Pamatnostādnes 2/2020 par Regulas 2016/679 46. panta 2. punkta a) apakšpunkta un 46. panta 3. punkta b) apakšpunkta piemērošanu personas datu nosūtīšanai starp EEZ publiskajām iestādēm un struktūrām un ārpus EEZ esošām publiskajām iestādēm un struktūrām

2.0 versija

Pieņemtas 2020. gada 15. decembrī

Versiju hronoloģija

2.0 versija	2020. gada 15. decembris	Pamatnostādņu pieņemšana pēc sabiedriskās apspriešanas
1.0 versija	2020. gada 18. februāris	Pamatnostādņu pieņemšana sabiedriskajai apspriešanai

Saturs

Eiropas Datu aizsardzības kolēģija,

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

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

ņemot vērā tās Reglamenta 12. un 22. pantu,

IR PIEŅĒMUSI ŠĪS PAMATNOSTĀDNES.

[1] Atsauces uz "dalībvalstīm" šajās pamatnostādnēs būtu jāsaprot kā atsauces uz "EEZ dalībvalstīm".

1. VISPĀRĪGI JAUTĀJUMI

1.1 Mērķis

1. Šā dokumenta mērķis ir sniegt norādes par Vispārīgās datu aizsardzības regulas (VDAR) 46. panta 2. punkta a) apakšpunkta un 46. panta 3. punkta b) apakšpunkta piemērošanu gadījumos, kad EEZ publiskās iestādes vai struktūras (turpmāk – "publiskās iestādes") nosūta personas datus trešo valstu publiskajām iestādēm vai starptautiskajām organizācijām, ciktāl tām nav piemērojams Eiropas Komisijas pieņemtais atzinums par aizsardzības līmeņa pietiekamību[2]. Publiskās iestādes var izvēlēties izmantot šos mehānismus, kuri VDAR tiek uzskatīti par tām piemērotākiem, taču var arī brīvi izmantot citus atbilstīgus rīkus, kas nodrošina atbilstošas garantijas saskaņā ar VDAR 46. pantu.

2. Šajās pamatnostādnēs ir paredzēts sniegt norādes par to, kādas garantijas Eiropas Datu aizsardzības kolēģijas (EDAK) ieskatā būtu nodrošināmas ar VDAR 46. panta 2. punkta a) apakšpunktā minēto juridiski saistošo un tiesiski īstenojamo instrumentu starp publiskām iestādēm vai struktūrām vai, ja tiek saņemta kompetentās uzraudzības iestādes (*SA*) atļauja, ar VDAR 46. panta 3. punkta b) apakšpunktā minētajiem noteikumiem, kuri iekļaujami administratīvajās vienošanās starp publiskajām iestādēm[3]. EDAK stingri iesaka pusēm sākumposmā atsaukties uz šīm pamatnostādnēm, ja tiek plānots noslēgt vai grozīt šos instrumentus vai vienošanās[4].

3. Šīs pamatnostādnes ir jāskata saistībā ar EDAK līdzšinējo darbu (tostarp saistībā ar dokumentiem, kurus ir apstiprinājusi tās priekšgājēja "29. panta darba grupa"[5] ("DG29")), kas skar galvenos jautājumus par teritoriālo darbības jomu un personas datu nosūtīšanu trešām valstīm[6]. Šīs pamatnostādnes tiks pārskatītas un vajadzības gadījumā atjauninātas, pamatojoties uz praktisko pieredzi, kas gūta, piemērojot VDAR.

4. Šīs pamatnostādnes attiecas uz datu starptautisku nosūtīšanu, ko publiskas iestādes veic dažādos administratīvās sadarbības nolūkos, kas ietilpst VDAR darbības jomā. Tādējādi un saskaņā ar VDAR 2. panta 2. punktu tās neattiecas uz datu nosūtīšanu, kas tiek veikta sabiedriskās drošības, aizsardzības vai valsts drošības nolūkā. Turklāt šīs pamatnostādnes neattiecas uz datu apstrādi un nosūtīšanu, ko kompetentās iestādes veic krimināltiesību aktu piemērošanas nolūkos, jo to reglamentē atsevišķs tiesību akts, Tiesībaizsardzības direktīva[7]. Visbeidzot, šajās pamatnostādnēs uzmanība ir vērsta vienīgi uz datu nosūtīšanu, ko savstarpēji veic publiskās iestādes, un nav aplūkotas situācijas, kad personu datus publiska iestāde nosūta privātam tiesību subjektam vai privātais tiesību subjekts nosūta publiskai iestādei.

---

[2] Piemēram, Japānas publiskās iestādes, uz kurām neattiecas lēmums par Japānas aizsardzības līmeņa pietiekamību, jo tas attiecas tikai uz privātā sektora organizācijām.

[3] Šajās pamatnostādnēs, lai norādītu VDAR 46. panta 2. punkta a) apakšpunktā minētos juridiski saistošos un tiesiski īstenojamos instrumentus un VDAR 46. panta 3. punkta b) apakšpunktā minētās administratīvās vienošanās, tiek izmantots termins "starptautiski nolīgumi".

[4] VDAR 96. pantā ir noteikts, ka nolīgumi, kas ir noslēgti pirms 2016. gada 24. maija, paliek spēkā līdz brīdim, kad tie tiek grozīti, aizstāti vai atcelti.

[5] ES datu aizsardzības iestāžu darba grupa, kas izveidota saskaņā ar Datu aizsardzības direktīvas 95/46/EK 29. pantu.

[6] Sk. 29. panta darba grupas dokumentu "Pietiekamības atsauces" (WP254 rev.01, ko EDAK ir apstiprinājusi 2018. gada 25. maijā), EDAK Pamatnostādnes 2/2018 par atkāpēm no Regulas 2016/679 49. panta un EDAK Pamatnostādnes 3/2018 par VDAR teritoriālo darbības jomu (3. pants).

[7] Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināls odus, un par šādu datu brīvu apriti.

1.2 Datu starptautiskajai nosūtīšanai piemērojamie vispārīgie noteikumi

5. Saskaņā ar VDAR 44. pantu datu nosūtītājam, kas nosūta personas datus trešām valstīm vai starptautiskajām organizācijām, ir jāizpilda ne tikai VDAR V nodaļas prasības, bet arī citi VDAR noteikumi. Proti, veicot apstrādes darbības, ir jāievēro VDAR 5. pantā noteiktie datu aizsardzības principi, VDAR 6. pantā noteiktais apstrādes likumīgums un VDAR 9. panta nosacījumi par īpašu kategoriju personas datu apstrādi. Tādējādi ir jāveic divkārša pārbaude: pirmkārt, pašai datu apstrādei ir jāpiemēro tiesiskais pamats un visi attiecīgie VDAR noteikumi; otrkārt, ir jāizpilda VDAR V nodaļā sniegtie noteikumi.

6. VDAR 46. pantā ir noteikts – "*ja nav pieņemts lēmums saskaņā ar 45. panta 3. punktu, pārzinis vai apstrādātājs var nosūtīt personas datus uz trešo valsti vai uz starptautisku organizāciju tikai tad, ja pārzinis vai apstrādātājs ir sniedzis atbilstošas garantijas, un ar nosacījumu, ka datu subjektiem ir pieejamas īstenojamas datu subjekta tiesības un efektīvi tiesiskās aizsardzības līdzekļi*". Šādas atbilstošas garantijas var nodrošināt ar juridiski saistošu un tiesiski īstenojamu instrumentu starp publiskām iestādēm vai struktūrām (VDAR 46. panta 2. punkta a) apakšpunkts) vai, saņemot kompetentās uzraudzības iestādes atļauju, ar noteikumiem, kuri iekļaujami administratīvajās vienošanās starp publiskām iestādēm vai struktūrām un kuri ietver īstenojamas un efektīvas datu subjektu tiesības (VDAR 46. panta 3. punkta b) apakšpunkts). Kā precizējusi Eiropas Savienības Tiesa (EST), šīm atbilstošām garantijām ir jābūt tādām, lai nodrošinātu, ka datu subjektiem, kuru personas dati tiek nosūtīti, tiek nodrošināts tāds aizsardzības līmenis, kas būtībā ir līdzvērtīgs EEZ garantētajam līmenim[8].

