Rekomendacijos

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Ieteikumi 01/2020 pasākumiem, kas papildina nosūtīšanas rīkus nolūkā nodrošināt atbilstību ES persondatu aizsardzības līmenim

Pieņemti 2020. gada 10. novembrī

Kopsavilkums

ES Vispārīgā datu aizsardzības regula (VDAR) tika pieņemta divējādam mērķim: atvieglot persondatu brīvu plūsmu Eiropas Savienībā, vienlaikus saglabājot personu pamattiesības un brīvības, jo īpaši viņu tiesības uz persondatu aizsardzību.

Nesenajā spriedumā lietā C-311/18 (*Schrems* II) Eiropas Savienības Tiesa (EST) mums atgādina, ka persondatu aizsardzībai Eiropas Ekonomikas zonā (EEZ) ir jāiet līdzi datiem, lai kur tie nonāktu. Persondatu nosūtīšana uz trešām valstīm nevar būt līdzeklis EEZ nodrošinātās aizsardzības apdraudēšanai vai mazināšanai. Tiesa to arī nosaka, paskaidrojot, ka aizsardzības līmenim trešās valstīs nav jābūt identiskam EEZ garantētajam, bet būtībā līdzvērtīgam. Tiesa arī uztur līguma standartklauzulu kā nosūtīšanas rīku spēkā esību, kas var kalpot, lai ar līgumu nodrošinātu būtībā līdzvērtīgu uz trešām valstīm nosūtīto datu aizsardzību.

Līguma standartklauzulas un citi nosūtīšanas rīki, kas minēti VDAR 46. pantā, nedarbojas vakuumā. Tiesa norāda, ka pārziņi vai apstrādātāji, kas darbojas kā eksportētāji, katrā atsevišķā un attiecīgā gadījumā sadarbībā ar importētāju trešā valstī atbild par pārbaudi, ja trešās valsts tiesību akti vai prakse apdraud atbilstošo garantiju, kas ietvertas VDAR 46. pantā paredzētajos nosūtīšanas rīkos, efektivitāti. Šādos gadījumos Tiesa joprojām atstāj eksportētājiem iespēju ieviest papildinošus pasākumus, kas novērš šīs aizsardzības nepilnības un paaugstina to līdz ES tiesību aktos prasītajam līmenim. Tiesa neprecizē, kādi varētu būt šie pasākumi. Tomēr Tiesa uzsver, ka eksportētājiem tie būs jāidentificē katrā gadījumā atsevišķi. Tas atbilst VDAR 5. panta 2. punkta pārskatatbildības principam, kas nosaka, ka pārziņiem jāatbild un tiem jāspēj pierādīt atbilstība VDAR principiem attiecībā uz persondatu apstrādi.

Lai palīdzētu eksportētājiem (pārziņiem vai apstrādātājiem, privātām vai publiskām struktūrām, kas persondatus apstrādā VDAR piemērošanas jomas ietvaros) sarežģītajā uzdevumā novērtēt trešās valstis un vajadzības gadījumā identificēt atbilstošus papildinošus pasākumus, Eiropas Datu aizsardzības kolēģija (EDAK) ir pieņēmusi šos ieteikumus. Šajos ieteikumos eksportētājiem ir sniegta virkne veicamo darbību, iespējamie informācijas avoti un daži piemēri papildinošiem pasākumiem, kādus var ieviest.

Kā **pirmo soli** EDAK iesaka eksportētājiem **apzināt savu datu nosūtīšanu.** Visas persondatu nosūtīšanas uz trešām valstīm kartēšana var būt sarežģīts uzdevums. Tomēr ir jāzina, kur nonāk persondati, lai nodrošinātu, ka tiem tiek piemērots būtībā līdzvērtīgs aizsardzības līmenis jebkur, kur tos apstrādā. Jums arī jāpārbauda, vai nosūtītie dati ir adekvāti, atbilstīgi un ietver tikai to, kas nepieciešams saistībā ar tiem nolūkiem, kuriem tie tiek nosūtīti un apstrādāti trešā valstī.

Otrais solis ir pārbaudīt **nosūtīšanas rīku, uz kuru balstās nosūtīšana**, starp VDAR V nodaļā uzskaitītajiem. Ja Eiropas Komisija jau ir pasludinājusi valsti, reģionu vai nozari, kurai jūs nosūtāt datus, par atbilstošu, pieņemot vienu no lēmumiem par aizsardzības līmeņa pietiekamību saskaņā ar VDAR 45. pantu vai iepriekšējo Direktīvu 95/46, ciktāl lēmums joprojām ir spēkā, jums nav jāveic nekādas citas darbības, kā tikai pārbaudīt, vai lēmums par aizsardzības līmeņa pietiekamību joprojām ir spēkā. Ja netiek pieņemts lēmums par aizsardzības līmeņa pietiekamību, regulāri un atkārtoti veicot datu nosūtīšanu, jums jāatsaucas uz kādu no VDAR 46. pantā uzskaitītajiem nosūtīšanas rīkiem. Tikai dažos gadījuma rakstura un neatkārtotas nosūtīšanas gadījumos jūs varat atsaukties uz kādu no VDAR 49. pantā paredzētajām atkāpēm, ja atbilstat minētajiem nosacījumiem.

Trešais solis ir novērtēt, vai **trešās valsts tiesību aktos vai praksē** ir kas tāds, kas jūsu konkrētās nosūtīšanas kontekstā var ietekmēt to nosūtīšanas rīku, uz kuriem jūs atsaucaties, atbilstošo garantiju efektivitāti. Novērtējumā jums būtu galvenokārt jāpievēršas trešo valstu tiesību aktiem, kas attiecas uz jūsu veikto nosūtīšanu, un VDAR 46. panta nosūtīšanas rīkam, uz kuru jūs atsaucaties un kurš var mazināt tā aizsardzības līmeni. Lai izvērtētu elementus, kas jāņem vērā, novērtējot trešās valsts tiesību aktus, ar ko reglamentē valsts iestāžu piekļuvi datiem uzraudzības nolūkā, lūdzu, skatiet EDAK Eiropas būtisko garantiju ieteikumus. Tas jo īpaši būtu rūpīgi jāapsver, ja tiesību akti, kas reglamentē valsts iestāžu piekļuvi datiem, ir neskaidri vai nav publiski pieejami. Ja nav tiesību aktu, kas reglamentē apstākļus, kādos valsts iestādes var piekļūt persondatiem, un jūs joprojām vēlaties nosūtīt datus, jums būtu jāizpēta citi būtiski un objektīvi faktori, nevis jāpaļaujas uz subjektīviem faktoriem, piemēram, cik liela ir iespēja, ka valsts iestādes piekļūs jūsu datiem ES standartiem neatbilstīgā veidā. Šis novērtējums būtu jāveic ar pienācīgu rūpību un pamatīgi tas jādokumentē, jo jūs būsiet atbildīgs par lēmumu, kuru pieņemsiet, pamatojoties uz to.

