lai nodrošinātu, ka sniegtie pārnesamie dati ir atbilstīgi un nav pārmērīgi attiecībā uz jauno datu apstrādi. Piemēram, ja datu pārnesamības pieprasījumu iesniedz tīmekļa e-pasta pakalpojumu sniedzējam un datu subjekts izmanto pieprasījumu, lai saņemtu e-pastus un nosūtītu tos drošai arhīvu platformai, jaunajam datu pārzinim nav jāapstrādā datu subjekta korespondentu kontaktinformācija. Ja šī informācija nav būtiska attiecībā uz jaunās apstrādes mērķi, tā nebūtu jāglabā un jāapstrādā. Jebkurā gadījumā saņēmējiem datu pārziņiem nav pienākuma pieņemt un apstrādāt personas datus, kas nosūtīti pēc datu pārnesamības pieprasījuma saņemšanas. Tāpat arī, ja datu subjekts pieprasa, lai dienestam, kas palīdz pārvaldīt viņa budžetu, tiktu nosūtīta sīka informācija par viņa bankas darījumiem, saņēmējam datu pārzinim nav jāpieņem visi dati, nedz arī jāglabā visa informācija par darījumiem, tiklīdz tā iezīmēta atbilstoši jaunajam pakalpojumam. Citiem

[9] Tiesības uz datu pārnesamību neaprobežojas ar personas datiem, kas ir noderīgi un būtiski līdzīgiem pakalpojumiem, ko sniedz datu pārziņa konkurenti.

[10] Ja iepriekšminētajā piemērā datu pārzinis nesaglabā ierakstu par dziesmām, ko atskaņojis lietotājs, šos personas datus nevar iekļaut datu pārnesamības pieprasījumā.

[11] Proti, pārzinis, kas saņem personas datus pēc tam, kad datu subjekts iesniedzis datu pārnesamības pieprasījumu citam datu pārzinim.

vārdiem, datiem, ko pieņem un uzglabā, vajadzētu būt vienīgi tādiem, kas ir vajadzīgi un būtiski tā pakalpojuma sniegšanai, ko nodrošina saņēmējs datu pārzinis.

Attiecībā uz personas datiem "saņēmēja" organizācija kļūst par datu jauno pārzini, un tai ir jāievēro VDAR 5. pantā noteiktie principi. Tāpēc "jaunajam" saņēmējam datu pārzinim pirms jebkura pārnesamo datu nosūtīšanas pieprasījuma ir skaidri un tieši jānorāda jaunās apstrādes mērķis atbilstoši 14. pantā izklāstītajām pārredzamības prasībām[12]. Attiecībā uz citu datu apstrādi, ko veic tā uzraudzībā, datu pārzinim būtu jāpiemēro 5. pantā noteiktie principi, tādi kā likumīgums, godprātība un pārredzamība, nolūka ierobežojumi, datu minimizēšana, precizitāte, integritāte un konfidencialitāte, glabāšanas ierobežojums un pārskatatbildība[13].

Datu pārziņiem, kas tur personas datus, vajadzētu būt gataviem veicināt sava datu subjekta tiesības uz datu pārnesamību. Datu pārziņi var arī izvēlēties pieņemt datus no datu subjekta, bet viņiem nav pienākuma to darīt.

- **Datu pārnesamība attiecībā pret datu subjektu citām tiesībām**

Kad persona īsteno savas tiesības uz datu pārnesamību, šī persona to dara, neskarot citas tiesības (kā tas ir gadījumā ar citām tiesībām, kas minētas VDAR). Datu subjekts var turpināt izmantot datu pārziņa pakalpojumu un gūt no tā labumu pat pēc datu pārnesamības darbības veikšanas. Datu pārnesamība automātiski neizraisa to dzēšanu[14] datu pārziņa sistēmās un neskar glabāšanas sākotnējo termiņu, ko piemēro nosūtītajiem datiem. Datu subjekts var īstenot savas tiesības, kamēr vien datu pārzinis apstrādā datus.

Tāpat arī, ja datu subjekts vēlas īstenot savas tiesības uz dzēšanu (tiesības "tikt aizmirstam", kas noteiktas 17. pantā), datu pārzinis nevar izmantot datu pārnesamību, lai kavētos vai atteiktos tos dzēst.

Ja datu subjekts atklāj, ka personas datos, kas pieprasīti saskaņā ar tiesībām uz datu pārnesamību, datu subjekta pieprasījums nav izpildīts pilnībā, atbilstoši VDAR 15. pantam tas būtu jāizpilda pilnībā turpmākajos personas datu pieprasījumos, ko iesniedz saskaņā ar tiesībām uz piekļuvi.

Turklāt tad, ja konkrētā Eiropas vai dalībvalsts citas jomas tiesību aktā ir noteikts kāds no attiecīgo datu pārnesamības veidiem, izpildot datu pārnesamības pieprasījumu saskaņā ar VDAR, ir jāņem vērā arī šajos konkrētajos tiesību aktos paredzētie noteikumi. Pirmkārt, ja no datu subjekta pieprasījuma skaidri izriet, ka viņa nodoms ir īstenot savas nevis VDAR, bet gan vienīgi nozares tiesību aktos paredzētās tiesības, VDAR datu pārnesamības noteikumus viņa pieprasījumam nepiemēro[15]. No otras puses, ja pieprasījuma mērķis ir VDAR paredzētā pārnesamība, minēto konkrēto tiesību aktu pastāvēšana nav svarīgāka par datu pārnesamības

[12] Turklāt jaunajam datu pārzinim nevajadzētu apstrādāt datus, kas nav atbilstīgi, un apstrādei jāietver tikai tas, kas nepieciešams jaunajos nolūkos, pat ja šie personas dati ietilpst globālākā datu kopumā, ko nosūta pārnesamības procesā. Personas datus, kas nav nepieciešami, lai sasniegtu jaunās apstrādes mērķi, vajadzētu pēc iespējas ātrāk dzēst.

[13] Tiklīdz datu pārzinis saņēmis personas datus, kas nosūtīti tiesību uz datu pārnesamību ietvaros, var uzskatīt, ka tos ir "sniedzis" datu subjekts, un saskaņā ar tiesībām uz datu pārnesamību tos var nosūtīt atkārtoti, ja tiek izpildīti pārējie nosacījumi, ko piemēro šīm tiesībām (proti, apstrādes juridiskais pamats, ...).

[14] Kā noteikts VDAR 17. pantā.

[15] Piemēram, ja datu subjekta pieprasījuma konkrētais mērķis ir nodrošināt konta informācijas pakalpojumu sniedzējam piekļuvi datu subjekta bankas konta vēsturei Maksājumu pakalpojumu direktīvā 2 (MPD2) paredzētajiem mērķiem, šādu piekļuvi sniedz saskaņā ar minētās direktīvas noteikumiem.

principa vispārēju attiecināšanu uz jebkuru datu pārzini, kā noteikts VDAR. Tā vietā katrā gadījumā atsevišķi ir jāvērtē, kā un vai vispār šie konkrētie tiesību akti var ietekmēt tiesības uz datu pārnesamību.

III. Kad piemēro datu pārnesamību?

- **Uz kādām apstrādes darbībām attiecas tiesības uz datu pārnesamību?**

Lai nodrošinātu atbilstību VDAR, datu pārziņiem ir jābūt skaidram juridiskajam pamatam personas datu apstrādei.