7. Papildus šim risinājumam vai ja šāda risinājuma nav, VDAR 49. pantā ir piedāvātas dažas īpašas situācijas, kad datus var starptautiski nosūtīt, ja Eiropas Komisija nav sniegusi atzinumu par atbilstības līmeņa pietiekamību[9]. Proti, viena no atkāpēm attiecas uz datu nosūtīšanu, kas nepieciešama, ja ir svarīgi iemesli sabiedrības interesēs, kas ir atzīti Savienības tiesībās vai tās dalībvalsts tiesībās, kuras ir piemērojamas datu pārzinim, tostarp starptautiskās sadarbības savstarpīguma nolūkos[10]. Tomēr, kā jau tika paskaidrots iepriekšējās EDAK izdotajās pamatnostādnēs, VDAR 49. pantā ietvertās atkāpes ir jāinterpretē šauri un tās galvenokārt attiecas uz gadījuma un neregulārām apstrādes darbībām[11].

1.3 Publiskas iestādes vai struktūras definīcija

8. VDAR nav definēts, kas ir "publiska iestāde vai struktūra". EDAK uzskata, ka tas ir pietiekami plašs jēdziens, kas aptver trešo valstu publiskās iestādes un starptautiskās organizācijas[12]. Attiecībā uz trešo valstu publiskajām iestādēm šis jēdziens ir jānosaka saskaņā ar attiecīgās valsts tiesību aktiem. Līdz ar to publiskās iestādes ir dažādu līmeņu valsts pārvaldes iestādes (piemēram, valsts, reģionālās un pašvaldību iestādes), bet var būt arī citas iestādes, kas ir publisko tiesību subjekti (piemēram, izpildaģentūras, universitātes, slimnīcas utt.)[13]. Saskaņā ar VDAR 4. panta 26. punktu "starptautiska

[8] Eiropas Savienības Tiesa, lieta C-311/18, *Data Protection Commissioner* pret *Facebook Ireland* un *Maximillian Schrems* (*Schrems II*), 96. punkts.
[9] Sīkāku informāciju par 49. pantu un tā mijiedarbību ar 46. pantu kopumā sk. EDAK Pamatnostādnēs 2/2018 par Regulas 2016/679 49. pantā ietvertajām atkāpēm.
[10] Sk. EDAK Pamatnostādnes 2/2018 par Regulas 2016/679 49. pantā ietvertajām atkāpēm, 10. lpp.
[11] Sk. EDAK Pamatnostādnes par Regulas 2016/679 49. pantā ietvertajām atkāpēm, 5. lpp.
[12] Sk. arī VDAR 108. apsvērumu.
[13] Sk. arī terminu "valsts sektora iestāde" un "publisko tiesību subjekts" definīciju 2. panta 1. un 2. punktā Eiropas Parlamenta un Padomes Direktīvā 2003/98/EK (2003. gada 17. novembris) par valsts sektora informācijas atkalizmantošanu (OV L 345, 31.12.2003., 90. lpp.).

organizācija" ir organizācija un tai pakārtotas struktūras, kas ir starptautisko publisko tiesību subjekti, vai jebkura cita struktūra, kas ir izveidota ar divu valstu nolīgumu vai uz tā pamata.

9. EDAK atgādina, ka VDAR piemēro, neskarot starptautisko tiesību normas, piemēram, tās, kas reglamentē starptautisko organizāciju privilēģijas un neaizskaramību. Vienlaikus ir svarīgi arī atgādināt, ka ikvienai EEZ publiskajai iestādei, kas nosūta datus starptautiskajām organizācijām, ir jāievēro VDAR noteikumi par datu nosūtīšanu trešām valstīm vai starptautiskajām organizācijām[14].

2. VISPĀRĪGI IETEIKUMI ATTIECĪBĀ UZ ATBILSTOŠĀM GARANTIJĀM SASKAŅĀ AR VDAR 46. PANTA 2. PUNKTA A) APAKŠPUNKTU UN 46. PANTA 3. PUNKTA B) APAKŠPUNKTU

10. Atšķirībā no Direktīvas 95/46/EK 26. panta 2. punkta VDAR 46. pantā ir paredzētas atbilstošas papildu garantijas, uz kuru pamata notiek datu nosūtīšana starp publiskajām iestādēm:

    i) juridiski saistošs un tiesiski īstenojams instruments, VDAR 46. panta 2. punkta a) apakšpunkts, vai
    ii) noteikumi, kuri iekļaujami administratīvajās vienošanās, VDAR 46. panta 3. punkta b) apakšpunkts.

    Šie instrumenti un vienošanās var būt divpusēji vai daudzpusēji.

11. Nākamajā iedaļā ir sniegti daži vispārīgi ieteikumi, kas palīdzēs nodrošināt, lai publisko iestāžu savstarpēji noslēgtie juridiski saistošie instrumenti vai administratīvās vienošanās (turpmāk – "starptautiski nolīgumi") atbilstu VDAR.

12. Lai arī VDAR 46. pantā un 108. apsvērumā nav sniegtas īpašas norādes par to, kādas garantijas ir jāietver šādos starptautiskajos nolīgumos, ņemot vērā VDAR 44. pantu[15] un EST neseno judikatūru[16], EDAK ir izstrādājusi minimālo garantiju sarakstu, kuras publiskajām iestādēm ir jāiekļauj savos starptautiskajos nolīgumos un uz kurām attiecas VDAR 46. panta 2. punkta a) apakšpunkts vai 46. panta 3. punkta b) apakšpunkts. Šo garantiju mērķis ir nodrošināt, ka VDAR noteiktais fizisko personu aizsardzības līmenis nemazinās, kad šo personu dati tiek nosūtīti uz valstīm ārpus EEZ, un ka datu subjektiem tiek nodrošināts aizsardzības līmenis, kas būtībā ir līdzvērtīgs tam, kāds ir garantēts Savienībā ar VDAR[17].

13. Saskaņā ar EST neseno judikatūru[18] dalībvalsts nosūtītājai publiskajai iestādei – vajadzības gadījumā ar saņēmējas publiskās iestādes atbalstu – ir jānovērtē, vai trešā valstī tiek ievērots Savienības tiesībās noteiktais aizsardzības līmenis, lai noteiktu, vai praksē var izpildīt starptautiskajā nolīgumā iekļautās garantijas, ņemot vērā, ka mijiedarbība ar trešās valsts tiesību aktiem var ietekmēt šo garantiju izpildi.

[14] Sk. EDAK Pamatnostādnes 3/2018 par VDAR teritoriālo darbības jomu, 23. lpp.
[15] VDAR 44. pantā ir noteikts: "*Piemēro visus šīs nodaļas noteikumus, lai nodrošinātu, ka nemazinās ar šo regulu garantētais fizisku personu aizsardzības līmenis.*"
[16] EST 2020. gada 16. jūlija spriedums lietā C-311/18, *Data Protection Commissioner* pret *Facebook Ireland Ltd.* un *Maximillian Schrems* (*Schrems II*).
[17] EST 2020. gada 16. jūlija spriedums lietā C-311/18, *Data Protection Commissioner* pret *Facebook Ireland Ltd.* un *Maximillian Schrems* (*Schrems II*), 105. punkts.
[18] Turpat.

14. Šajā saistībā būtu arī jāatzīmē, ka, tiecoties nodrošināt šajās pamatnostādnēs uzskaitītās garantijas, starptautiskos nolīgumus var izstrādāt, pamatojoties uz jau spēkā esošiem trešās valsts tiesību vai starptautiskas organizācijas iekšējo noteikumu / tiesiskā regulējuma elementiem.

2.1 Nolūks un darbības joma

15. Starptautiskajos nolīgumos būtu jādefinē to darbības joma un būtu skaidri un konkrēti jānosaka to nolūks. Turklāt būtu skaidri jānorāda, kādu kategoriju personas dati tiek skarti un kādā veidā tiek apstrādāti personas dati, kas tiek nosūtīti un apstrādāti saskaņā ar nolīgumu.