Ceturtais solis ir identificēt un pieņemt papildinošus pasākumus, kas nepieciešami, lai nosūtīto datu aizsardzības līmenis būtu būtiski līdzvērtīgs ES standartam. Šis solis ir nepieciešams tikai tad, ja jūsu novērtējumā tiek konstatēts, ka trešo valstu tiesību akti ietekmē tā VDAR 46. pantā minētā nosūtīšanas rīka efektivitāti, uz kuru jūs atsaucaties vai domājat atsaukties nosūtīšanas kontekstā. Šajos ieteikumos (2. pielikumā) ir neizsmeļošs papildinošu pasākumu piemēru saraksts, kā arī daži nosacījumi, kas nepieciešami to efektivitātes nodrošināšanai. Tāpat kā 46. panta nosūtīšanas rīkos ietverto piemēroto garantiju gadījumā, daži papildinoši pasākumi var būt efektīvi dažās valstīs, taču ne vienmēr citās. Jūs būsiet atbildīgs par to efektivitātes novērtēšanu attiecībā uz nosūtīšanu, ņemot vērā trešo valstu tiesību aktus un nosūtīšanas rīku, uz kuru atsaucaties, un jūs būsiet atbildīgs par pieņemto lēmumu. Šim nolūkam var būt nepieciešams apvienot vairākus papildinošos pasākumus. Jūs galu galā varat secināt, ka neviens papildinošais pasākums nevar nodrošināt būtībā līdzvērtīgu aizsardzības līmeni jūsu konkrētās nosūtīšanas gadījumā. Gadījumā, kad neviens papildinošais pasākums nav piemērots, jums ir jāatturas no nosūtīšanas, jāaptur vai jāizbeidz tā, lai netiktu apdraudēts persondatu aizsardzības līmenis. Šo papildinošo pasākumu novērtējums būtu jāveic ar pienācīgu rūpību un jādokumentē.

Piektais solis ir **veikt** jebkādas **formālas procesuālas darbības**, kas nepieciešamas jūsu papildinošā pasākuma pieņemšanai, atkarībā no VDAR 46. pantā minētā nosūtīšanas rīka, uz kuru atsaucaties. Šajos ieteikumos precizētas šīs formalitātes. Jums var būt jāapspriežas ar kompetentām uzraudzības iestādēm par dažām no šīm darbībām.

Sestais un pēdējais solis būs atbilstošā laika intervālā atkārtoti novērtēt datiem, kurus nosūtāt uz trešām valstīm, nodrošināto aizsardzības līmeni un uzraudzīt, vai ir bijuši vai būs kādi notikumi, kas tos varētu ietekmēt. Pārskatatbildības princips prasa nepārtrauktu modrību attiecībā uz persondatu aizsardzības līmeni.

Uzraudzības iestādes turpinās izmantot savas pilnvaras VDAR piemērošanas uzraudzībai un izpildes panākšanai. Uzraudzības iestādes pievērsīs pienācīgu uzmanību darbībām, kuras eksportētāji veic, lai nodrošinātu, ka viņu nosūtītajiem datiem tiek nodrošināts būtībā līdzvērtīgs aizsardzības līmenis. Kā atgādina Tiesa, uzraudzības iestādes apturēs vai aizliegs datu nosūtīšanu tajos gadījumos, kad izmeklēšanas vai sūdzības rezultātā konstatēs, ka nav iespējams nodrošināt būtībā līdzvērtīgu aizsardzības līmeni.

Uzraudzības iestādes turpinās izstrādāt vadlīnijas eksportētājiem un koordinēt savas darbības EDAK, lai nodrošinātu konsekvenci ES datu aizsardzības tiesību aktu piemērošanā.

Satura rādītājs

Eiropas Datu aizsardzības kolēģija,

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

ņemot vērā Eiropas Ekonomikas zonas (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 Reglamenta 12. un 22. pantu,

tā kā:

(1) Eiropas Savienības Tiesa (EST) savā 2020. gada 16. jūlija spriedumā lietā *Data Protection Commissioner pret Facebook Ireland Ltd, Maximillian Schrems*, C-311/18, secina, ka VDAR 46. panta 1. punkts un 46. panta 2. punkta c) apakšpunkts ir jāinterpretē tādējādi, ka atbilstošām garantijām, īstenojamām tiesībām un efektīviem tiesiskās aizsardzības līdzekļiem, ko pieprasa šie noteikumi, jānodrošina, ka datu subjektiem, kuru persondati tiek nosūtīti uz trešo valsti saskaņā ar standarta datu aizsardzības klauzulām, tiek nodrošināts būtībā līdzvērtīgs aizsardzības līmenis tam, kuru šī regula garantē Eiropas Savienībā, lasot kopā ar Eiropas Savienības Pamattiesību hartu[2].

(2) Kā uzsvēra Tiesa, fizisko personu aizsardzības līmenis, kas būtībā ir līdzvērtīgs VDAR garantētajam Eiropas Savienībā, lasot tos kopā ar Hartu, ir jānodrošina neatkarīgi no V nodaļas noteikumiem, uz kura pamata persondati tiek nosūtīti uz trešo valsti. V nodaļas noteikumu mērķis ir nodrošināt šī augsta līmeņa aizsardzības nepārtrauktību, ja persondati tiek nosūtīti uz trešo valsti[3].

(3) VDAR 108. apsvērumā un 46. panta 1. punktā paredzēts, ka, kamēr ES lēmums par aizsardzības līmeņa pietiekamību nav pieņemts, pārzinim vai apstrādātājam būtu jāveic pasākumi, kas kompensētu datu aizsardzības trūkumus trešā valstī, paredzot atbilstošas garantijas datu subjektam. Pārzinis vai apstrādātājs var nodrošināt atbilstošas garantijas, neprasot īpašu uzraudzības iestādes atļauju, izmantojot kādu no VDAR 46. panta 2. punktā uzskaitītajiem nosūtīšanas rīkiem, piemēram, standarta datu aizsardzības klauzulas.

(4) Tiesa precizē, ka Komisijas pieņemtās standarta datu aizsardzības klauzulas ir paredzētas tikai, lai sniegtu līgumiskās garantijas, kas vienādi piemērojamas visās trešās valstīs Eiropas Savienībā reģistrētiem pārziņiem un apstrādātājiem. Standarta datu aizsardzības klauzulas to līgumiskā rakstura dēļ nav saistošas trešo valstu valsts iestādēm, jo tās nav līgumslēdzējas puses. Līdz ar to datu eksportētājiem, iespējams, jāpapildina šajās standarta datu aizsardzības klauzulās ietvertās garantijas ar papildinošiem pasākumiem, lai nodrošinātu atbilstību ES tiesību aktos noteiktajam aizsardzības

[1] Šajā dokumentā atsauces uz "dalībvalstīm" būtu jāsaprot kā atsauces uz "EEZ dalībvalstīm".
[2] EST 2020. gada 16. jūlija spiedums lietā *Data Protection Commissioner pret Facebook Ireland Ltd, Maximillian Schrems (turpmāk* — C-311/18 (*Schrems* II)), otrais secinājums.
[3] Lieta C-311/18 (*Schrems* II), 92. un 93. punkts.

līmenim konkrētā trešā valstī. Tiesa atsaucas uz VDAR 109. apsvērumu, kurā minēta šī iespēja, un mudina pārziņus un apstrādātājus to izmantot[4].