Saskaņā ar VDAR 20. panta 1. punkta a) apakšpunktu, lai uz apstrādes darbībām **attiektos datu pārnesamība**, tām ir jāpamatojas uz:

- datu subjekta piekrišanu (ievērojot 6. panta 1. punkta a) apakšpunktu vai 9. panta 2. punkta a) apakšpunktu attiecībā uz personas datu īpašām kategorijām);

- vai uz līgumu, kura līgumslēdzēja puse ir datu subjekts atbilstoši 6. panta 1. punkta b) apakšpunktam.

Kā piemērus personas datiem, kas parasti ir datu pārnesamības darbības jomā, var minēt to grāmatu nosaukumus, kuras persona iegādājusies tiešsaistes grāmatnīcā, vai dziesmas, kas noklausītas, izmantojot mūzikas straumēšanas pakalpojumu, jo šos datus apstrādā, pamatojoties uz tāda līguma izpildi, kura līgumslēdzēja puse ir datu subjekts.

VDAR nenosaka vispārējas tiesības uz datu pārnesamību gadījumos, kad personas datu apstrāde pamatojas uz piekrišanu vai līgumu[16]. Piemēram, finanšu iestādēm nav pienākuma atbildēt uz datu pārnesamības pieprasījumu attiecībā uz personas datiem, ko apstrādā to pienākumu ietvaros, izpildot pienākumu novērst un atklāt nelikumīgi iegūtu līdzekļu legalizāciju un citus finanšu noziegumus; tāpat arī datu pārnesamība neattiecas uz profesionālo kontaktinformāciju, ko apstrādā uzņēmumu savstarpējās darījumattiecībās gadījumos, kad apstrāde nepamatojas ne uz datu subjekta piekrišanu, ne līgumu, kura līgumslēdzēja puse ir datu subjekts.

Attiecībā uz darbinieku datiem tiesības uz datu pārnesamību parasti piemēro vienīgi tad, ja apstrāde pamatojas uz līgumu, kura līgumslēdzēja puse ir datu subjekts. Šajā kontekstā nelīdzsvarota ietekmes sadalījuma dēļ starp darba devēju un darba ņēmēju daudzos gadījumos netiks uzskatīts, ka piekrišana ir sniegta labprātīgi[17]. Tā vietā cilvēkresursu datu apstrādes

[16] Sk. VDAR 68. apsvērumu un 20. panta 3. punktu. VDAR 68. apsvērumā un 20. panta 3. punktā noteikts, ka datu pārnesamība neattiecas uz apstrādi gadījumos, kad tā ir vajadzīga, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot datu pārzinim piešķirtas oficiālas pilnvaras, vai kad datu pārzinis pilda sabiedrisku vai juridisku pienākumu. Tāpēc šādos gadījumos datu pārziņiem nav pienākuma nodrošināt pārnesamību. Tomēr laba prakse ir izstrādāt procesus, lai varētu automātiski atbildēt uz pārnesamības pieprasījumiem, ievērojot principus, kas reglamentē tiesības uz datu pārnesamību. Piemērs varētu būt valsts pakalpojums, ar kura palīdzību var viegli lejupielādēt iepriekšējos paziņojumus par iedzīvotāju ienākuma nodokli. Kā datu pārnesamības labas prakses piemēru tādas apstrādes gadījumā, kuras juridiskais pamats ir nepieciešamība leģitīmās interesēs un esošo brīvprātīgo shēmu vajadzībām, sk. 29. panta Darba grupas Atzinuma Nr. 6/2014 par pārziņa leģitīmajām interesēm (*WP* 217) 47. un 48. lpp.

[17] Kā norādīja 29. panta Darba grupa savā 2001. gada 13. septembra Atzinumā Nr. 8/2001 (*WP* 48).

juridiskais pamats dažkārt ir leģitīmas intereses vai nepieciešamība pildīt konkrētus juridiskus pienākumus nodarbinātības jomā. Praksē tiesības uz datu pārnesamību cilvēkresursu kontekstā neapšaubāmi attieksies uz dažām apstrādes darbībām (tādām kā darba samaksas un kompensācijas pakalpojumi, iekšējā darbā pieņemšana), bet daudzās citās situācijās būs vajadzīga katram atsevišķam gadījumam piemērota pieeja, lai pārbaudītu, vai ir izpildīti visi nosacījumi, kas attiecas uz tiesībām uz datu pārnesamību.

Visbeidzot, tiesības uz datu pārnesamību piemēro tad, ja datu apstrādi "veic ar automatizētiem līdzekļiem", tāpēc tās neattiecas uz lielāko daļu lietu papīra formātā.

- **Kādi personas dati ir jāiekļauj?**

Saskaņā ar 20. panta 1. punktu, lai uz datiem attiektos tiesības uz datu pārnesamību, tiem ir jābūt:

- personas datiem, kas attiecas uz datu subjektu un
- kurus viņš *sniedzis* datu pārzinim.

VDAR 20. panta 4. punktā arī noteikts, ka šīs tiesības nelabvēlīgi neietekmē citu personu tiesības un brīvības.

Pirmais nosacījums: personas dati, kas attiecas uz datu subjektu

Datu pārnesamības pieprasījuma darbības jomā ir vienīgi personas dati. Tāpēc jebkuri dati, kas ir anonīmi[18] vai neattiecas uz datu subjektu, nebūs tā darbības jomā. Tomēr pieprasījuma darbības jomā ir pseidoanonīmi dati, kas skaidri sasaistāmi ar datu subjektu (piemēram, ja viņš ir norādījis attiecīgo identifikatoru, sal. ar 11. panta 2. punktu).

Daudzās situācijās datu pārziņi apstrādās informāciju, kas satur vairāku datu subjektu personas datus. Šādā gadījumā datu pārziņiem nevajadzētu pārāk ierobežoti interpretēt frāzi "datu subjekta personas dati". Piemēram, telefona sarunu, starppersonu ziņojumapmaiņas vai IP balss pārraides ieraksti var saturēt (abonenta konta vēsturē) informāciju par trešām personām, kas saistītas ar ienākošajiem vai izejošajiem zvaniem. Lai gan tādējādi ieraksti saturēs personas datus par daudziem cilvēkiem, būtu jānodrošina, ka, atbildot uz datu pārnesamības pieprasījumiem, abonenti var saņemt šos ierakstus, jo tie attiecas (arī) uz datu subjektu. Tomēr tad, ja šādus ierakstus pēc tam nosūta jaunam datu pārzinim, šim jaunajam datu pārzinim nevajadzētu tos apstrādāt tādiem mērķiem, kas nelabvēlīgi ietekmē trešo personu tiesības un brīvības (sk. trešo nosacījumu).

Otrais nosacījums: dati, ko sniedz datu subjekts

Otrais nosacījums sašaurina darbības jomu, attiecinot to vienīgi uz datiem, ko "sniedz" datu subjekts.