2.2 Definīcijas

16. Starptautiskajos nolīgumos būtu jāiekļauj konkrētajam nolīgumam atbilstošo personas datu pamatjēdzienu un tiesību definīcijas saskaņā ar VDAR. Piemēram, ja nolīgumos ir minēti tādi svarīgi termini kā "personas dati", "personas datu apstrāde", "datu pārzinis", "datu apstrādātājs", "saņēmējs" un "sensitīvi dati", būtu jāsniedz to definīcija.

2.3 Datu aizsardzības principi

17. Starptautiskajos nolīgumos īpaši formulē prasību, ka datu aizsardzības pamatprincipi ir jāievēro abām pusēm.

2.3.1. Nolūka ierobežošanas princips

18. Starptautiskajos nolīgumos ir jānorāda, ar kādu nolūku personas dati tiek nosūtīti un apstrādāti, tostarp kādi ir atbilstoši to turpmākās apstrādes nolūki, kā arī ir jānodrošina, ka netiks veikta datu turpmāka apstrāde neatbilstošos nolūkos. Atbilstošs nolūks var būt datu saglabāšana, lai tos arhivētu sabiedrības interesēs, kā arī to apstrāde zinātniskās vai vēstures izpētes nolūkos vai statistikas nolūkos. Lai būtu lielāka skaidrība, ieteicams starptautiskā nolīguma tekstā uzskaitīt konkrētos datu apstrādes un nosūtīšanas nolūkus.

19. Lai izvairītos no tā, ka funkcijas kļūst pārāk izplūdušas, nolīgumos būtu arī jānorāda, ka nosūtītos datus drīkst izmantot tikai nolīgumā skaidri norādītos nolūkos, izņemot, kā norādīts nākamajā punktā.

20. Ja abas starptautiskā nolīguma puses vēlas ļaut, lai saņēmēja publiskā iestāde nosūtītos personas datus izmanto vēl kādā citā atbilstošā veidā, šī saņēmēja iestāde drīkst tos turpmāk izmantot tikai tad, ja tas atbilst sākotnējam nolūkam un ja par to ir iepriekš informēta datus sūtījusī publiskā iestāde, kas īpašu iemeslu dēļ var tam iebilst.

2.3.2. Datu precizitātes un minimizēšanas princips

21. Starptautiskajā nolīgumā ir jānorāda, ka nosūtītajiem un turpmāk apstrādātajiem datiem ir jābūt adekvātiem, atbilstīgiem un jāietver tikai tas, kas nepieciešams to nosūtīšanas un turpmākas apstrādes nolūkos.

22. Šis datu minimizēšanas princips praksē ir svarīgs, lai netiktu nosūtīti neatbilstīgi vai pārmērīgi personas dati.

23. Turklāt datiem būtu jābūt precīziem un atjauninātiem, ņemot vērā to apstrādes nolūkus. Tādēļ starptautiskajā nolīgumā ir jāparedz, ka datu sūtītāja iestāde nodrošina, ka visi saskaņā ar līgumu nosūtītie dati ir precīzi un attiecīgā gadījumā – atjaunināti. Turklāt nolīgumā būtu jāparedz, ka gadījumā, ja viena puse ir konstatējusi, ka ir nosūtīti vai tiek apstrādāti neprecīzi vai novecojuši dati, tai

ir nekavējoties jāinformē otra puse. Visbeidzot, nolīgumā būtu jāparedz, ka gadījumā, ja ir gūts apliecinājums, ka nosūtītie vai apstrādātie dati ir neprecīzi, tai pusei, kas apstrādā šos datus, ir jāveic visi saprātīgi pasākumi, lai izlabotu vai dzēstu šo informāciju.

2.3.3. Uzglabāšanas ierobežojuma princips

24. Pusēm ir jānodrošina, ka starptautiskajā nolīgumā ir iekļauta datu glabāšanas klauzula. Tajā būtu jo īpaši jānorāda, ka personas datus neuzglabā uz neierobežotu laiku, bet tur tādā veidā, lai datu subjektus varētu identificēt tikai tik ilgi, cik tas ir bijis nepieciešams datu nosūtīšanas un turpmākās apstrādes nolūkos. Tostarp datus var uzglabāt tik ilgi, cik nepieciešams arhivēšanai sabiedrības interesēs, zinātniskās un vēstures izpētes nolūkos vai statistikas nolūkos, ar nosacījumu, ka ir īstenoti atbilstoši tehniskie un organizatoriskie pasākumi, lai aizsargātu datu subjektu tiesības un brīvības, piemēram, papildu tehniskie pasākumi (piemēram, drošības pasākumi, pseidonimizācija) un piekļuves ierobežojumi. Ja maksimālais datu glabāšanas laiks nav jau noteikts valsts tiesību aktos vai starptautiskas organizācijas iekšējos noteikumos / tiesiskajā regulējumā, šis laiks būtu jānorāda nolīguma tekstā.

2.3.4. Datu drošība un konfidencialitāte

25. Pusēm būtu jāapņemas nodrošināt nosūtīto un apstrādāto personas datu drošību un konfidencialitāti. Proti, pusēm būtu jāapņemas īstenot atbilstošus tehniskos un organizatoriskos pasākumus, lai aizsargātu pret nejaušu vai nelikumīgu piekļuvi personas datiem, datu iznīcināšanu, nozaudēšanu, pārveidošanu vai neatļautu izpaušanu. Šie pasākumi varētu būt, piemēram, šifrēšana, tostarp nosūtīšanas laikā, pseidonimizācija, marķējums, kas norāda, ka personas dati ir nosūtīti no EEZ, piekļuves personas datiem ierobežošana, personas datu droša uzglabāšana vai tādas politikas īstenošana, kas izstrādāta, lai nodrošinātu personas datu turēšanas drošību un konfidencialitāti.
Nosakot drošības līmeni, būtu jāņem vērā riski, jaunākie tehniskie sasniegumi un saistītās izmaksas.

26. Starptautiskajā nolīgumā var arī paredzēt, ka gadījumā, ja viena no pusēm uzzina par personas datu pārkāpumu, tā iespējami drīz informē otru pusi (vai puses) un ar saprātīgiem un atbilstošiem līdzekļiem novērš personas datu pārkāpumu un mazina iespējamās nelabvēlīgās sekas, tostarp, bez nepamatotas kavēšanās sazinoties ar datu subjektu, kura personas datu pārkāpums ir noticis, ja šis pārkāpums varētu radīt augstus fiziskas personas tiesību un brīvību apdraudējumus.
Starptautiskajā nolīgumā ieteicams norādīt, cik ilgā laikā ir jāpaziņo par personas datu pārkāpumu, kā arī noteikt datu subjekta informēšanas procedūras.

2.4 Datu subjektu tiesības

27. Starptautiskajā nolīgumā ir jānodrošina īstenojamas un efektīvas datu subjekta tiesības, kā noteikts VDAR 46. panta 1. punktā un 108. apsvērumā.

28. Nolīgumā būtu jāuzskaita datu subjektiem pieejamās tiesības, tostarp konkrētas saistības, ko puses ir uzņēmušās šo tiesību nodrošināšanai. Lai to īstenošana būtu efektīva, starptautiskajā nolīgumā ir jāparedz pasākumi, kas nodrošina šo tiesību piemērošanu praksē. Turklāt datu subjekta tiesību pārkāpuma gadījumā ir jānodrošina atbilstīgi tiesiskās aizsardzības līdzekļi.

2.4.1. Tiesības uz pārredzamību

29. Pusēm ir jānodrošina, ka starptautiskajā nolīgumā ir skaidri formulētas pušu saistības nodrošināt pārredzamību.

30. No vienas puses, būtu jāiekļauj vispārīgs informatīvs paziņojums, norādot vismaz informāciju par to, kā un kāpēc publiskās iestādes drīkst apstrādāt un nosūtīt personas datus, kādus attiecīgos rīkus izmanto nosūtīšanai, kurām struktūrvienībām šos datus var nosūtīt, kādas ir datu subjektu tiesības un piemērojamie ierobežojumi, pieejamie tiesiskās aizsardzības mehānismi un kontaktinformācija pretenzijas vai prasības iesniegšanai.