(5) Tiesa norādīja, ka tieši datu eksportētājam katrā atsevišķā un attiecīgā gadījumā sadarbībā ar datu importētāju jāpārbauda, vai galamērķa trešās valsts tiesību akti nodrošina būtībā līdzvērtīgu persondatu aizsardzības līmenis atbilstīgi ES tiesību aktiem persondatiem, kas nosūtīti saskaņā ar standarta datu aizsardzības klauzulām, vajadzības gadījumā paredzot papildinošus pasākumus tiem, kas piedāvāti šajās klauzulās[5].

(6) Ja Eiropas Savienībā reģistrēts pārzinis vai apstrādātājs nespēj veikt atbilstošus papildinošos pasākumus, lai garantētu būtībā līdzvērtīgu aizsardzības līmeni saskaņā ar ES tiesību aktiem, pārzinim vai apstrādātājam vai, ja tāda nav, kompetentajai uzraudzības iestādei ir jāaptur vai jāpārtrauc persondatu nosūtīšana uz attiecīgo trešo valsti[6].

(7) Ne VDAR, ne Tiesa nenosaka un neprecizē "papildu garantijas", "papildu pasākumus" vai "papildinošos pasākumus" VDAR 46. panta 2. punktā uzskaitīto nosūtīšanas rīku garantijām, kurus pārziņi un apstrādātāji var pieņemt, lai nodrošinātu atbilstību ES tiesību aktos noteiktajam aizsardzības līmenim konkrētā trešā valstī.

(8) EDAK ir nolēmusi pēc savas iniciatīvas izskatīt šo jautājumu un sniegt pārziņiem un apstrādātājiem, kuri darbojas kā eksportētāji, ieteikumus procesam, kuru viņi var izmantot, identificējot un pieņemot papildinošus pasākumus. Šo ieteikumu mērķis ir nodrošināt metodiku eksportētājiem, nosakot, vai un kādi papildinošie pasākumi būtu jāievieš viņu īstenotajai nosūtīšanai. Eksportētāju galvenā atbildība ir nodrošināt, lai nosūtītajiem datiem trešā valstī tiktu nodrošināts tāds aizsardzības līmenis, kas būtībā ir līdzvērtīgs ES garantētajam. Ar šiem ieteikumiem EDAK vēlas sekmēt VDAR un Tiesas nolēmuma konsekventu piemērošanu atbilstoši EDAK pilnvarām[7].

IR PIEŅĒMUSI ŠO IETEIKUMU.

[4] Lieta C-311/18 (Schrems II), 132. un 133. punkts.
[5] Lieta C-311/18 (*Schrems* II), 134. punkts.
[6] Lieta C-311/18 (*Schrems* II), 135. punkts.
[7] VDAR 70. panta 1. punkta e) apakšpunkts.

1 PĀRSKATATBILDĪBA PAR DATU NOSŪTĪŠANU

1. ES primārajos tiesību aktos tiesības uz datu aizsardzību tiek uzskatītas par pamattiesībām[8]. Attiecīgi tiesībām uz datu aizsardzību tiek garantēts augsts aizsardzības līmenis, un ierobežojumus var noteikt tikai tad, ja tie ir paredzēti likumā, ievēro to tiesību būtību, ir samērīgi, nepieciešami un patiesi atbilst vispārējas nozīmes mērķiem, kurus atzīst Savienība, vai nepieciešamībai aizsargāt citu tiesības un brīvības[9]. Tiesības uz persondatu aizsardzību nav absolūtas; tās ir jāņem vērā saistībā ar to funkciju sabiedrībā un jālīdzsvaro ar citām pamattiesībām saskaņā ar proporcionalitātes principu[10].

2. Dati, kas nonāk trešās valstīs ārpus EEZ, jāgarantē būtībā līdzvērtīgs ES garantētajam aizsardzības līmenim, lai nodrošinātu, ka netiek mazināts VDAR garantētais aizsardzības līmenis.

3. Tiesības uz datu aizsardzību ir aktīvas savā raksturā. Tas uzliek pienākumu eksportētājiem un importētājiem (neatkarīgi no tā, vai tie ir pārziņi un/vai apstrādātāji) iet tālāk par šo tiesību atzīšanu vai pasīvu ievērošanu[11]. Pārziņiem un apstrādātājiem jācenšas aktīvi un nepārtraukti nodrošināt atbilstību tiesībām uz datu aizsardzību, īstenojot juridiskus, tehniskus un organizatoriskus pasākumus, kas nodrošina to efektivitāti. Pārziņiem un apstrādātājiem arī jāspēj apliecināt šos centienus datu subjektiem, plašākai sabiedrībai un datu aizsardzības uzraudzības iestādēm. Šis ir tā saucamais pārskatatbildības princips[12].

4. Pārskatatbildības princips, kas nepieciešams, lai nodrošinātu VDAR piešķirtā aizsardzības līmeņa efektīvu piemērošanu, attiecas arī uz datu nosūtīšanu uz trešām valstīm[13], jo tā pati par sevi ir datu apstrādes veids[14]. Kā Tiesa uzsvēra savā spriedumā, aizsardzības līmenis, kas būtībā ir līdzvērtīgs VDAR garantētajam Eiropas Savienībā, lasot tos kopā ar Hartu, ir jānodrošina neatkarīgi no tās nodaļas noteikuma, uz kura pamata persondati tiek nosūtīti uz trešo valsti[15].

5. Spriedumā lietā *Schrems* II Tiesa uzsvēra eksportētāju un importētāju pienākumu nodrošināt, ka persondatu apstrāde tikusi un joprojām tiek veikta atbilstīgi ES datu aizsardzības likumos noteiktajam aizsardzības līmenim, un apturēt nosūtīšanu un/vai izbeigt līgumu, ja datu importētājs neievēro vai vairs nespēj ievērot attiecīgajā līgumā starp eksportētāju un importētāju iekļautās standarta datu aizsardzības klauzulas[16]. Pārzinim vai apstrādātājam, kas darbojas kā eksportētājs, jānodrošina, lai importētāji, pildot šos pienākumus, attiecīgā gadījumā sadarbotos ar eksportētāju, informējot to, piemēram, par jebkādām izmaiņām, kas ietekmē importētāja valstī saņemto persondatu aizsardzības līmeni[17]. Šie pienākumi ir VDAR pārskatatbildības principa piemērošana datu nosūtīšanai[18].

---

[8] Pamattiesību hartas 8. panta 1. punkts un LESD 16. panta 1. punkts, VDAR preambulas 1. apsvērums, 1. panta 2. punkts.