Ir daudz piemēru saistībā ar personas datiem, ko datu subjekts "sniedz" apzināti un aktīvi, piemēram, konta dati (piem., pasta adrese, lietotāja vārds, vecums), kas iesniegti, izmantojot tiešsaistes veidlapas. Tomēr dati, ko "sniedz" datu subjekts, tiek iegūti, arī novērojot viņa darbības. Tāpēc 29. panta Darba grupa uzskata, ka, lai nodrošinātu šo jauno tiesību pilnu

[18] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

vērtību, vārdā "sniedz" būtu jāietver arī personas dati, ko novēro, lietotājiem veicot tādas darbības kā neapstrādātu datu apstrāde, izmantojot viedo mērierīci vai tīklam pieslēgtu objektu citus veidus[19], darbību žurnālus, tīmekļa vietnes lietošanas vēsturi vai meklēšanas darbības.

Pēdējā minētā datu kategorija neietver datus, ko radījis datu pārzinis (izmantojot novērotos datus vai datus, kas tieši sniegti kā izejas dati), piemēram, lietotāja profilu, kas izveidots, analizējot savāktos neapstrādātos viedo mērījumu datus.

Lai noteiktu, vai uz datiem attiecas tiesības uz datu pārnesamību, atkarībā no to izcelsmes var nošķirt dažādas datu kategorijas. Par datiem, ko "sniedz datu subjekts", var uzskatīt turpmāk minētās kategorijas:

- **dati, ko aktīvi un apzināti sniedz datu subjekts** (piemēram, pasta adrese, lietotāja vārds, vecums utt.);
- **novērotie dati, ko sniedz datu subjekts, izmantojot pakalpojumu vai ierīci.** Tie, piemēram, var ietvert personas veiktās meklēšanas vēsturi, informāciju par datu plūsmu un atrašanās vietas datus. Tie var ietvert arī citus neapstrādātus datus, piemēram, sirdspukstus, ko izsekojusi valkājamierīce.

Turpretī izrietošos un iegūtos datus rada datu pārzinis, pamatojoties uz datiem, ko "sniedz datu subjekts". Piemēram, lietotāja veselības stāvokļa novērtējuma rezultātus vai profilu, kas izveidots riska pārvaldības un finanšu noteikumu kontekstā (piem., lai piešķirtu kredītspējas novērtējumu vai nodrošinātu nelikumīgi iegūtu līdzekļu legalizācijas novēršanas noteikumu ievērošanu), kā tādu nevar uzskatīt par datiem, ko "sniedz" datu subjekts. Lai gan šādi dati var būt daļa no profila, ko uztur datu pārzinis, un izriet vai ir iegūti, analizējot datus, ko sniedz datu subjekts (piemēram, veicot darbības), parasti šie dati netiks uzskatīti par tādiem, ko "sniedz datu subjekts", un tādējādi nebūs šo jauno tiesību darbības jomā[20].

Kopumā, ņemot vērā tiesību uz datu pārnesamību politikas mērķus, termins "sniedz datu subjekts" ir jāinterpretē plaši, un no tā būtu jāizslēdz "izrietošie dati" un "iegūtie dati", kas ietver personas datus, ko rada pakalpojuma sniedzējs (piemēram, algoritmiskos rezultātus). Datu pārzinis var izslēgt minētos izrietošos datus, bet vajadzētu iekļaut visus pārējos personas datus, ko sniedz datu subjekts, izmantojot tehniskos līdzekļus, kurus nodrošina datu pārzinis[21].

Tādējādi termins "sniedz" ietver personas datus, kas ir saistīti ar datu subjekta darbībām vai izriet no personas uzvedības novērošanas, bet neietver datus, ko iegūst, pēc tam analizējot minēto uzvedību. Turpretī jebkuri personas dati, ko rada datu pārzinis, veicot datu apstrādi,

[19] Ja datu subjekts varēs izgūt datus, kas iegūti, vērojot viņa darbības, datu subjekts arī varēs gūt labāku ieskatu par īstenošanas izvēlēm, ko veic datu pārzinis attiecībā uz novērotajiem datiem, un varēs labāk izvēlēties, kādus datus viņš ir gatavs sniegt, lai saņemtu līdzīgu pakalpojumu, un būs informēts par to, kādā mērā tiek ievērotas viņa tiesības uz privātumu.

[20] Tomēr saskaņā ar VDAR 15. pantu (kurā sniegta atsauce uz piekļuves tiesībām) datu subjekts joprojām var izmantot savas "tiesības saņemt no pārziņa apstiprinājumu par to, vai attiecībā uz datu subjektu tiek vai netiek apstrādāti personas dati, un, ja tiek, datu subjektam ir tiesības piekļūt attiecīgajiem datiem", kā arī saņemt informāciju par to, "ka pastāv automatizēta lēmumu pieņemšana, tostarp profilēšana, kas minēta 22. panta 1. un 4. punktā, un – vismaz minētajos gadījumos – jēgpilna informācija par tajā ietverto loģiku, kā arī šādas apstrādes nozīmīgumu un paredzamajām sekām attiecībā uz datu subjektu".

[21] Tas ietver visus datus, kas novēroti par datu subjektu to darbību laikā, kuru nolūkā datus vāc, piemēram, darījumu vēsturi vai piekļuves žurnālu. Arī datus, kas savākti, izsekojot un izdarot ierakstus par datu subjektu (tādus kā lietotne, kas ieraksta sirdspukstus, vai tehnoloģija, ko izmanto, lai izsekotu pārlūkošanas paradumus), vajadzētu uzskatīt par tādiem, ko viņš "sniedz", pat ja datus nenosūta aktīvi vai apzināti.

piemēram, personalizācijas un ieteikumu procesā vai klasificējot vai profilējot lietotājus, ir dati, kas izriet vai ir iegūti, izmantojot personas datus, ko sniedz datu subjekts, un uz tiem neattiecas tiesības uz datu pārnesamību.

Trešais nosacījums: tiesības uz datu pārnesamību nelabvēlīgi neietekmē citu personu tiesības un brīvības

Attiecībā uz citu datu subjektu personas datiem

Trešais nosacījums ir paredzēts, lai izvairītos no tādu datu izgūšanas un nosūtīšanas jaunam datu pārzinim, kas satur citu datu subjektu (kas nav devuši piekrišanu) personas datus, gadījumos, kad šos datus varētu apstrādāt tā, ka tie nelabvēlīgi ietekmētu citu datu subjektu tiesības un brīvības (VDAR 20. panta 4. punkts)[22].

Šāda nelabvēlīga ietekme rastos, ja, piemēram, datu nosūtīšana no viena datu pārziņa citam pārzinim liegtu trešām personām īstenot to kā datu subjektu tiesības, kas paredzētas VDAR (piemēram, tiesības uz informāciju, piekļuvi utt.).

Datu subjekts, kas ierosina savu datu nosūtīšanu citam datu pārzinim, vai nu dod piekrišanu jaunajam datu pārzinim apstrādāt viņa datus, vai arī noslēdz līgumu ar minēto pārzini. Ja datu kopumā ir iekļauti trešo personu personas dati, apstrādei jānosaka cits juridiskais pamats. Piemēram, datu pārzinis var ievērot 6. panta 1. punkta f) apakšpunktā minētās leģitīmās intereses, ja datu pārziņa mērķis ir sniegt datu subjektam pakalpojumu, kas ļauj viņam apstrādāt datus tikai personiska vai mājsaimnieciska pasākuma gaitā. Datu subjekts ir atbildīgs par apstrādes darbībām, ko viņš ierosina tādas savas darbības kontekstā, kas attiecas uz trešām personām un var tās ietekmēt, ciktāl par minēto apstrādi nekādā veidā nelemj datu pārzinis.