31. Tomēr ir svarīgi atgādināt, ka nosūtītājai publiskajai iestādei nepietiek vien norādīt vispārīgu informāciju savā tīmekļa vietnē. Nosūtītājai publiskajai iestādei būtu jānodrošina, ka datu subjektiem tiek sniegta individuāla informācija saskaņā ar VDAR 13. un 14. pantā noteiktajām paziņošanas prasībām[19].
Starptautiskajā nolīgumā var iekļaut arī dažus izņēmumus attiecībā uz šīs individuālās informācijas sniegšanu. Šie izņēmumi ir ierobežoti, un tiem būtu jāsaskan ar VDAR 14. panta 5. punkta nosacījumiem, piemēram, informāciju var nesniegt, ja tā jau ir datu subjekta rīcībā vai ja šādas informācijas sniegšana nav iespējama vai tā prasītu nesamērīgi lielas pūles.

32. Pusēm ir jānodrošina, ka starptautiskais nolīgums ir pieejams datu subjektiem pēc pieprasījuma un ka starptautiskais nolīgums vai attiecīgie noteikumi, kas sniedz atbilstošās garantijas, ir publiski pieejami pušu tīmekļa vietnē. Starptautiskā nolīguma tekstu pirms publiskošanas vai tā kopijas nosūtīšanas var rediģēt, ciktāl tas nepieciešams, lai aizsargātu sensitīvu vai citu konfidenciālu informāciju. Lai datu subjekts varētu saprast starptautiskā nolīguma saturu, vajadzības gadījumā pusēm ir jāsniedz nolīguma jēgpilns kopsavilkums.

2.4.2. Tiesības uz piekļuvi datiem, to labošanu, dzēšanu, apstrādes ierobežošanu un tiesības iebilst

33. Starptautiskajos nolīgumos būtu jāgarantē, ka datu subjektam ir tiesības iegūt informāciju par visiem ar viņu saistītajiem personas datiem, kas tiek apstrādāti, tiesības piekļūt šiem datiem, kā arī tiesības uz to labošanu, dzēšanu un apstrādes ierobežojumiem un attiecīgā gadījumā tiesības iebilst pret datu apstrādi, pamatojoties uz datu subjekta konkrēto situāciju.

34. Attiecībā uz piekļuves tiesībām starptautiskajos nolīgumos būtu jānorāda, ka ikvienai fiziskai personai ir jābūt tiesīgai no saņēmējas publiskās iestādes iegūt apstiprinājumu par savu personas datu apstrādāšanu vai neapstrādāšanu un, ja dati tiek apstrādāti, ir jābūt tiesīgai piekļūt šiem datiem, kā arī saņemt konkrētu informāciju saistībā ar datu apstrādi, tostarp uzzināt, kāds ir datu apstrādes nolūks, kādu kategoriju personas dati ir apstrādāti, kādiem saņēmējiem personas dati ir izpausti, cik ilgi tos ir paredzēts saglabāt un kādas ir tiesiskās aizsardzības iespējas.

35. Nolīgumā būtu arī jānorāda, kādos gadījumos var izmantot šīs tiesības, un jāietver kārtība, kā datu subjekti var īstenot šīs savas tiesības attiecībā pret abām nolīguma pusēm un kā tām uz šiem pieprasījumiem ir jāreaģē. Piemēram, attiecībā uz datu dzēšanu starptautiskajā nolīgumā varētu norādīt, ka dati ir jādzēš, ja informācija ir apstrādāta nelikumīgi vai ja to vairs nav nepieciešams apstrādāt. Turklāt starptautiskajā nolīgumā būtu jānorāda, ka nolīguma puses pamatotā veidā un savlaicīgi reaģēs uz datu subjektu pieprasījumiem. Starptautiskajā nolīgumā var arī norādīt, ka nolīguma puses atbilstoši rīkojas, piemēram, iekasē saprātīgas nodevas, kas sedz administratīvās izmaksas, ja datu subjektu pieprasījumi ir acīmredzami nepamatoti vai pārmērīgi, jo īpaši, ja tie tiek iesniegti atkārtoti.

[19] Sk. EDAK Pamatnostādnes par Regulā 2016/679 paredzēto pārredzamību, WP 260, rev. 01, 13.–22. lpp.

36. Starptautiskajā nolīgumā būtu arī jāparedz, ka nosūtītājai publiskajai iestādei ir pienākums bez nepamatotas kavēšanās un saprātīgā termiņā (piemēram, viens mēnesis) informēt datu subjektu pēc viņa personas datu nosūtīšanas par to, kādas darbības ir veiktas pēc šīs personas pieprasījuma saskaņā ar tai starptautiskajā nolīgumā noteiktajām tiesībām. Visbeidzot, ja nolīguma puses nav veikušas darbības, reaģējot uz datu subjekta pieprasījumu, tām bez kavēšanās un saprātīgā termiņā (piemēram, viens mēnesis pēc pieprasījuma saņemšanas) būtu jāinformē datu subjekts par šādas rīcības iemesliem un par iespēju iesniegt sūdzību un vērsties tiesā.

37. Starptautiskajā nolīgumā var ietvert arī šo tiesību izņēmumus. Piemēram, var iekļaut VDAR 15. panta 4. punktā un 17. panta 3. punktā noteiktos izņēmumus attiecībā uz piekļuves tiesībām un dzēšanu. Var paredzēt arī individuālo tiesību izņēmumus gadījumos, ja personas datus apstrādā zinātniskos vai vēstures izpētes nolūkos, statistikas nolūkos vai arhivēšanas nolūkos, ciktāl šo tiesību īstenošana varētu padarīt neiespējamu šo konkrēto mērķu sasniegšanu vai būtiski tos ietekmēt, un ar nosacījumu, ka ir nodrošinātas pienācīgas garantijas (piemēram, tehniskie un organizatoriskie pasākumi, tostarp pseidonimizācija). Visbeidzot, nolīgumā var paredzēt, ka puses var noraidīt pieprasījumu rīkoties, ja tas ir acīmredzami nepamatots vai pārmērīgs.

2.4.3. Automatizēta individuālu lēmumu pieņemšana

38. Starptautiskajos nolīgumos attiecīgajā gadījumā kā vispārējs princips būtu jāiekļauj arī klauzula, ka saņēmēja publiskā iestāde nepieņems lēmumu, pamatojoties vienīgi uz individuālu lēmumu automatizētu pieņemšanu, tostarp profilēšanu, kas rada tiesiskas sekas attiecīgajam datu subjektam vai kā līdzīgi ietekmē šo datu subjektu. Ja datus nosūta arī tāpēc, lai saņēmējai publiskajai iestādei būtu iespēja pieņemt lēmumus, pamatojoties vienīgi uz automatizētu apstrādi VDAR 22. panta nozīmē, tas būtu jādara tikai saskaņā ar starptautiskajā nolīgumā ietvertiem īpašiem nosacījumiem, piemēram, ja no datu subjekta ir iegūta skaidri izteikta piekrišana. Ja lēmums neatbilst šiem nosacījumiem, datu subjektam būtu jābūt tiesīgam tam nepakļauties. Ja ir atļauta automatizēta individuālu lēmumu pieņemšana, starptautiskajā nolīgumā katrā ziņā būtu jānodrošina nepieciešamās garantijas, tostarp tiesības būt informētam par konkrētiem lēmumu pieņemšanas iemesliem un loģiku, lai izlabotu neprecīzu vai nepilnīgu informāciju, apstrīdētu lēmumu un lai panāktu cilvēka iejaukšanos.