[9] ES Pamattiesību hartas 52. panta 1. punkts.

[10] VDAR 4. apsvērums un spriedums lietā C-507/17 *Google LLC*, kas ir *Google Inc.* tiesību pārņēmēja, pret *Commission nationale de l'informatique et des libertés* (*CNIL*), 60. punkts.

[11] Lietas C-92/09 un C-93/02 *Volker* un *Markus Schencke GbR* pret *Land Hessen*, ģenerāladvokātes *Sharpston* secinājumi, 2010. gada 17. jūnijs, 71. punkts.

[12] VDAR 5. panta 2. punkts un 28. panta 3. punkta h) apakšpunkts.

[13] VDAR 44. pants un 101. apsvērums, kā arī VDAR 47. panta 2. punkta d) apakšpunkts.

[14] EST 2015. gada 6. oktobra spriedums lietā *Maximillian Schrems pret Data Protection Commissioner, (turpmāk* — C-362/14 (*Schrems* I)), 45. punkts.

[15] Lieta C-311/18 (*Schrems* II), 92. un 93. punkts.

[16] Lieta C-311/18 (*Schrems* II), 134., 135., 139., 140., 141. un 142. punkts.

[17] Lieta C-311/18 (*Schrems* II), 134. punkts.

[18] VDAR 5. panta 2. punkts un 28. panta 3. punkta h) apakšpunkts.

2 CEĻVEDIS. PĀRSKATATBILDĪBAS PRINCIPA PIEMĒROŠANA DATU NOSŪTĪŠANAI PRAKSĒ

6. Šeit turpmāk ir sniegts ceļvedis ar soļiem, kas jāveic, lai konstatētu, vai jums (datu eksportētājam) ir jāievieš papildinoši pasākumi likumīgai datu nosūtīšanai ārpus EEZ. "Jūs" šajā dokumentā nozīmē pārzini vai apstrādātāju, kas darbojas kā datu eksportētājs un apstrādā persondatus VDAR piemērošanas jomas ietvaros, tostarp veic datu apstrādi kā privātpersonas un valsts pārvaldes struktūras, nosūtot datus privātām struktūrām[19]. Kas attiecas uz persondatu nosūtīšanu starp valsts pārvaldes struktūrām, īpašas vadlīnijas ir sniegtas *Pamatnostādnēs 2/2020 par Regulas 2016/679 46. panta 2. punkta a) apakšpunktu un 46. panta 3. punkta b) apakšpunktu persondatu nosūtīšanai starp EEZ un ārpus EEZ esošām valsts iestādēm un struktūrām*[20].

7. Jums atbilstoši jādokumentē šis novērtējums un izvēlētie un īstenotie papildinošie pasākumi, kā arī pēc pieprasījuma šāda dokumentācija jādara pieejama kompetentajai uzraudzības iestādei[21].

2.1 1. solis. Apzināt savu datu nosūtīšanu

8. Lai zinātu, kas jums (datu eksportētājam) var būt nepieciešams, lai varētu turpināt vai veikt jaunu persondatu nosūtīšanu[22], vispirms ir jāpārliecinās, ka jūs pilnībā pārzināt savu datu nosūtīšanu (apzināt savu datu nosūtīšanu). Visas nosūtīšanas reģistrēšana un kartēšana var būt sarežģīts uzdevums uzņēmumiem, kuru veiktā datu nosūtīšana uz trešām valstīm ir daudzkārtēja, daudzveidīga un regulāra un kuri izmanto virkni apstrādātāju un apakšapstrādātāju. Savu datu nosūtīšanas apzināšana ir būtisks pirmais solis, lai izpildītu saistības atbilstīgi pārskatatbildības principam.

9. Lai gūtu pilnīgu izpratni par jūsu veikto nosūtīšanu, varat izmantot apstrādes darbību uzskaiti, kuru jums var būt pienākums uzturēt, rīkojoties kā pārzinim vai apstrādātājam saskaņā ar VDAR 30. pantu[23]. Jums var palīdzēt arī iepriekšējās darbības, kas veiktas nolūkā izpildīt pienākumu informēt datu

[19] Skatīt EDAK Pamatnostādnes 3/2018 par VDAR teritoriālo darbības jomu (3. pants) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_lv.

[20] EDAK Pamatnostādnes 2/2020 par Regulas 2016/679 46. panta 2. punkta a) apakšpunktu un 46. panta 3. punkta b) apakšpunktu persondatu nosūtīšanai starp EEZ un ārpus EEZ esošām valsts iestādēm un struktūrām; skatīt https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_lv.

[21] VDAR 5. panta 2. punkts un 24. panta 1. punkts.

[22] Lūdzu, ņemiet vērā, ka trešās valsts struktūras attālinātā piekļuve datiem, kas atrodas EEZ, arī tiek uzskatīta par nosūtīšanu.

[23] Skatīt VDAR 30. pantu un jo īpaši 1. punkta e) apakšpunktu un 2. punkta c) apakšpunktu. Turklāt apstrādes reģistrācijas dokumentos būtu jāietver apstrādes darbību apraksts (tostarp, bet ne tikai, datu subjektu kategorijas, persondatu kategorijas un apstrādes nolūki, kā arī konkrēta informācija par datu nosūtīšanu). Daži pārziņi un apstrādātāji ir atbrīvoti no pienākuma veikt apstrādes uzskaiti (VDAR 30. panta 5. punkts). Vadlīnijas par šādiem atbrīvojumiem skatīt 29. panta darba grupas nostājas dokumentā par atkāpēm no pienākuma uzturēt apstrādes darbību uzskaiti saskaņā ar VDAR 30. panta 5. punktu (EDAK apstiprināja 2018. gada 25. maijā).

subjektus saskaņā ar VDAR 13. panta 1. punkta f) apakšpunktu un 14. panta 1. punkta f) apakšpunktu par viņu persondatu nosūtīšanu uz trešām valstīm[24].

10. Kartējot nosūtīšanu, neaizmirstiet apsvērt arī tālāku nosūtīšanu, piemēram, vai jūsu apstrādātāji ārpus EEZ nosūta persondatus, kurus esat viņiem uzticējis, apakšapstrādātājam citā trešā valstī vai tajā pašā trešā valstī[25].

11. Saskaņā ar VDAR ietverto "datu minimizēšanas" principu[26] jums arī jāpārbauda, vai nosūtītie dati ir adekvāti, atbilstīgi un ietver tikai to, kas nepieciešams to nolūkos, kuriem tie tiek nosūtīti un apstrādāti trešā valstī.

12. Šīs darbības jāveic pirms jebkādas nosūtīšanas veikšanas un jāatjaunina pirms nosūtīšanas atsākšanas pēc datu nosūtīšanas darbību apturēšanas: jums jāzina, kur var atrasties eksportētie persondati vai kur importētāji tos var apstrādāt (galamērķu karte).