Piemēram, tīmekļa e-pasta pakalpojums var ļaut izveidot datu subjekta kontaktu, draugu, radinieku, ģimenes locekļu un plašākas vides sarakstu. Tā kā šie dati ir saistīti ar identificējamu personu, kas vēlas īstenot savas tiesības uz datu pārnesamību (un ir tos radījusi), datu pārziņiem vajadzētu nosūtīt minētajam datu subjektam visu ienākošo un izejošo e-pastu sarakstu.

Tāpat arī datu subjekta bankas konts var saturēt personas datus, kas attiecas ne tikai uz konta turētāja, bet arī uz citu personu darījumiem (piemēram, ja tās ir pārskaitījušas naudu konta turētājam). Maz ticams, ka pēc tam, kad iesniegts pārnesamības pieprasījums, bankas konta informācijas nosūtīšana konta turētājam varētu nelabvēlīgi ietekmēt minēto trešo personu tiesības un brīvības, ja abos piemēros šo datus izmanto vienam un tam pašam nolūkam (proti, kontaktadresi vai datu subjekta bankas konta vēsturi izmanto vienīgi datu subjekts).

Turpretī trešo personu tiesības un brīvības netiks ievērotas, ja jaunais datu pārzinis izmantos personas datus citiem nolūkiem, piemēram, ja saņēmējs datu pārzinis citu personu personas datus, kas ietverti datu subjekta kontaktu sarakstā, izmantos tirgvedības nolūkiem.

Tāpēc, lai novērstu nelabvēlīgu ietekmi uz iesaistītajām trešām personām, minētos personas datus ir atļauts apstrādāt citam pārzinim vienīgi tiktāl, ciktāl šie dati ir pieprasītāja lietotāja vienpersoniskā uzraudzībā un tos apstrādā tikai personiskām vai mājsaimnieciskām

[22] VDAR 68. apsvērumā ir noteikts, ka "ja konkrēts personas datu kopums attiecas uz vairākiem datu subjektiem, tad tiesībām saņemt personas datus nebūtu jāskar citu datu subjektu tiesības un brīvības saskaņā ar šo regulu."

vajadzībām. "Jaunais" saņēmējs datu pārzinis (kuram var nosūtīt datus pēc lietotāja pieprasījuma) nedrīkst izmantot nosūtītus trešo personu datus savām vajadzībām, piemēram, lai piedāvātu tirgvedības produktus un pakalpojumus minētajiem citiem trešo personu datu subjektiem. Piemēram, šo informāciju nevajadzētu izmantot, lai pilnveidotu trešo personu datu subjekta profilu un bez tā ziņas vai piekrišanas atjaunotu viņa sociālo vidi[23]. Tāpat arī to nevar izmantot, lai izgūtu informāciju par minētajām trešām personām un izstrādātu īpašus profilus, pat ja viņu personas datus jau tur datu pārzinis. Pretējā gadījumā minētā apstrāde varētu būt nelikumīga un negodīga, īpaši ja attiecīgās trešās personas nav informētas un nevar īstenot savas kā datu subjektu tiesības.

Turklāt visu datu pārziņu (gan "sūtītāju", gan "saņēmēju") vadošā prakse ir ieviest rīkus, lai datu subjekti varētu izvēlēties attiecīgos datus, ko viņi vēlas saņemt un nosūtīt, un attiecīgā gadījumā izslēgt citu personu datus. Tas palīdzēs vēl vairāk samazināt to trešo personu riskus, kuru personas dati varētu tikt pārnesti.

Papildus tam datu pārziņiem būtu jāievieš piekrišanas mehānismi attiecībā uz citiem iesaistītajiem datu subjektiem, lai atvieglotu datu nosūtīšanu gadījumos, kad šīs personas ir gatavas dot piekrišanu, piemēram, ja arī tās vēlas pārvietot savus datus kādam citam datu pārzinim. Šāda situācija varētu rasties, piemēram, saistībā ar sociālajiem tīkliem, tomēr lēmums par to, kādu vadošo praksi ievērot, ir jāpieņem datu pārziņiem.

Attiecībā uz datiem, uz kuriem attiecas intelektuālā īpašuma tiesības un tirdzniecības noslēpumi

Citu personu tiesības un brīvības ir minētas 20. panta 4. punktā. Lai gan tās nav tieši saistītas ar pārnesamību, šīs tiesības var saprast kā tādas, kas "ietver tirdzniecības noslēpumus vai intelektuālā īpašuma tiesības jo īpaši autortiesības, ar ko aizsargāta programmatūra". Pat ja šīs tiesības būtu jāapsver, pirms atbildēt uz datu pārnesamības pieprasījumu, tomēr "minēto apsvērumu rezultātam nevajadzētu būt tādam, ka datu subjektam tiek atteikts sniegt jebkādu informāciju". Turklāt datu pārzinim nevajadzētu noraidīt datu pārnesamības pieprasījumu, pamatojoties uz citu līgumtiesību pārkāpumu (piemēram, nesamaksātu parādu vai tirdzniecības konfliktu ar datu subjektu).

Tiesības uz datu pārnesamību nav personas tiesības ļaunprātīgi izmantot informāciju tādā veidā, ko varētu kvalificēt kā negodīgu praksi vai kas būtu intelektuālā īpašuma tiesību pārkāpums.

Iespējams uzņēmējdarbības risks tomēr nevar pats par sevi kalpot par pamatu tam, lai atteiktos atbildēt uz datu pārnesamības pieprasījumu, un personas datus, ko sniedz datu subjekti, datu pārzinis var nosūtīt tādā veidā, ka informācija, uz kuru attiecas tirdzniecības noslēpumi vai intelektuālā īpašuma tiesības, netiek publiskota.

IV. <u>Kā vispārīgos noteikumus, kas reglamentē datu subjektu tiesību īstenošanu, piemēro datu pārnesamībai?</u>

- **Kāda iepriekšēja informācija būtu sniedzama datu subjektam?**

[23] Izmantojot personas datus, ko nosūta datu subjekts, īstenojot savas tiesības uz datu pārnesamību, sociālās tīklošanas pakalpojumam nevajadzētu papildināt savu dalībnieku profilu, neievērojot pārredzamības principu un nepārliecinoties, vai attiecībā uz šo konkrēto apstrādi dalībnieki balstās uz attiecīgu juridisko pamatu.

Lai ievērotu jaunās tiesības uz datu pārnesamību, datu pārziņiem ir jāinformē datu subjekti par jauno tiesību uz pārnesamību pastāvēšanu. Ja attiecīgos personas datus vāc tieši no datu subjekta, tas jādara "personas datu iegūšanas laikā". Ja personas dati nav iegūti no datu subjekta, datu pārzinim ir jāsniedz 13. panta 2. punkta b) apakšpunktā un 14. panta 2. punkta c) apakšpunktā prasītā informācija.

" Ja personas dati nav iegūti no datu subjekta", 14. panta 3. punktā ir noteikts, ka informācija jāsniedz saprātīgā termiņā, kas nepārsniedz vienu mēnesi pēc datu iegūšanas, kad ar datu subjektu notiek pirmā saziņa vai kad dati tiek izpausti trešām personām[24].