2.4.4. Tiesības uz tiesisko aizsardzību

39. Datu subjektam garantētajām tiesībām ir jābūt īstenojamām un efektīvām. Tāpēc datu subjektam ir jābūt iespējai saņemt tiesisko aizsardzību. Šo pamatnostādņu 2.7. un 3. iedaļā ir sniegti vairāki piemēri, kādā veidā piedāvāt šos tiesiskās aizsardzības mehānismus.

2.4.5. Datu subjektu tiesību ierobežojumi

40. Starptautiskajā nolīgumā var norādīt arī datu subjektu tiesību ierobežojumus. Šiem ierobežojumiem būtu jāatbilst VDAR 23. pantā noteiktajiem ierobežojumiem. Ierobežojumam ir jābūt tādam, kas ir demokrātiskā sabiedrībā nepieciešams un samērīgs, lai garantētu sabiedrības interesēm svarīgus mērķus, kas uzskaitīti VDAR 23. panta 1. punktā, tostarp citu personu tiesību un brīvību aizsardzību, valsts drošību, aizsardzību vai noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu vai saukšanu pie atbildības par tiem. Ierobežojums ir jānosaka ar likumu vai – starptautiskas organizācijas gadījumā – ar piemērojamajiem iekšējiem noteikumiem / tiesisko regulējumu, un to turpina tik ilgi, kamēr pastāv tā piemērošanas iemesls.

2.5 Datu tālākas nosūtīšanas un to apmaiņas (tostarp izpaušanas un valdības piekļuves) ierobežojumi

41. Starptautiskajā nolīgumā principā būtu īpaši jāparedz, ka saņēmēja publiskā iestāde vai starptautiskā organizācija nedrīkst sūtīt tālāk datus citiem saņēmējiem, kuriem nolīgums nav saistošs. Atkarībā no darbības priekšmeta un konkrētajiem apstākļiem nolīguma puses var uzskatīt, ka ir nepieciešams atļaut tālāku nosūtīšanu. Šajā gadījumā saskaņā ar nosacījumu, ka tiek ievērots nolūka ierobežojuma princips[20], starptautiskajā nolīgumā būtu jāparedz, ka datus var tālāk nosūtīt tikai tad, ja nosūtītāja publiskā iestāde ir iepriekš devusi skaidru atļauju un saņēmējas trešās personas ir apņēmušās ievērot tādus pašus datu aizsardzības principus un garantijas, kādi ir iekļauti starptautiskajā nolīgumā. Būtu jāietver apņemšanās nodrošināt datu subjektiem tādas pašas datu aizsardzības tiesības un garantijas, kādas ir iekļautas starptautiskajā nolīgumā, lai nodrošinātu, ka datu aizsardzības līmenis nepasliktināsies, ja dati tiks nosūtīti tālāk.

42. Principā tālākai nosūtīšanai piemērojamās garantijas būtu piemērojamas arī personas datu apmaiņai valsts iekšienē, t. i., starptautiskajos nolīgumos nedrīkstētu pieļaut datu turpmāku apmaiņu un attiecībā uz to izņēmumi kopumā būtu pieļaujami vienīgi tad, ja nosūtītāja publiskā iestāde ir devusi iepriekšēju un skaidru atļauju un saņēmējas trešās personas ir apņēmušās ievērot tādus pašus datu aizsardzības principus un garantijas, kādi ir iekļauti starptautiskajā nolīgumā.

43. Saņēmējai publiskajai iestādei vai starptautiskajai organizācijai, pirms tā pieprasa nosūtītājai publiskajai iestādei skaidru atļauju, ieteicams sniegt pietiekamu informāciju par to, kāda veida personas datus tā plāno nosūtīt (vai ar tiem apmainīties), kādu iemeslu dēļ vai kādiem nolūkiem tā uzskata par nepieciešamu personas datu nosūtīšanu vai apmaiņu un kurām valstīm vai starptautiskajām organizācijām tā plāno pārsūtīt personas datus, – tas ļaus novērtēt trešās valsts tiesību aktus vai starptautisko organizāciju piemērotos iekšējos noteikumus vai tiesisko regulējumu.

44. Gadījumā, ja atļauja ir nepieciešama, lai veiktu personas datu apmaiņu ar trešo personu, kas atrodas tajā pašā valstī, kurā atrodas saņēmēja publiskā iestāde vai cita starptautiskā organizācija, šādu apmaiņu drīkst atļaut īpašos gadījumos vai nu ar nosūtītājas publiskās iestādes iepriekšēju un skaidru atļauju, vai arī ja saņēmēja trešā persona ir sniegusi saistošu apņemšanos ievērot starptautiskajā nolīgumā ietvertos principus un garantijas.

45. Turklāt starptautiskajā nolīgumā varētu noteikt, kādos īpašos ārkārtas apstākļos varētu notikt datu tālāka apmaiņa bez iepriekšējas atļaujas vai minētās apņemšanās saskaņā ar VDAR 49. pantā uzskaitītajām atkāpēm, piemēram, ja šī īpašā datu apmaiņa ir nepieciešama, lai aizsargātu datu subjekta vai citu personu vitālās intereses vai lai celtu, īstenotu vai aizstāvētu likumīgas prasības. Šādi ārkārtas apstākļi varētu rasties arī tad, ja tālāka apmaiņa ir jāveic saskaņā ar saņēmējas puses tiesību aktiem, ja tas nepieciešams tiešā saistībā ar izmeklēšanu/tiesvedību.

46. Iepriekšējā punktā minētajos gadījumos starptautiskajā nolīgumā būtu skaidri jānosaka, kādos īpašos un ārkārtas apstākļos šāda datu apmaiņa ir atļauta. Saņēmējai publiskajai iestādei vai starptautiskajai organizācijai būtu arī pienākums pirms datu apmaiņas veikšanas informēt nosūtītāju publisko iestādi un iekļaut informāciju par to, ar kādiem datiem tā grasās apmainīties, kas ir saņēmēja trešā persona un kāds ir datu apmaiņas tiesiskais pamats. Savukārt nosūtītājai publiskajai iestādei būtu jāreģistrē šādi saņēmējas publiskās iestādes vai starptautiskās organizācijas paziņojumi un jāsniedz šī informācija uzraudzības iestādei pēc tās pieprasījuma. Ja šāda paziņošana pirms datu apmaiņas apdraudēs ar likumu noteikto konfidencialitātes saistību izpildi, piemēram, izmeklēšanas konfidencialitātes

[20] Sk. iepriekš 2.3.1. iedaļu.

nodrošināšanu, šī īpašā informācija būtu jāsniedz iespējami drīzākā laikā pēc datu apmaiņas. Šādā gadījumā būtu regulāri jāsniedz nosūtītājai iestādei vispārīga informācija par noteiktā laikposmā saņemto pieprasījumu veidu, tostarp informācija par to, kādu kategoriju dati ir prasīti, kas ir pieprasījuma iesniedzēja iestāde un kāds ir datu nodošanas tiesiskais pamats.

47. Visos minētajos scenārijos starptautiskajos nolīgumos drīkstētu atļaut tikai personas datu izpaušanu citām tās pašas trešās valsts publiskajām iestādēm, kurā atrodas arī saņēmējas publiskās iestādes, nepārsniedzot to, kas ir nepieciešams un samērīgs demokrātiskā sabiedrībā, lai aizsargātu nozīmīgus sabiedrības interešu mērķus, kuri uzskaitīti VDAR 23. panta 1. punktā, un saskaņā ar EST judikatūru. Lai uzraudzības nolūkos novērtētu trešās valsts publisko iestāžu iespējamo piekļuvi, nosūtītājai publiskajai iestādei būtu jāņem vērā elementi, kas norādīti četrās Eiropas būtiskajās garantijās[21]. Tostarp personām, kas ir saņēmējas publiskās iestādes datu subjekti trešā valstī, ir jābūt pieejamiem efektīviem tiesiskās aizsardzības līdzekļiem, ja to datiem piekļūst publiskās iestādes[22]. Ja datus nosūta starptautiskām organizācijām, jebkādai šādai piekļuvei ir jānotiek, ievērojot starptautiskās tiesības un jo īpaši neskarot starptautiskās organizācijas privilēģijas un neaizskaramību.