13. Paturiet prātā, ka attālināta piekļuve no trešās valsts (piemēram, atbalsta situācijās) un/vai glabāšana mākonī, kas atrodas ārpus EEZ, arī tiek uzskatīta par nosūtīšanu[27]. Precīzāk, ja jūs izmantojat starptautisku mākoņu infrastruktūru, jums jāizvērtē, vai jūsu dati tiks nosūtīti uz trešām valstīm un kur, ja vien mākoņa pakalpojuma sniedzējs savā līgumā nepārprotami nenorāda, ka dati vispār netiks apstrādāti trešās valstīs.

2.2 2. solis. Identificēt nosūtīšanas rīkus, uz kuriem atsaucaties

14. Otrais solis, kas jums jāveic, ir identificēt starp VDAR V nodaļā uzskaitītajiem un paredzētajiem nosūtīšanas rīkiem tos, uz kuriem jūs atsaucaties.

Lēmumi par aizsardzības līmeņa pietiekamību

15. Eiropas Komisija, pieņemot **lēmumus par aizsardzības līmeņa pietiekamību** attiecībā uz noteiktām vai visām trešām valstīm, uz kurām jūs nosūtāt persondatus, var atzīt, ka tās nodrošina atbilstošu persondatu aizsardzības līmeni[28].

16. Šāda lēmuma par aizsardzības līmeņa pietiekamību rezultātā persondati var tikt pārsūtīti no EEZ uz šo trešo valsti, un nav nepieciešami VDAR 46. pantā uzskaitītie nosūtīšanas rīki.

---

[24] Saskaņā ar VDAR pārredzamības noteikumiem jums ir pienākums informēt datu subjektus par persondatu nosūtīšanu uz trešām valstīm (VDAR 13. panta 1. punkta f) apakšpunkts un 14. panta 1. punkta f) apakšpunkts). Jums jo īpaši ir pienākums informēt viņus par to, vai ir pieņemts Eiropas Komisijas lēmums par aizsardzības līmeņa pietiekamību, un nosūtīšanas gadījumā, kas minēts VDAR 46. vai 47. pantā vai VDAR 49. panta 1. punkta otrajā daļā, jānorāda atbilstošas vai piemērotas garantijas un līdzekļi, ar kādiem iegūt to kopiju vai kur tie ir pieejami. Datu subjektam sniegtajai informācijai jābūt pareizai un aktuālai, jo īpaši ņemot vērā Tiesas judikatūru attiecībā uz nosūtīšanu.

[25] Ja pārzinis ir sniedzis iepriekšēju konkrētu vai vispārēju rakstisku atļauju atbilstīgi VDAR 28. panta 2. punktam.

[26] VDAR 5. panta 1. punkta c) apakšpunkts.

[27] Skatīt Bieži uzdoto jautājumu Nr. 11: *"jāņem vērā, ka pat piekļuves nodrošināšana datiem no trešās valsts, piemēram, administratīvos nolūkos, arī ir uzskatāma par nosūtīšanu"*, EDAK, Bieži uzdotie jautājumi par Eiropas Savienības Tiesas spriedumu lietā C-311/18 *Data Protection Commissioner pret Facebook Ireland Ltd* un *Maximillian Schrems*, 2020. gada 23. jūlijs.

[28] Eiropas Komisijai ir tiesības, pamatojoties uz VDAR 45. pantu, noteikt, vai valsts ārpus ES nodrošina pietiekamu datu aizsardzības līmeni. Tāpat Eiropas Komisijai ir pilnvaras noteikt, vai starptautiska organizācija nodrošina pietiekamu aizsardzības līmeni.

17. Lēmumus par aizsardzības līmeņa pietiekamību var attiecināt uz valsti kopumā vai tikai uz tās daļu. Lēmumus par aizsardzības līmeņa pietiekamību var attiecināt uz visu datu nosūtīšanu uz valsti vai arī tos var attiecināt tikai uz noteiktiem nosūtīšanas veidiem (piemēram, vienā sektorā)[29].

18. Eiropas Komisija savā tīmekļa vietnē publicē savu lēmumu par aizsardzības līmeņa pietiekamību sarakstu[30].

19. Ja nosūtāt persondatus uz trešām valstīm, reģioniem vai sektoriem, uz ko attiecina Komisijas lēmumu par aizsardzības līmeņa pietiekamību (ciktāl piemērojams), **jums nav jāveic nekādas turpmākas darbības, kā aprakstīts šajos ieteikumos[31].** Tomēr jums joprojām jāuzrauga, vai lēmumi par aizsardzības līmeņa pietiekamību, kas attiecas uz jūsu veikto nosūtīšanu, netiek atcelti vai atzīti par spēkā neesošiem[32].

20. Tomēr lēmumi par aizsardzības līmeņa pietiekamību neliedz datu subjektiem iesniegt sūdzību. Tie arī neliedz uzraudzības iestādēm celt prasību valsts tiesā, ja tām ir šaubas par lēmuma pamatotību, lai valsts tiesa varētu iesniegt EST lūgumu sniegt prejudiciālu nolēmumu nolūkā pārbaudīt šo lēmumu spēkā esību[33].

Piemērs: ES pilsonis *Schrems* kungs 2013. gada jūnijā iesniedza sūdzību Īrijas Datu aizsardzības komisijā (*DPC*) un lūdza šo uzraudzības iestādi aizliegt vai apturēt viņa persondatu nosūtīšanu no *Facebook Ireland* uz Amerikas Savienotajām Valstīm, jo viņš uzskatīja, ka Amerikas Savienoto Valstu tiesību akti un prakse nenodrošina pietiekamu tās teritorijā esošo persondatu aizsardzību pret valsts iestāžu tur veiktajām uzraudzības darbībām. *DPC* sūdzību noraidīja, pamatojoties jo īpaši uz to, ka Eiropas Komisija Lēmumā 2000/520 uzskatīja, ka "drošības zonas" shēmas ietvaros Amerikas Savienotās Valstis nodrošina atbilstošu nosūtīto persondatu aizsardzības līmeni ("Drošības zonas" lēmums). *Schrems* kungs apstrīdēja *DPC* lēmumu, un Īrijas Augstā tiesa vērsās Eiropas Savienības Tiesā (EST) ar jautājumu par Lēmuma 2000/520 spēkā esību. Pēc tam EST nolēma atzīt par spēku zaudējušu Komisijas Lēmumu 2000/520 par "drošības zonas" privātuma principu sniegtās aizsardzības atbilstību[34].

[29] VDAR 45. panta 1. punkts.

[30] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_lv.

[31] Ja jūs un datu importētājs esat īstenojuši pasākumus, lai izpildītu citas VDAR noteiktās saistības; citādi īstenojiet šos pasākumus.