Sniedzot pieprasīto informāciju, datu pārziņiem ir jānodrošina tiesību uz datu pārnesamību nošķiršana no citām tiesībām. Tāpēc 29. panta Darba grupa jo īpaši iesaka datu pārziņiem nepārprotami paskaidrot atšķirības starp datu veidiem, ko datu subjekts var saņemt, izmantojot savas tiesības uz piekļuvi un datu pārnesamību.

Papildus tam darba grupa iesaka datu pārziņiem vienmēr iekļaut informāciju par tiesībām uz datu pārnesamību, pirms datu subjekti slēdz kādu no saviem kontiem. Tas ļauj lietotājiem pirms līguma izbeigšanas izvērtēt savus personas datus un tos viegli nosūtīt uz savu ierīci vai citam pakalpojumu sniedzējam.

Visbeidzot, kā vadošu praksi "saņēmējiem" datu pārziņiem 29. panta Darba grupa iesaka sniegt datu subjektiem pilnu informāciju par personas datu īpatnībām, kas ir būtiskas viņu pakalpojumu sniegšanai. Papildus godprātīgas apstrādes nodrošināšanai tas ļauj lietotājiem ierobežot riskus trešām personām, kā arī personas datu jebkuru citu nevajadzīgu dublēšanos, pat ja nav iesaistīti citi datu subjekti.

- **Kā datu pārzinis var identificēt datu subjektu, pirms atbildēt uz viņa pieprasījumu?**

VDAR nav preskriptīvu prasību par to, kā autentificēt datu subjektu. Tomēr VDAR 12. panta 2. punktā ir noteikts, ka datu pārzinis neatsakās rīkoties pēc datu subjekta pieprasījuma par savu tiesību (tostarp tiesību uz datu pārnesamību) īstenošanu, izņemot gadījumus, kad nolūki, kādos pārzinis apstrādā personas datus, neprasa pārzinim identificēt datu subjektu, un pārzinis var uzskatāmi parādīt, ka nespēj identificēt datu subjektu. Tomēr, kā noteikts 11. panta 2. punktā, šādos gadījumos datu subjekts var sniegt papildu informāciju, kas ļauj viņu identificēt. Papildus tam 12. panta 6. punktā ir noteikts, ka tad, ja pārzinim ir pamatotas šaubas par datu subjekta identitāti, viņš var prasīt, lai tiktu sniegta papildu informācija datu subjekta identitātes apstiprināšanai. Ja datu subjekts sniedz papildu informāciju, kas ļauj viņu identificēt, datu pārzinis neatsakās rīkoties pēc pieprasījuma. Ja informācija un tiešsaistē savāktie dati ir saistīti ar pseidonīmiem vai unikāliem identifikatoriem, datu pārziņi var ieviest atbilstošas procedūras, kas ļauj personai iesniegt datu pārnesamības pieprasījumu un pieprasīt un saņemt savus datus. Jebkurā gadījumā datu pārziņiem ir jāievieš autentifikācijas procedūra, lai stingri pārliecinātos par tā datu subjekta identitāti, kas pieprasa savus personas datus vai plašāk īsteno tiesības, kas piešķirtas ar VDAR.

Šīs procedūras bieži vien jau pastāv. Datu pārzinis bieži vien jau ir autentificējis datu subjektu, pirms noslēgt līgumu vai saņemt viņa piekrišanu apstrādei. Līdz ar to personas

[24] VDAR 12. pantā ir noteikts, ka datu pārziņi nodrošina "visu [..] saziņu kodolīgā, pārredzamā, saprotamā un viegli pieejamā veidā, izmantojot skaidru un vienkāršu valodu, jo īpaši attiecībā uz visu informāciju, kas konkrēti paredzēta bērnam."

datus, ko izmanto, lai reģistrētu personu, uz kuru attiecas apstrāde, var izmantot arī kā pierādījumus, lai datu subjektu autentificētu pārnesamības nolūkā[25].

Lai gan šajos gadījumos datu subjektu iepriekšējai identifikācijai varētu būt nepieciešami viņu juridiskās identitātes pierādījumi, šāda pārbaude var nebūt svarīga, lai izvērtētu saikni starp datiem un attiecīgo personu, jo šī saikne nav saistīta ar oficiālo vai juridisko identitāti. Būtībā datu pārziņa spēja pieprasīt papildu informāciju, lai noteiktu personas identitāti, nevar būt par iemeslu pārmērīgām prasībām un tādu personas datu vākšanai, kas nav būtiski vai nepieciešami, lai nostiprinātu saikni starp personu un pieprasītajiem personas datiem.

Daudzos gadījumos šādas autentifikācijas procedūras jau ir ieviestas. Piemēram, lietotājvārdus un paroles bieži vien izmanto, lai personas varētu piekļūt saviem datiem e-pasta kontos, sociālās tīklošanas kontos un kontos, ko izmanto dažādiem citiem pakalpojumiem, dažus no kuriem personas izvēlas izmantot, neatklājot savu vārdu un uzvārdu un identitāti.

Ja datu subjekta pieprasīto datu izmērs dara problemātisku to nosūtīšanu internetā, tā vietā, lai, iespējams, pagarinātu pieprasījuma izpildes termiņu ne ilgāk kā uz trīs mēnešiem[26], datu pārzinim var būt nepieciešams apsvērt arī alternatīvus līdzekļus datu sniegšanai, tādus kā straumēšanas izmantošana vai to saglabāšana uz CD, DVD vai citiem fiziskiem nesējiem, vai arī atļaut tieši nosūtīt personas datus citam datu pārzinim (saskaņā ar VDAR 20. panta 2. punktu, ja tas ir tehniski iespējams).

- **Kāds ir noteiktais termiņš atbildēšanai uz pārnesamības pieprasījumu?**

VDAR 12. panta 3. punktā ir noteikts, ka datu pārzinis "bez nepamatotas kavēšanās" un jebkurā gadījumā "mēneša laikā pēc pieprasījuma saņemšanas" datu subjektu "informē par darbību, kas veikta". Sarežģītos gadījumos šo viena mēneša laikposmu var pagarināt ne ilgāk kā uz trīs mēnešiem ar noteikumu, ka datu subjekts mēneša laikā no sākotnējā pieprasījuma ir informēts par šādas kavēšanās iemesliem.

Datu pārziņi, kas sniedz informācijas sabiedrības pakalpojumus, varētu būt labāk sagatavoti tam, lai izpildītu pieprasījumus ļoti īsā laikposmā. Lai apmierinātu lietotāju vēlmes, laba prakse ir noteikt termiņu, kādā parasti ir iespējams atbildēt uz datu pārnesamības pieprasījumiem, un paziņot to datu subjektiem.

Saskaņā ar 12. panta 4. punktu datu pārziņi, kas atsakās atbildēt uz pārnesamības pieprasījumu, vēlākais mēneša laikā pēc pieprasījuma saņemšanas informē datu subjektu "par darbības neveikšanas iemesliem un par iespēju iesniegt sūdzību uzraudzības iestādei un vērsties tiesā".

Datu pārziņiem ir jāpilda pienākums atbildēt noteiktajā termiņā, pat ja tas attiecas uz atteikumu. Citiem vārdiem, datu pārzinis nevar klusēt, kad viņam lūdz atbildēt uz datu pārnesamības pieprasījumu.