48. Atkarībā no konkrētā gadījuma dažkārt ir lietderīgi prasīt, lai starptautiskajam nolīgumam tiktu pievienots pielikums, kurā uzskaitīti tiesību akti, kas reglamentē datu tālāku apmaiņu ar citām publiskajām iestādēm saņēmējā valstī, tostarp uzraudzības nolūkos. Par visām šāda pielikuma izmaiņām datu nosūtītāja puse būtu jāinformē noteiktā laikposmā.

2.6 Īpašo kategoriju dati

49. Ja saskaņā ar starptautisku nolīgumu ir paredzēts sūtīt īpašo kategoriju personas datus VDAR 9. panta 1. punkta nozīmē, tajā būtu jāiekļauj papildu garantijas, kas jāīsteno saņēmējai publiskajai iestādei vai starptautiskajai organizācijai, lai risinātu īpašus riskus. Šīs papildu garantijas varētu būt, piemēram, piekļuves ierobežojumi, informācijas apstrādes nolūka ierobežojumi, ierobežojumi attiecībā uz tālāku nosūtīšanu utt., vai arī īpašas garantijas, piemēram, papildu drošības pasākumi, kuru veikšanai ir nepieciešams īpaši apmācīt darbiniekus, kuriem ir atļauts piekļūt šai informācijai.

2.7 Tiesiskās aizsardzības mehānismi

50. Lai garantētu datu subjekta tiesību īstenojamību un efektivitāti, starptautiskajā nolīgumā ir jāparedz sistēma, kas ļauj datu subjektiem savās interesēs izmantot tiesiskās aizsardzības mehānismus arī pēc tam, kad to dati ir nosūtīti EEZ nepiederošai trešai valstij vai starptautiskai organizācijai. Šiem tiesiskās aizsardzības mehānismiem ir jānodrošina, ka personas, pret kurām ir neatbilstīgi piemēroti izvēlētā instrumenta noteikumi, var vērsties pēc palīdzības, un tādējādi datu subjektiem, kuru personas dati ir nosūtīti no EEZ, ir iespēja iesniegt sūdzības par šādu neatbilstību un panākt šo sūdzību izskatīšanu. Proti, jānodrošina, ka datu subjekti var efektīvā veidā iesniegt sūdzību publiskajām iestādēm, kas ir starptautiskā nolīguma puses, un (vai nu tieši, vai vēršoties pie attiecīgās puses) neatkarīgam pārraudzības mehānismam. Turklāt principā vajadzētu būt pieejamiem tiesiskās aizsardzības līdzekļiem.

51. Pirmkārt, saņēmējai publiskajai iestādei būtu jāapņemas ieviest mehānismu, kā efektīvi un laikus tiks apstrādātas un risinātas datu subjektu sūdzības par saskaņoto datu aizsardzības garantiju izpildi.

[21] Sk. EDAK Ieteikumus 02/2020 attiecībā uz Eiropas būtiskajām garantijām uzraudzības pasākumiem.
[22] Sk. EDAK Ieteikumus 02/2020, D garantija, 13. un nākamie punkti.

Turklāt datu subjektiem būtu jādod iespēja administratīvā kārtībā efektīvi vērsties pie neatkarīgas pārraudzības iestādes, tostarp pie neatkarīgas datu aizsardzības iestādes, ja tāda ir pieejama[23].

52. Otrkārt, nolīgumā būtu jāparedz tiesiskās aizsardzības līdzekļi, tostarp atlīdzība par materiālo un morālo kaitējumu, kas radies personas datu prettiesiskas apstrādes rezultātā. Ja nav iespējams nodrošināt efektīvu tiesisko aizsardzību, piemēram, valsts tiesību aktos noteikto ierobežojumu vai saņēmējas publiskās iestādes īpašā statusa dēļ (piemēram, tai ir starptautiskas organizācijas statuss), starptautiskajā nolīgumā ir jāparedz alternatīvas garantijas. Šīm alternatīvajām garantijām ir jābūt tādām, lai datu subjektam tiktu sniegtas garantijas, kas būtībā ir līdzvērtīgas Eiropas Savienības Pamattiesību hartas (ES Harta) 47. pantā noteiktajām[24].

53. Šādā gadījumā starptautiskajā nolīgumā varētu izveidot struktūru, kas ļauj datu subjektam īstenot savas tiesības ārpus tiesas, piemēram, izmantojot saistošus tiesai pielīdzināmus mehānismus, piemēram, šķīrējtiesu, vai alternatīvus strīdu izšķiršanas mehānismus, piemēram, mediāciju, kas garantētu neatkarīgu pārskatīšanu un būtu saistoši saņēmējai publiskai iestādei[25]. Turklāt publiskā iestāde, kas nosūta personas datus, varētu uzņemties atbildību par kaitējuma atlīdzināšanu, ja neatkarīgā izvērtēšanā tiek gūts apliecinājums par personas datu prettiesisku apstrādi.
Izņēmuma kārtā nolīgumā var noteikt citus vienlīdz neatkarīgus un efektīvus tiesiskās aizsardzības mehānismus, piemēram, efektīvus tiesiskās aizsardzības mehānismus, kurus īsteno starptautiskas organizācijas.

54. Attiecībā uz visiem minētajiem tiesiskās aizsardzības mehānismiem starptautiskajā nolīgumā būtu jāiekļauj pienākums katrai pusei informēt otru pusi par tiesvedības iznākumu, jo īpaši, ja fiziskās personas sūdzība ir noraidīta vai nav atrisināta.

55. Tiesiskās aizsardzības mehānisms ir jāapvieno ar iespēju nosūtītājai publiskajai iestādei apturēt vai pārtraukt starptautiskajā nolīgumā paredzēto personas datu sūtīšanu, ja puses nav atrisinājušas strīdu izlīguma ceļā, līdz tā uzskata, ka saņēmēja publiskā iestāde ir pienācīgi atrisinājusi strīdus jautājumu. Līdztekus šādai datu sūtīšanas apturēšanai vai pārtraukšanai ir jāparedz, ka saņēmēja publiskā iestāde apņemas nosūtīt atpakaļ vai dzēst personas datus. Nosūtītājas publiskās iestādes pienākums ir informēt valsts kompetento uzraudzības iestādi par to, ka datu sūtīšana tiek apturēta vai pārtraukta.

[23] Sk. arī 2.8. iedaļu par uzraudzības mehānismu.
[24] EST 2020. gada 16. jūlija spriedums lietā C-311/18, *Data Protection Commissioner* pret *Facebook Ireland Ltd.* un *Maximillian Schrems* (*Schrems II*), 96. punkts, 186. un nākamie punkti.
[25] EST 2015. gada 6. oktobra spriedums lietā C-362/14, *Maximillian Schrems* pret *Data Protection Commissioner* (*Schrems*), 41. un 95. punkts; EST 2020. gada 16. jūlija spriedums lietā C-311/18, *Data Protection Commissioner* pret *Facebook Ireland Ltd.* un *Maximillian Schrems* (*Schrems II*), 186., 187., 189. punkts, 195. un nākamie punkti.

2.8 Uzraudzības mehānismi

56. Lai pārliecinātos, ka visas starptautiskajā nolīgumā noteiktās saistības tiek izpildītas, tajā ir jāparedz neatkarīga uzraudzība, kas pārrauga nolīguma pienācīgu piemērošanu un iejaukšanos nolīgumā noteiktajās tiesībās.