[32] Eiropas Komisijai periodiski jāpārskata visi lēmumi par aizsardzības līmeņa pietiekamību un jāuzrauga, vai trešās valstis, kuras ir ieguvējas no šiem lēmumiem par aizsardzības līmeņa pietiekamību, joprojām nodrošina pienācīgu aizsardzības līmeni (skatīt VDAR 45. panta 3. punktu un 45. panta 4. punktu). Tāpat EST var atzīt par spēkā neesošiem lēmumus par aizsardzības līmeņa pietiekamību (skatīt tās spriedumus lietās C-362/14 (*Schrems* I) un C-311/18 (*Schrems* II).

[33] Lieta C-311/18 (*Schrems* II), 118. un 120. punkts. Uzraudzības iestādes nedrīkst ignorēt lēmumu par aizsardzības līmeņa pietiekamību un apturēt vai aizliegt persondatu nosūtīšanu uz šādām valstīm, atsaucoties tikai uz aizsardzības līmeņa nepietiekamību. Tās var izmantot savas pilnvaras apturēt vai aizliegt persondatu nosūtīšanu uz šo trešo valsti tikai, pamatojoties uz citiem iemesliem (piemēram, nepietiekami drošības pasākumi, pārkāpjot VDAR 32. pantu, datu apstrādei kā tādai nav juridiska pamata, pārkāpjot VDAR 6. pantu). Uzraudzības iestādes var pilnīgi neatkarīgi pārbaudīt, vai šo datu nosūtīšana atbilst VDAR noteiktajām prasībām, un attiecīgā gadījumā iesniegt prasību valsts tiesā, ja tām ir šaubas par Komisijas lēmuma par aizsardzības līmeņa pietiekamību spēkā esību, lai tālāk vērstos Eiropas Savienības Tiesā ar lūgumu sniegt prejudiciālu nolēmumu nolūkā pārbaudīt lēmuma spēkā esību.

[34] Lieta C-362/14 (*Schrems* I).

VDAR 46. pants — nosūtīšanas rīki

21. VDAR 46. pantā uzskaitīti vairāki nosūtīšanas rīki ar "atbilstošām garantijām", kurus eksportētāji var izmantot persondatu nosūtīšanai uz trešām valstīm gadījumos, kad nav lēmumu par aizsardzības līmeņa pietiekamību. Galvenie VDAR 46. pantā minētie nosūtīšanas rīku veidi ir šādi:

- standarta datu aizsardzības klauzulas (LSK);
- saistoši uzņēmuma noteikumi (SUN);
- rīcības kodeksi;
- sertifikācijas mehānismi;
- *ad hoc* līgumu klauzulas.

22. Neatkarīgi no izvēlētā VDAR 46. panta nosūtīšanas rīka ir jānodrošina, lai nosūtītie persondati kopumā saņemtu būtībā līdzvērtīgu aizsardzības līmeni.

23. VDAR 46. pantā pārsvarā sniegtas līgumiska rakstura atbilstošas garantijas, kuras var izmantot nosūtīšanai uz visām trešām valstīm. Pateicoties situācijai trešā valstī, uz kuru jūs nosūtāt datus, joprojām var būt nepieciešams papildināt šos nosūtīšanas rīkus un garantijas ar papildinošiem pasākumiem ("papildinošie pasākumi"), lai nodrošinātu būtībā līdzvērtīgu aizsardzības līmeni[35].

Atkāpes

24. Papildus lēmumiem par atbilstību un VDAR 46. panta nosūtīšanas rīkiem VDAR pastāv trešā iespēja, kas ļauj nosūtīt persondatus noteiktās situācijās. Ievērojot konkrētus nosacījumus, jūs joprojām varat nosūtīt persondatus, pamatojoties uz VDAR 49. pantā minēto atkāpi.

25. VDAR 49. pantam ir izņēmuma raksturs. Tajā ietvertās atkāpes ir skaidrojamas ierobežoti un galvenokārt attiecas uz apstrādes darbībām, kas ir neregulāras un neatkārtojas. EDAK ir izdevusi Pamatnostādnes 2/2018 par atkāpēm no 49. panta saskaņā ar Regulu 2016/679. [36]

26. Pirms atsaukties uz VDAR 49. pantā paredzēto atkāpi, jums jāpārbauda, vai jūsu veiktā nosūtīšana atbilst stingrajiem nosacījumiem, kurus šis noteikums nosaka katrai atkāpei.

***

27. Ja jūsu veikto nosūtīšanu nav iespējams juridiski pamatot ar lēmumu par aizsardzības līmeņa pietiekamību vai 49. pantā ietverto atkāpi, veiciet 3. soli.

2.3 3. solis. Novērtējiet, vai VDAR 46. pantā minētais nosūtīšanas rīks, uz kuru atsaucaties, ir efektīvs, ņemot vērā visus nosūtīšanas apstākļus

28. VDAR 46. pantā minētā nosūtīšanas rīka izvēle var nebūt pietiekama. Nosūtīšanas rīkam jānodrošina, lai nosūtīšana neietekmētu VDAR garantēto aizsardzības līmeni[37]. Citiem vārdiem sakot, jūsu nosūtīšanas rīkam praksē jābūt efektīvam.

[35] Lieta C-311/18 (*Schrems* II), 130. un 133. punkts. Skatīt arī 2.3. punktu turpmāk.
[36] Vairāk informācijas skatīt https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_lv.
[37] VDAR 44. pants.

29. Efektīvs nozīmē, ka nosūtītajiem persondatiem trešā valstī tiek nodrošināts tāds aizsardzības līmenis, kas būtībā ir līdzvērtīgs EEZ garantētajam[38]. Tas tā nav, ja datu importētājam ir liegts izpildīt savas saistības, kas izriet no izvēlētā VDAR 46. pantā minētā nosūtīšanas rīka nosūtīšanai piemērojamo trešās valsts tiesību aktu un prakses dēļ.

30. Tādēļ attiecīgā gadījumā sadarbībā ar importētāju ir jānovērtē, vai trešās valsts tiesību aktos vai praksē ir kas tāds, kas jūsu konkrētās nosūtīšanas kontekstā var ietekmēt 46. pantā minētā nosūtīšanas rīka, uz kuru jūs atsaucaties, atbilstošo garantiju efektivitāti. Attiecīgā gadījumā jūsu datu importētājam būtu jāsniedz attiecīgie avoti un informācija par trešo valsti, kurā tas ir reģistrēts, un tiesību aktiem, kas piemērojami nosūtīšanai. Jūs varat atsaukties arī uz citiem informācijas avotiem, piemēram, uz tiem, kas uzskaitīti neizsmeļošajā sarakstā 3. pielikumā[39].

31. Novērtējumā būtu jāņem vērā visi nosūtīšanā iesaistītie dalībnieki (piemēram, pārziņi, apstrādātāji un apakšapstrādātāji, kas apstrādā datus trešā valstī), kas identificēti nosūtīšanas kartēšanas uzdevumā. Jo vairāk iesaistīto pārziņu, apstrādātāju vai importētāju, jo sarežģītāks būs jūsu novērtējums. Šajā novērtējumā jums būs jāņem vērā arī jebkāda iespējama tālāko nosūtīšana.