- **Kādos gadījumos var noraidīt datu pārnesamības pieprasījumu vai pieprasīt par to maksu?**

[25] Piemēram, ja datu apstrāde ir saistīta ar lietotāja kontu, attiecīgais pieteikumvārds un parole varētu būt pietiekami, lai identificētu datu subjektu.
[26] VDAR 12. panta 3. punkts: "Pārzinis informē par darbību, kas veikta pēc pieprasījuma".

Saskaņā ar 12. pantu datu pārzinim ir aizliegts pieprasīt maksu par personas datu sniegšanu, ja vien pārzinis nevar parādīt, ka pieprasījumi ir acīmredzami nepamatoti vai pārmērīgi, "jo īpaši to regulāras atkārtošanās dēļ". Informācijas sabiedrības pakalpojumu sniedzējiem, kas specializējas personas datu automatizētā apstrādē, tādu automatizētu sistēmu ieviešana kā lietojumprogrammu saskarnes[27] var atvieglot datu apmaiņu ar datu subjektu un tādējādi mazināt iespējamo slogu, ko rada pieprasījumu regulāra atkārtošanās. Tāpēc vajadzētu būt ļoti nelielam skaitam gadījumu, kad datu pārzinis spēj pamatot atteikumu sniegt pieprasīto informāciju pat attiecībā uz vairākkārtējiem datu pārnesamības pieprasījumiem.

Turklāt, lai noteiktu pieprasījuma pārmērīgumu, nebūtu jāņem vērā to procesu kopējās izmaksas, kas izveidoti, lai atbildētu uz datu pārnesamības pieprasījumiem. Faktiski VDAR 12. pantā galvenā uzmanība pievērsta pieprasījumiem, ko iesniedz viens datu subjekts, nevis pieprasījumu, kurus saņem datu pārzinis, kopējam skaitam. Tāpēc nevajadzētu pieprasīt, lai datu subjekti atlīdzina sistēmas ieviešanas kopējās izmaksas, nedz arī tās izmantot, lai pamatotu atteikumu atbildēt uz pārnesamības pieprasījumiem.

V. Kā jāsniedz pārnesamie dati?

- Kādi ir datu sniegšanas līdzekļi, kurus sagaida, ka ieviesīs datu pārzinis?

VDAR 20. panta 1. punktā ir noteikts, ka datu subjektiem ir tiesības datus nosūtīt citam pārzinim, un pārzinis, kuram attiecīgie personas dati sniegti, tam nerada nekādus šķēršļus.

Šos šķēršļus var raksturot kā jebkurus juridiskus, tehniskus vai finanšu šķēršļus, ko rada datu pārzinis, lai datu subjektam vai citam datu pārzinim atturētos sniegt vai palēninātu piekļuvi, nosūtīšanu vai atkalizmantošanu. Šāds šķērslis, piemēram, varētu būt maksa, ko pieprasa par datu piegādi, sadarbspējas vai piekļuves neesamība kādam datu formātam vai lietojumprogrammu saskarnei, vai nodrošinātajam formātam, pārmērīga kavēšanās vai tas, ka ir sarežģīti izgūt datu pilnu kopumu, datu kopuma apzināta pieslēpšana vai īpašas un neatbilstošas vai pārmērīgas nozaru standartizācijas vai akreditācijas prasības[28].

Ar 20. panta 2. punktu datu pārziņiem tiek noteikts arī pienākums personas datus nosūtīt tieši no viena datu pārziņa citam pārzinim, "ja tas ir tehniski iespējams".

Datu nosūtīšanas tehniskā iespējamība no viena datu pārziņa citam pārzinim būtu jāvērtē katrā gadījumā atsevišķi. VDAR 68. apsvērumā precizētas "tehniskās iespējamības" robežas, norādot, ka "[šīm tiesībām] nebūtu jārada pārziņiem pienākums ieviest vai uzturēt apstrādes sistēmas, kas ir tehniski saderīgas".

No datu pārziņiem sagaida, ka viņi nosūtīs personas datus savstarpēji izmantojamā formātā, tomēr ar to netiek noteikts pienākums citiem datu pārziņiem atbalstīt šos formātus. Tāpēc tieša nosūtīšana no viena datu pārziņa citam pārzinim varētu notikt tad, ja ir iespējama saziņa starp divām sistēmām drošā veidā[29] un saņēmēja sistēma ir tehniski spējīga saņemt ienākošos datus. Ja tiešu nosūtīšanu liedz tehniski šķēršļi, datu pārzinis izskaidro datu subjektiem

[27] Lietojumprogrammu saskarne ir lietojumu saskarnes vai tīmekļa pakalpojumi, kurus dara pieejamus datu pārziņi, lai citas sistēmas vai lietojumi varētu savienoties un strādāt ar savām sistēmām.

[28] Varētu rasties daži tādi leģitīmi šķēršļi kā tie, kas ir saistīti ar citu personu tiesībām un brīvībām un minēti 20. panta 4. punktā, vai arī tādi, kas ir saistīti ar pārziņu sistēmu drošību. Datu pārziņa pienākums ir pamatot, kāpēc šādi šķēršļi ir leģitīmi un kāpēc tie nav šķēršļi 20. panta 1. punkta nozīmē.

[29] Izmantojot autentificētu saziņu ar datu šifrēšanas nepieciešamo līmeni.

minētos šķēršļus, jo pretējā gadījumā viņa lēmumam būs līdzīgas sekas kā atteikumam veikt darbību, ko pieprasījis datu subjekts (12. panta 4. punkts).

Tehniskā līmenī datu pārziņiem būtu jāizpēta un jāizvērtē divi dažādi un savstarpēji papildinoši veidi, kā pārnesamos datus darīt pieejamus datu subjektiem vai citiem datu pārziņiem:

- pārnesamo datu visa kopuma (vai globālā datu kopuma daļu vairāku izvilkumu) tieša nosūtīšana;
- automatizēts rīks, kas ļauj iegūt attiecīgos datus.

Gadījumos, kas saistīti ar sarežģītiem un lieliem datu kopumiem, datu pārziņi varētu dot priekšroku otrajam veidam, jo tas ļauj iegūt datu kopuma jebkuru daļu, kas ir būtiska datu subjektam viņa pieprasījuma kontekstā, var palīdzēt samazināt risku un, iespējams, ļauj izmantot datu sinhronizācijas mehānismus[30] (piemēram, regulāras saziņas kontekstā starp datu pārziņiem). Tas varētu būt labāks veids, kā nodrošināt "jaunā" pārziņa atbilstību, un laba prakse, kā samazināt privātās dzīves aizskāruma riskus no sākotnējā datu pārziņa puses.

Šos divus dažādos un, iespējams, savstarpēji papildinošos attiecīgo pārnesamo datu sniegšanas veidus varētu īstenot, darot datus pieejamus ar dažādiem līdzekļiem, tādiem kā, piemēram, droša ziņojumapmaiņa, SFTP serveris, droša tīmekļa lietojumprogrammu saskarne vai tīmekļa portāls. Datu subjektiem būtu jādod iespēja izmantot personas datu krātuvi, personiskās informācijas pārvaldības sistēmu[31] vai citus uzticamu trešo personu veidus, lai turētu un uzglabātu personas datus un atļautu datu pārziņiem pēc vajadzības piekļūt personas datiem un tos apstrādāt.