57. Pirmkārt, nolīgumā būtu jāparedz iekšējā uzraudzība, lai nodrošinātu nolīguma noteikumu ievērošanu. Katrai nolīguma pusei būtu periodiski jāveic iekšējās pārbaudes, lai pārliecinātos par ieviestajām procedūrām un par nolīgumā noteikto garantiju efektīvu piemērošanu. Periodiskajās iekšējās pārbaudēs būtu jāpārliecinās arī par izmaiņām tiesību aktos, kas varētu liegt pusei (pusēm) ievērot starptautiskajā nolīgumā ietvertos datu aizsardzības principus un noteiktās garantijas. Turklāt nolīgumā varētu paredzēt, ka viena puse var pieprasīt arī otrai pusei veikt šādu pārskatīšanu. Starptautiskajā nolīgumā ir jāparedz prasība, ka nolīguma pusēm ir jāreaģē uz otras puses jautājumiem par nolīgumā noteikto garantiju efektīvu īstenošanu. Nolīguma pusei, kas veic pārskatīšanu, pārbaužu rezultāti būtu jāpaziņo otrai pusei (pusēm). Ideālā gadījumā jāpaziņo būtu arī neatkarīgajam pārraudzības mehānismam, kas reglamentē nolīguma darbību.

58. Turklāt starptautiskajā nolīgumā ir jāparedz, ka nolīguma pusei ir pienākums nekavējoties informēt otru pusi, ja tā kādu iemeslu dēļ nespēj efektīvi īstenot nolīgumā noteiktās garantijas. Šādā gadījumā starptautiskajā nolīgumā ir jāparedz iespēja, ka nosūtītāja publiskā iestāde aptur vai pārtrauc starptautiskajā nolīgumā paredzēto personas datu sūtīšanu saņēmējai publiskajai iestādei līdz brīdim, kad šī saņēmēja iestāde paziņo nosūtītājai iestādei par to, ka atkal spēj rīkoties atbilstoši noteiktajām garantijām. Nosūtītājas iestādes pienākums ir paziņot valsts kompetentajai uzraudzības iestādei par situācijas izmaiņām, kā arī par datu sūtīšanas apturēšanu vai nolīguma izbeigšanu.

59. Otrkārt, nolīgumā ir jāparedz neatkarīga uzraudzība, kas nodrošina, ka nolīguma puses izpilda nolīguma noteikumus. Tas izriet tieši no ES Hartas[26] un Eiropas Cilvēktiesību konvencijas (ECTK)[27] saskaņā ar Eiropas Cilvēktiesību tiesas (ECT) judikatūru un primāro tiesību aktu noteikumiem[28], kā arī saskaņā ar atbilstošo judikatūru.

60. EST kopš 2015. gada[29] ir vairākkārtīgi norādījusi, ka ir nepieciešams neatkarīgs tiesiskās aizsardzības un uzraudzības mehānisms[30]. Līdzīgi ECT savos nolēmumos ir bieži uzsvērusi, ka gadījumā, ja notiek

---

[26] ES Hartas 7., 8. un 47. pants.

[27] ECTK 8. pants.

[28] Lisabonas līguma 6. pants.
"1. *Savienība atzīst tiesības, brīvības un principus, kas izklāstīti 2000. gada 7. decembra Eiropas Savienības Pamattiesību hartā, kura pielāgota Strasbūrā, 2007. gada 12. decembrī, un šai Hartai ir tāds pats juridiskais spēks kā Līgumiem.*
Hartas noteikumi nekādā ziņā nepaplašina Savienības kompetences, kā tās noteiktas Līgumos.
Hartā paredzētās tiesības, brīvības un principus interpretē saskaņā ar Hartas VII sadaļas vispārējiem noteikumiem, ar ko reglamentē tās interpretēšanu un piemērošanu, un pienācīgi ņemot vērā Hartā minētos paskaidrojumus, kuros izklāsta minēto noteikumu pamatu.
2. Savienība pievienojas Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijai. Šī pievienošanās neietekmē Savienības kompetences, kā tās noteiktas Līgumos.
3. Pamattiesības, kas garantētas Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijā un kas izriet no dalībvalstu kopīgajām konstitucionālajām tradīcijām, ir Savienības tiesību vispārīgo principu pamats."

[29] EST 2015. gada 6. oktobra spriedums lietā C-362/14, *Maximillian Schrems* pret *Data Protection Commissioner* (*Schrems*), 41. un 95. punkts.

[30] EST 2017. gada 27. jūlija atzinums 1/15 par nolīgumu starp Eiropas Savienību un Kanādu par pasažieru datu reģistra datu pārsūtīšanu, 2017. gada 26. jūlijs, 228. un nākamie punkti; EST 2019. gada 30. aprīļa atzinums 1/17 par visaptverošo ekonomikas un tirdzniecības nolīgumu starp Kanādu un Eiropas Savienību, 190. un nākamie punkti.

iejaukšanās ECTK 8. pantā noteiktajās tiesībās uz privātās dzīves neaizskaramību, pārraudzības sistēmai ir jābūt efektīvai, neatkarīgai un objektīvai[31].

61. Nolīgumā varētu, piemēram, atsaukties uz pārraudzību, ko īsteno kompetentā uzraudzības iestāde, ja tāda ir valstī, kurā atrodas publiskā iestāde, kas saņem EEZ personas datus, pat ja VDAR nav noteikts, ka kompetentajai uzraudzības iestādei ir jābūt ārējai pārraudzības iestādei. Turklāt nolīgumā varētu iekļaut saņēmējas puses brīvprātīgu apņemšanos sadarboties ar EEZ uzraudzības iestādēm.

62. Ja nav uzraudzības iestādes, kas būtu konkrēti atbildīga par datu aizsardzības likuma uzraudzību trešā valstī vai starptautiskajā organizācijā, neatkarīgs, efektīvs un objektīvs pārraudzības mehānisms ir jānodrošina ar citādiem līdzekļiem. Neatkarīgas uzraudzības mehānisma veids ir atkarīgs no katras konkrētās situācijas.

63. Nolīgumā, piemēram, varētu norādīt trešā valstī esošās pārraudzības iestādes, kas nav uzraudzības iestādes datu aizsardzības jomā. Turklāt, ja nav iespējams strukturāli vai institucionāli nodrošināt ārēju neatkarīgu pārraudzību, piemēram, noteiktu starptautisko organizāciju privilēģiju un neaizskaramības dēļ, šādu pārraudzību varētu nodrošināt, izmantojot funkcionāli autonomus mehānismus. Šim mehānismam ir jābūt tādam, kas, pats par sevi nebūdams ārējs mehānisms, tomēr veic savas funkcijas neatkarīgi, t. i., netiek saņemti norādījumi, ir pietiekami tehniskie, finanšu un cilvēkresursi utt. Jānodrošina, ka saņēmējai pusei šīs pārraudzības iestādes lēmumi ir saistoši.

2.9 Izbeigšanas klauzula

64. Starptautiskajā nolīgumā būtu jāparedz, ka visus personas datus, kas no EEZ ir nosūtīti saskaņā ar šo nolīgumu pirms tā faktiskās izbeigšanas, turpina apstrādāt saskaņā ar starptautiskā nolīguma noteikumiem.

[31] ECT, 1978. gada 6. septembris, *Klass* pret Vāciju, 55. un 56. punkts. Prasība, kas izriet no ECT sprieduma, ir piemērojama arī attiecībā uz iejaukšanos ES Hartas 7. un 8. pantā noteiktajās tiesībās, jo saskaņā ar ES Hartas 52. panta 3. punktu šo pamattiesību nozīme un apjoms ir tāds pats kā ECTK 8. pantā noteiktajām tiesībām.

3. ĪPAŠA INFORMĀCIJA PAR VDAR 46. PANTU

3.1 Īpaša informācija par juridiski saistošiem un tiesiski īstenojamiem instrumentiem – VDAR 46. panta 2. punkta a) apakšpunkts

65. Saskaņā ar VDAR 46. panta 2. punkta a) apakšpunktu EEZ publiskās iestādes var nosūtīt datus publiskajām iestādēm trešā valstī vai starptautiskai organizācijai, pamatojoties uz instrumentiem, ko tās savstarpēji noslēgušas, iepriekš neprasot īpašu atļauju uzraudzības iestādei. Šiem instrumentiem ir jābūt juridiski saistošiem un tiesiski īstenojamiem. Tāpēc saskaņā ar šo noteikumu var izmantot starptautiskus līgumus, publisko tiesību līgumus vai tieši piemērojamus administratīvus nolīgumus.