32. Šajā nolūkā jums jāpārbauda katras nosūtīšanas īpašības un jānosaka, kā uz šo nosūtīšanu attiecas tās valsts iekšējais tiesiskais regulējums, uz kuru dati tiek nosūtīti (vai tālāk nosūtīti).

33. Piemērojamais tiesiskais konteksts būs atkarīgs no nosūtīšanas apstākļiem, jo īpaši:

- nolūkiem, kādiem dati tiek nosūtīti un apstrādāti (piemēram, tirgvedība, cilvēkresursi, glabāšana, IT atbalsts, klīniskie pētījumi);
- apstrādē iesaistīto subjektu veidiem (publiski/privāti; pārzinis/apstrādātājs);
- nozares, kurā tiek veikta nosūtīšana (piemēram, adtech, telekomunikāciju, finanšu u. c.);
- nosūtīto persondatu kategorijām (piemēram, persondati, kas attiecas uz bērniem, var ietilpt noteiktu trešo valstu tiesību aktu darbības jomā);
- vai dati tiks glabāti trešā valstī, vai ir tikai nodrošināta attālināta piekļuve datiem, kas glabājas ES/EEZ;
- nosūtāmo datu formāta (t. i., parastā tekstā / pseidonimizēti vai šifrēti40);
- iespējas, ka datus var tālāk nosūtīt no trešās valsts uz citu trešo valsti[41].

34. Piemērojamos tiesību aktos jums būs jāizvērtē, vai tas neietekmē jūsu izvēlētajā VDAR 46. panta nosūtīšanas rīkā ietvertās saistības. Jums būtu jāpārbauda, vai saistības, kas ļauj datu subjektiem īstenot savas tiesības saistībā ar starptautisko nosūtīšanu (piemēram, piekļuves, labošanas un dzēšanas pieprasījumi attiecībā uz nosūtītajiem datiem), var tikt efektīvi piemērotas praksē un vai galamērķa trešās valsts likumi tos nemazina.

35. Jums jānovērtē attiecīgie vispārīgā rakstura noteikumi, ciktāl tie ietekmē VDAR 46. panta nosūtīšanas rīkā ietverto garantiju efektīvu piemērošanu un indivīdu pamattiesības (jo īpaši datu subjekta tiesiskā aizsardzības gadījumā, ja trešo valstu valsts iestādes piekļūst nosūtītajiem datiem).

[38] Lieta C-311/18 (*Schrems* II), 105. punkts un otrais secinājums.
[39] Skatīt arī šeit turpmāk 43. punktu.
[40] Dažas trešās valstis neļauj importēt šifrētus datus.
[41] Ja pārzinis ir sniedzis iepriekšēju konkrētu vai vispārēju rakstisku atļauju atbilstīgi VDAR 28. panta 2. punktam.

36. Jebkurā gadījumā jums būtu jāpievērš īpaša uzmanība visiem attiecīgajiem tiesību aktiem, jo īpaši tiesību aktiem, ar ko nosaka prasības persondatu izpaušanai valsts iestādēm vai piešķir šādām valsts iestādēm pilnvaras piekļūt persondatiem (piemēram, krimināltiesību, regulatīvās uzraudzības un valsts drošības nolūkiem). Ja šīs prasības vai pilnvaras nepārsniedz to, kas ir nepieciešami un samērīgi demokrātiskā sabiedrībā[42], tās nedrīkst ietekmēt VDAR 46. panta nosūtīšanas rīkā, uz kuru jūs atsaucaties, ietvertās saistības.

37. ES standarti, piemēram, ES Pamattiesību hartas 47. un 52. pants, jāizmanto kā atsauce, lai novērtētu, vai šāda valsts iestāžu piekļuve nepārsniedz to, kas ir nepieciešami un samērīgi demokrātiskā sabiedrībā, un vai datu subjektiem tiek nodrošināta efektīva tiesiskā aizsardzība.

38. Veicot šo novērtējumu, jāņem vērā dažādi šīs trešās valsts tiesību sistēmas aspekti, piemēram, būtiski ir arī VDAR 45. panta 2. punktā uzskaitītie elementi[43]. Piemēram, tiesiskuma situācija trešā valstī var būt būtiska, novērtējot pieejamo mehānismu efektivitāti, lai personas varētu saņemt tiesisko aizsardzību (tiesā) pret nelikumīgu valdības piekļuvi persondatiem. Visaptveroša datu aizsardzības likuma vai neatkarīgas datu aizsardzības iestādes esība, kā arī to starptautisko dokumentu ievērošana, ar ko paredz datu aizsardzības garantijas, var palīdzēt nodrošināt valdības iejaukšanās samērīgumu[44].

***

39. EDAK Eiropas būtisko garantiju (EBG) ieteikumos ir iekļauti elementi, kas jāizvērtē, nosakot, vai tiesisko regulējumu, ar ko reglamentē trešo valstu valsts iestāžu, kas ir valsts drošības aģentūras vai tiesībaizsardzības iestādes, piekļuvi persondatiem, var uzskatīt par attaisnojamu iejaukšanos (kas tādējādi neietekmē VDAR 46. panta nosūtīšanas rīkā ietvertās saistības) vai nē. Tas jo īpaši būtu rūpīgi jāapsver, ja tiesību akti, kas reglamentē valsts iestāžu piekļuvi datiem, ir neskaidri vai nav publiski pieejami.

40. Piemērojot datu nosūtīšanas situācijai, pamatojoties uz 46. panta nosūtīšanas rīkiem, EDAK Eiropas būtisko garantiju ieteikumi var palīdzēt gan datu eksportētājam, gan datu importētājam novērtēt, vai šādas pilnvaras nepamatoti iejaucas datu importētāja pienākumos nodrošināt būtisku līdzvērtību.

41. Būtībā līdzvērtīga aizsardzības līmeņa trūkums būs jo īpaši redzams, ja trešās valsts tiesību akti vai prakse attiecībā uz jūsu īstenoto nosūtīšanu neatbilst Eiropas būtisko garantiju prasībām.

42. Jūsu novērtējumam vispirms ir jābalstās uz publiski pieejamiem tiesību aktiem. Tomēr dažās situācijās ar to nepietiks, jo trešās valstīs var nebūt attiecīgie tiesību akti. Šajā gadījumā, ja jūs joprojām vēlaties paredzēt datu nosūtīšanu, jums būtu jāizpēta citi būtiski un objektīvi faktori[45], nevis jāpaļaujas uz subjektīviem faktoriem, piemēram, cik liela ir iespēja, ka valsts iestādes piekļūs jūsu datiem ES

[42] Skatīt ES Pamattiesību hartas 47. un 52. pantu, VDAR 23. panta 1. punktu un EDAK Ieteikumus 02/2020 par Eiropas būtiskām garantijām uzraudzības pasākumiem, 2020. gada 10. novembris, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_lv.

[43] Lieta C-311/18 (*Schrems* II), 104. punkts.