- **<u>Kāds ir sagaidāmais datu formāts?</u>**

VDAR izvirza prasību datu pārziņiem personas datus, ko pieprasa persona, sniegt tādā formātā, kas atbalsta atkalizmantošanu. Konkrēti, VDAR 20. panta 1. punktā ir noteikts, ka personas dati jāsniedz "strukturētā, plaši izmantotā un mašīnlasāmā formātā". VDAR 68. apsvērumā precizēts, ka šim formātam vajadzētu būt savstarpēji izmantojamam, kas ir termins, kurš ES definēts[32] šādi:

> *dažādu un atšķirīgu organizāciju spēja nodrošināt mijiedarbību savstarpēji izdevīgu un saskaņotu kopīgu mērķu sasniegšanā, tostarp apmainoties ar informāciju un zināšanām starp organizācijām, izmantojot uzņēmējdarbības procesus, ko tās atbalsta ar datu apmaiņu starp to attiecīgām IKT sistēmām.*

Termini "strukturēts", "plaši izmantots" un "mašīnlasāms" ir obligāto prasību kopums, kam būtu jāatvieglo datu formāta, ko nodrošina datu pārzinis, sadarbspēja. Tādējādi "strukturēts,

[30] Sinhronizācijas mehānisms var palīdzēt izpildīt vispārējos pienākumus, kas minēti VDAR 5. pantā, kurā noteikts, ka "personas dati ir [..] precīzi un, ja vajadzīgs, atjaunināti".
[31] Par personiskās informācijas pārvaldības sistēmām (PIPS), skatīt, piemēram, EDAU Atzinumu Nr. 9/2016, kas ir pieejams https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf
[32] Eiropas Parlamenta un Padomes 2009. gada 16. septembra Lēmuma Nr. 922/2009/EK par Eiropas valstu pārvaldes iestāžu sadarbspējas risinājumiem (*ISA*) 2. pants, OV L 260, 3.10.2009., 20. lpp.

plaši izmantots un mašīnlasāms" ir līdzekļu specifikācijas, savukārt sadarbspēja ir vēlamais iznākums.

Direktīvas 2013/37/ES[33,34] 21. apsvērumā termins "mašīnlasāms" definēts šādi:

> *datnes formāts, kas ir strukturēts tā, lai lietojumprogrammas var viegli identificēt, atpazīt un iegūt no dokumenta specifiskus datus, tostarp atsevišķas faktoloģiskas vienības un to iekšējo struktūru. Datnēs šifrēti dati, kas strukturēti mašīnlasāmā formātā, ir mašīnlasāmi dati. Mašīnlasāmi formāti var būt gan atvērti formāti, gan komerciāli formāti; tiem var būt un var nebūt formāli standarti. Datnes formātā šifrēti dokumenti, kuru automātiskā apstrāde ir ierobežota, jo datus no šiem dokumentiem nav iespējams atlasīt vai ir sarežģīti to izdarīt, nebūtu jāuzskata par dokumentiem mašīnlasāmā formātā. Attiecīgos gadījumos dalībvalstīm būtu jāveicina atvērtu mašīnlasāmu formātu lietošana.*

Ņemot vērā iespējamo to datu veidu plašo klāstu, ko varētu apstrādāt datu pārzinis, VDAR nav paredzēti konkrēti ieteikumi attiecībā uz sniedzamo personas datu formātu. Vispiemērotākais formāts dažādās nozarēs atšķirsies, un atbilstoši formāti, iespējams, jau pastāv, un tāds vienmēr ir jāizvēlas, lai dati būti interpretējami un nodrošinātu datu subjektam datu pārnesamības augstu pakāpi. Par piemērotu pieeju netiek uzskatīti formāti, uz kuriem attiecas dārgi licencēšanas ierobežojumi.

VDAR 68. apsvērumā precizēts, ka "*Datu subjekta tiesībām nosūtīt vai saņemt personas datus par sevi nebūtu jārada pārziņiem pienākums ieviest vai uzturēt apstrādes sistēmas, kas ir tehniski saderīgas.*" **Tādējādi pārnesamības mērķis ir radīt savstarpēji izmantojamas, nevis saderīgas sistēmas**[35]**.**

Sagaida, ka personas datus sniegs tādos formātos, kam ir augsts abstrakcijas līmenis no iekšējiem vai patentētiem formātiem. Datu pārnesamība kā tāda ietver datu apstrādes, ko veic datu pārziņi, papildu slāni nolūkā iegūt datus no platformas un filtrēt personas datus, uz kuriem neattiecas pārnesamība, tādus kā izrietošie dati vai dati, kas saistīti ar drošības sistēmām. Tādējādi datu pārziņi tiek mudināti savās sistēmās iepriekš identificēt datus, uz kuriem attiecas pārnesamība. Šī datu papildu apstrāde tiks uzskatīta par tādu, ko veic papildus datu galvenajai apstrādei, jo tās nolūks nav sasniegt jaunu mērķi, ko definējis datu pārzinis.

Ja konkrētā nozarē vai kontekstā nav formātu, kas tiek plaši izmantoti, **datu pārziņiem būtu jāsniedz personas dati, izmantojot plaši izmantotus atvērtus formātus (piem., *XML, JSON, CSV*, …) apvienojumā ar** noderīgiem **metadatiem iespējami visaugstākajā detalizācijas līmenī,** vienlaikus saglabājot augstu abstrakcijas līmeni. Metadati kā tādi būtu jāizmanto, lai precīzi aprakstītu apmainītās informācijas nozīmi. Šiem metadatiem vajadzētu būt pietiekamiem, lai padarītu iespējamu šo funkciju un datu atkalizmantošanu, bet, protams, neatklājot tirdzniecības noslēpumus. Tāpēc ir maz ticams, ka e-pasta iesūtnes *PDF* versiju sniegšana kādai personai būs pietiekami strukturēta vai aprakstoša, lai iesūtnes datus varētu

[33] Ar ko groza Direktīvu 2003/98/EK par valsts sektora informācijas atkalizmantošanu.

[34] ES glosārijā (http://eur-lex.europa.eu/eli-register/glossary.html) sniegts papildu precizējums attiecībā uz to, kas domāts ar šajā pamatnostādnē lietotajiem jēdzieniem, tādiem kā *mašīnlasāms, sadarbspēja*, atvērts formāts, *standarts, metadati*.

[35] ISO/IEC 2382-01 sadarbspēja definēta šādi: "Spēja sazināties, izpildīt programmas vai nosūtīt datus starp dažādām funkcionālajām vienībām tādā veidā, ka lietotājam ir vajadzīgas nelielas zināšanas par minēto vienību unikālajām īpašībām, vai arī tās vispār nav vajadzīgas."

viegli atkalizmantot. Tā vietā, lai nodrošinātu e-pasta datu efektīvu atkalizmantošanu, šos datus vajadzētu sniegt tādā formātā, kas saglabā visus metadatus. Izvēloties datu formātu, kādā sniegt personas datus, datu pārzinim būtu jāapsver, kā šis formāts ietekmēs vai kavēs personas tiesības uz datu atkalizmantošanu. Gadījumos, kad datu pārzinis var piedāvāt datu subjektam vairākas izvēles iespējas attiecībā uz personas datu vēlamo formātu, būtu jāsniedz šīs izvēles ietekmes nepārprotams skaidrojums. Tomēr papildu metadatu apstrāde vienīgi tādā nolūkā, ka tie varētu būt vajadzīgi vai vēlami, lai atbildētu uz datu pārnesamības pieprasījumu, nerada leģitīmu pamatu šādai apstrādei.