66. Visos juridiski saistošajos un tiesiski īstenojamajos instrumentos būtu jāiekļauj VDAR prasīto galveno datu aizsardzības principu un datu subjektu tiesību kopums.

67. Nolīguma pusēm ir jāapņemas izstrādāt pienācīgas datu aizsardzības garantijas attiecībā uz datu nosūtīšanu. Tādējādi nolīgumā būtu arī jānosaka, kādā veidā saņēmēja publiskā iestāde piemēros šos galvenos datu aizsardzības pamatprincipus un datu subjektu tiesības visiem nosūtītajiem personas datiem, lai nodrošinātu, ka ar VDAR noteiktais fizisko personu aizsardzības līmenis nesamazinās.

68. Ja juridiski saistošajos un tiesiski īstenojamajos instrumentos nav iespējams nodrošināt efektīvu tiesisko aizsardzību un ir jāvienojas par alternatīvu tiesiskās aizsardzības mehānismu, EEZ publiskajām iestādēm pirms šādu instrumentu noslēgšanas būtu jākonsultējas ar kompetento uzraudzības iestādi.

69. Pat ja instrumenta forma nav izšķiroša, kamēr instruments ir juridiski saistošs un tiesiski īstenojams, EDAK ieskatā labākais risinājums būtu iekļaut sīki izstrādātas datu aizsardzības klauzulas tieši pašā instrumentā. Ja tomēr šāds risinājums nav realizējams konkrētu apstākļu dēļ, EDAK stingri iesaka iekļaut vismaz vispārīgu klauzulu, nosakot datu aizsardzības principus tieši instrumenta tekstā un sīkāk izstrādātus noteikumus un garantijas iekļaujot instrumenta pielikumā.

3.2 Īpaša informācija par administratīvās vienošanās instrumentiem – VDAR 46. panta 3. punkta b) apakšpunkts

70. VDAR 46. panta 3. punkta b) apakšpunktā ir paredzēti arī alternatīvi instrumenti, proti, administratīvas vienošanās, piemēram, saprašanās memorandi, kas nodrošina aizsardzību tādējādi, ka abas puses apņemas īstenot savu kopīgo vienošanos.

71. Šajā saistībā VDAR 46. panta 1. punktā un 108. apsvērumā ir noteikts, ka šādiem vienošanās instrumentiem ir jānodrošina īstenojamas datu subjektu tiesības un efektīvi tiesiskās aizsardzības līdzekļi. Ja garantijas tiek sniegtas juridiski nesaistošos administratīvās vienošanās dokumentos, ir nepieciešams saņemt kompetentās uzraudzības iestādes atļauju.

72. Būtu rūpīgi jāizvērtē, vai izmantot juridiski nesaistošas administratīvas vienošanās, lai nodrošinātu garantijas publiskajā sektorā, ņemot vērā attiecīgo datu būtību un to apstrādes nolūku. Ja trešās valsts tiesību aktos vai starptautiskās organizācijas iekšējos noteikumos / tiesiskajā regulējumā nav noteiktas EEZ fizisko personu datu aizsardzības tiesības un tiesiskā aizsardzība, priekšroka būtu dodama juridiski saistoša nolīguma slēgšanai. Ieviestajiem pasākumiem neatkarīgi no pieņemtā instrumenta veida ir jābūt efektīviem, lai nodrošinātu pienācīgu īstenošanu, izpildes panākšanu un uzraudzību.

73. Noslēdzot administratīvu vienošanos, ir jāveic konkrēti pasākumi, lai nodrošinātu efektīvas individuālās tiesības, tiesisko aizsardzību un pārraudzību. Proti, lai nodrošinātu efektīvas un īstenojamas tiesības, nesaistošajā instrumentā būtu jāiekļauj EEZ personas datu saņēmējas publiskās iestādes garantijas, ka

individuālās tiesības ir pilnībā nodrošinātas šīs iestādes valsts tiesību aktos un ka EEZ fiziskās personas tās var īstenot saskaņā ar tādiem pašiem nosacījumiem, kādi ir piemērojami attiecīgās trešās valsts pilsoņiem un iedzīvotājiem. Tas pats attiecas uz gadījumu, ja EEZ fiziskajām personām ir pieejami administratīvie un tiesiskās aizsardzības līdzekļi saņēmējas publiskās iestādes valsts tiesiskajā regulējumā. Līdzīgi starptautiskajām organizācijām būtu jāsniedz apliecinājumi par individuālajām tiesībām, kas ir paredzētas to iekšējos noteikumos, kā arī par pieejamajiem tiesiskās aizsardzības mehānismiem.

74. Pretējā gadījumā pusēm individuālās tiesības būtu jāgarantē ar īpašām saistībām, ko uzņēmušās puses, kā arī papildus būtu jāparedz procesuāli mehānismi, kas nodrošinātu to efektivitāti un sniegtu personai tiesisko aizsardzību. Šīm īpašajām saistībām un procesuālajiem mehānismiem ir jābūt tādiem, lai praksē nodrošinātais aizsardzības līmenis būtībā būtu līdzvērtīgs tam, kādu Savienībā garantē ar VDAR. Šādi procesuāli mehānismi var būt, piemēram, pušu apņemšanās savstarpēji informēt par EEZ fizisko personu pieprasījumiem un savlaicīgi risināt strīdus vai prasījumus.

75. Turklāt, ja šādus strīdus vai prasījumus puses nevar pašas atrisināt izlīguma ceļā, jānodrošina, ka fiziskai personai tiek sniegta neatkarīga un efektīva tiesiskā aizsardzība ar alternatīviem mehānismiem, piemēram, fiziskai personai tiek dota iespēja izmantot alternatīvu strīda risināšanas mehānismu, piemēram, šķīrējtiesu vai mediāciju. Šādam alternatīvam strīdu izšķiršanas mehānismam ir jābūt saistošam[32].

76. Katrā konkrētajā gadījumā administratīvās vienošanās dokumentā būtu jāsniedz visu vai dažu minēto pasākumu apvienojums, lai nodrošinātu efektīvu tiesisko aizsardzību. Pieļaujami ir arī citi pasākumi, kas nav iekļauti šajās pamatnostādnēs, ja vien tie nodrošina neatkarīgu un efektīvu tiesisko aizsardzību.

77. Katru administratīvo vienošanos, kas izstrādāta saskaņā ar VDAR 46. panta 3. punkta b) apakšpunktu, katrā atsevišķajā gadījumā izvērtēs kompetentā uzraudzības iestāde, attiecīgā gadījumā ievērojot attiecīgo EDAK procedūru. Kompetentā uzraudzības iestāde savu izvērtējumu veiks, pamatojoties uz šajās pamatnostādnēs sniegtajiem vispārējiem ieteikumiem, taču īpašos gadījumos tā var prasīt sniegt arī lielākas garantijas.

[32] EST 2020. gada 16. jūlija spriedums lietā C-311/18, *Data Protection Commissioner* pret *Facebook Ireland Ltd.* un *Maximillian Schrems* (*Schrems II*), 189. punkts, 196. un nākamie punkti.

4. PROCESUĀLI JAUTĀJUMI

78. Administratīvas vienošanās, kas noslēgtas saskaņā ar VDAR 46. panta 3. punkta b) apakšpunktu, tiks izvērtētas katrā atsevišķajā gadījumā, ņemot vērā, ka ir jāsaņem atļauja no kompetentās uzraudzības iestādes, kura saskaņā ar VDAR 46. panta 4. punktu piemēro VDAR 64. panta 2. punktā noteikto konsekvences mehānismu. Kad alternatīvie tiesiskās aizsardzības mehānismi tiek iekļauti VDAR 46. panta 2. punkta a) apakšpunktā noteiktajos saistošajos un īstenojamajos instrumentos, EDAK iesaka konsultēties arī ar kompetento uzraudzības iestādi. EDAK stingri iesaka konsultēties ar kompetento uzraudzības iestādi procesa sākumposmā.

Eiropas Datu aizsardzības kolēģijas vārdā –

priekšsēdētāja

(*Andrea Jelinek*)