29. panta Darba grupa aktīvi mudina nozares ieinteresētās personas un tirdzniecības asociācijas sadarboties un kopīgi strādāt, lai izveidotu savstarpēji izmantojamu standartu un formātu kopumu un izpildītu prasības, ko izvirza tiesības uz datu pārnesamību. Šī problēma ir risināta arī Eiropas sadarbspējas satvarā (*EIF*), izstrādājot un saskaņojot pieeju tādu organizāciju sadarbspējai, kuras vēlas kopīgi sniegt sabiedriskus pakalpojumus. Tā piemērošanas jomā šis satvars nosaka tādus kopīgus elementus kā vārdu krājums, jēdzieni, principi, politika, pamatnostādnes, ieteikumi, standarti, specifikācijas un prakse[36].

- **Kā rīkoties, ja ir jāvāc liela apjoma un sarežģīti personas dati?**

VDAR nav izskaidrots, kā risināt jautājumu, ja ir jāvāc liela apjoma dati, datu struktūra ir sarežģīta vai rodas citas tehniskas problēmas, kas varētu radīt grūtības datu pārziņiem vai datu subjektiem.

Tomēr visos gadījumos ir ļoti svarīgi, lai persona varētu pilnībā saprast to personas datu definīciju, shēmu un struktūru, kurus var sniegt datu pārzinis. Piemēram, datus vispirms varētu sniegt kopsavilkuma veidā, izmantojot informācijas paneļus, kas ļauj datu subjektam pārnest personas datu apakškopas, nevis datus kopumā. Datu pārzinim vajadzētu sniegt pārskatu "kodolīgā, pārredzamā, saprotamā un viegli pieejamā veidā, izmantojot skaidru un vienkāršu valodu" (sk. VDAR 12. panta 1. punktu), lai datu subjektam vienmēr būtu skaidra informācija par to, kādus datus lejupielādēt vai nosūtīt citam datu pārzinim attiecībā uz konkrēto nolūku. Piemēram, datu subjektiem vajadzētu spēt izmantot lietojumprogrammatūru, lai viegli identificētu, atpazītu un apstrādātu tās datus.

Kā iepriekš minēts, praktisks veids, kā atbildēt uz datu pārnesamības pieprasījumiem, varētu būt piedāvāt pienācīgi nodrošinātu un dokumentētu lietojumprogrammu saskarni. Tas varētu ļaut personām iesniegt datu pārzinim savu personas datu pieprasījumus, izmantojot savu vai trešo personu programmatūru, vai atļaut citiem (tostarp citam datu pārzinim) to darīt viņu vārdā, kā noteikts VDAR 20. panta 2. punktā. Piešķirot piekļuvi datiem ar ārēji pieejamas lietojumprogrammas saskarnes palīdzību, varētu būt iespējams arī piedāvāt sarežģītāku piekļuves sistēmu, kas ļauj personām veikt turpmākus datu pieprasījumus pilnīgas lejupielādes vai delta funkcijas veidā, kas satur tikai tās izmaiņas, kas notikušas kopš pēdējās lejupielādes, un šie papildu pieprasījumi nebūtu apgrūtinoši datu pārzinim.

- **Kā pārnesamos datus var padarīt drošus?**

Saskaņā ar VDAR 5. panta 1. punkta f) apakšpunktu datu pārziņiem būtu jāgarantē "atbilstoša personas datu drošība, tostarp aizsardzība pret neatļautu vai nelikumīgu apstrādi un pret

[36] Avots: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu, izmantojot atbilstošus tehniskos vai organizatoriskos pasākumus".

Tomēr dažas drošības problēmas var izraisīt arī personas datu nosūtīšana datu subjektam.

Kā datu pārziņi var nodrošināt, ka personas dati tiek droši nogādāti īstajai personai?

Tā kā datu pārnesamības mērķis ir izņemt personas datus no datu pārziņa informācijas sistēmas, attiecībā uz minētajiem datiem nosūtīšana var kļūt par iespējamu riska avotu (īpaši datu aizsardzības pārkāpumu dēļ nosūtīšanas laikā). Datu pārzinis ir atbildīgs par visu drošības pasākumu veikšanu, kas ir nepieciešami, lai personas dati tiktu droši nosūtīti (izmantojot šifrēšanu no viena gala līdz otram jeb datu šifrēšanu) pareizajam adresātam (izmantojot stingrus autentifikācijas pasākumus), bet arī turpinātu aizsargāt personas datus, kas paliek viņu sistēmās, kā arī par pārredzamām procedūrām datu aizsardzības pārkāpumu novēršanai[37]. Datu pārziņiem būtu jāizvērtē īpašie riski, kas saistīti ar datu pārnesamību, un jāveic atbilstoši risku mazināšanas pasākumi.

Šādi riska mazināšanas pasākumi varētu ietvert autentifikācijas papildu procedūru, tādu kā kopīgs noslēpums, vai citu autentifikācijas faktoru, tādu kā vienreizējā parole, izmantošanu, ja datu subjektu jau ir nepieciešams autentificēt; nosūtīšanas pārtraukšanu vai iesaldēšanu, ja ir aizdomas, ka konta drošība bijusi apdraudēta; tiešas nosūtīšanas gadījumos no viena datu pārziņa citam pārzinim būtu jāizmanto autentifikācija pēc pilnvarojuma, piemēram, autentifikācija ar marķierierīces palīdzību.

Šādiem drošības pasākumiem nevajadzētu būt traucējoša rakstura, un tie nedrīkst liegt lietotājiem īstenot viņu tiesības, piemēram, uzliekot papildu izmaksas.

Kā palīdzēt lietotājiem aizsargāt viņu personas datu uzglabāšanu viņu pašu sistēmās?

Izgūstot savus personas datus no kāda tiešsaistes pakalpojuma, vienmēr pastāv risks, ka lietotāji tos varētu uzglabāt ne tik drošās sistēmās kā tā, ko piedāvā pakalpojums. Datu subjekts, kas pieprasa datus, ir atbildīgs par pareizo pasākumu apzināšanu personas datu aizsardzībai savā sistēmā. Tomēr, lai veiktu pasākumus izgūtās informācijas aizsardzībai, viņi par to būtu jāinformē. Kā vadošās prakses piemēru, lai palīdzētu datu subjektam sasniegt šo mērķi, datu pārziņi varētu izmantot arī ieteikumus attiecībā uz atbilstošu formātu(-iem), šifrēšanas rīkiem un citiem drošības pasākumiem.

* * *

Briselē, 2016. gada 13. decembrī

Darba grupas vārdā —
priekšsēdētāja
Isabelle FALQUE-PIERROTIN

[37] Saskaņā ar Direktīvu (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā.

Pēdējo reizi pārskatītas un pieņemtas 2017. gada 5. aprīlī

Darba grupas vārdā —
priekšsēdētāja
Isabelle FALQUE-PIERROTIN