[44] Piemēram: Konvencija Nr. 108 (Konvencija par personu aizsardzību attiecībā uz persondatu automātisku apstrādi, ETS Nr. 108) vai Konvencija Nr. 108+ (Modernizētā Konvencija par personu aizsardzību attiecībā uz persondatu apstrādi, CETS Nr. 223) nodrošina īstenojamus starptautiskus tiesiskās aizsardzības līdzekļus datu aizsardzības pārkāpumu gadījumā un veicina minimālo persondatu aizsardzības līmeni un privātās dzīves ievērošanu.

[45] Skatīt 43. punktu turpmāk, kā arī 3. pielikumu.

standartiem neatbilstīgā veidā. Šis novērtējums būtu jāveic ar pienācīgu rūpību un pamatīgi tas jādokumentē, jo jūs būsiet atbildīgs par lēmumu, kuru pieņemsiet, pamatojoties uz to[46].

43. Novērtējumu varat papildināt ar informāciju, kas iegūta no citiem avotiem[47], piemēram:

- elementiem, kas apliecina, ka trešās valsts iestāde centīsies piekļūt datiem ar vai bez datu importētāja ziņas, ņemot vērā zināmos precedentus, tiesību aktus un praksi;
- elementiem, kas apliecina, ka trešās valsts iestāde varēs piekļūt datiem, izmantojot datu importētāju vai tieši pārtverot sakaru kanālu, ņemot vērā zināmos precedentus, juridiskās pilnvaras, kā arī tās rīcībā esošos tehniskos, finanšu un cilvēkresursus.

44. Jūsu novērtējumā galu galā var atklāties, ka VDAR 46. panta nosūtīšanas rīks, uz kuru jūs atsaucaties un tajā ietvertās garantijas:

- faktiski nodrošina nosūtītajiem persondatiem trešā valstī tādu aizsardzības līmeni, kas būtībā ir līdzvērtīgs EEZ garantētajam. Trešās valsts tiesību akti un prakse, ko piemēro nosūtīšanai, ļauj datu importētājam izpildīt saistības saskaņā ar izvēlēto nosūtīšanas rīku. Jums būtu atkārtoti jāizvērtē atbilstošos intervālos vai arī, ja tiek konstatētas būtiskas izmaiņas (skatīt 6. soli).
- faktiski nenodrošina būtībā līdzvērtīgu aizsardzības līmeni. Datu importētājs nevar izpildīt savas saistības, pamatojoties uz trešās valsts tiesību aktiem un/vai praksi, ko piemēro nosūtīšanai. EST uzsvēra, ka gadījumos, kad VDAR 46. panta nosūtīšanas rīki ir nepietiekami, datu eksportētāja pienākums ir vai nu ieviest efektīvus papildinošos pasākumus, vai neveikt persondatu nosūtīšanu[48].

EST, piemēram, uzskatīja, ka ASV *FISA* 702. pants neievēro obligātās garantijas, kas izriet no ES tiesību aktos noteiktā samērīguma principa, un nevar uzskatīt, ka tas piemērojams tikai tādā apjomā, kas vajadzīgs. Tas nozīmē, ka saskaņā ar *FISA* 702. pantu atļauto programmu aizsardzības līmenis būtībā nav līdzvērtīgs ES tiesību aktos paredzētajām garantijām. Rezultātā, ja uz datu importētāju vai jebkuru citu saņēmēju, kuram datu importētājs izpauž datus, attiecas *FISA* 702. panta[49], LSK vai citi VDAR 46. panta nosūtīšanas rīki, šādas nosūtīšanas ietvaros uz tiem var atsaukties tikai tad, ja papildu tehniskie papildinošie pasākumi nodrošina, ka piekļuve nosūtītajiem datiem ir neiespējama vai neefektīva.

[46] VDAR 5. panta 2. punkts.
[47] Skatīt arī 3. pielikumu.
[48] EST spriedums lietā C-311/18 (*Schrems* II), 134. un 135. punkts.
[49] *FISA* 702. pantu piemēro, ja dati tiek iegūti "no elektronisko sakaru pakalpojumu sniedzēja vai ar tā palīdzību" (*FISA* 702. pants = *USC* 50. sadaļas 1881.a pants, saskaņā ar h)(2)(A)(vi) punktu, kas savukārt ir definēts *USC* 50. sadaļas 1881. panta b) punkta 4. daļā kā
"A) telesakaru operators saskaņā ar 47. sadaļas 153. pantā sniegto definīciju;
B) elektronisko sakaru pakalpojumu sniedzējs saskaņā ar 18. sadaļas 2510. pantā sniegto definīciju;
C) attālināto datošanas pakalpojumu sniedzējs saskaņā ar 18. sadaļas 2711. pantā sniegto definīciju;
D) jebkurš cits sakaru pakalpojumu sniedzējs, kuram ir piekļuve vada vai elektroniskajai saziņai, tiklīdz šāda saziņa tiek pārsūtīta vai, uzglabājot šādu saziņu; vai
E) A, B, C vai D daļā aprakstītās struktūras amatpersona, darbinieks vai pārstāvis."

2.4 4. solis. Pieņemt papildinošus pasākumus

45. Ja jūsu 3. solī veiktā novērtējuma rezultātā ir atklājies, ka jūsu VDAR 46. panta nosūtīšanas rīks nav efektīvs, attiecīgā gadījumā sadarbībā ar importētāju jāapsver, vai pastāv papildinoši pasākumi, kuri, pievienojot tos nosūtīšanas rīkos ietvertajām garantijām, varētu nodrošināt nosūtītajiem datiem trešā valstī tādu aizsardzības līmeni, kas būtībā ir līdzvērtīgs ES garantētajam[50]. "Papildinošie pasākumi" pēc definīcijas papildina garantijas, kas jau ir paredzētas VDAR 46. pantā[51].

46. Izmantojot konkrētu VDAR 46. panta nosūtīšanas rīku, jums katrā gadījumā atsevišķi jānosaka, kuri papildinošie pasākumi varētu būt efektīvi vairākkārtējai nosūtīšanai uz konkrētu trešo valsti. Jūs varēsiet balstīties savos iepriekšējos izvērtējumos (1., 2., un 3. iepriekš) soļa ietvaros, un pārbaudīt, ņemot vērā tur izdarītos secinājumus, papildinošo pasākumu iespējamo efektivitāti, garantējot nepieciešamo aizsardzības līmeni.

47. Principā papildinošiem pasākumiem var būt līgumisks, tehnisks vai organizatorisks raksturs. Dažādu pasākumu apvienošana tā, lai tie atbalstītu un palīdzētu viens otram, var uzlabot aizsardzības līmeni un tādējādi veicināt ES standartu sasniegšanu.

48. Līgumiskie un organizatoriskie pasākumi vien nenovērsīs trešo valstu valsts iestāžu piekļuvi persondatiem (ja tas nepamatoti traucē datu importētāja pienākumiem nodrošināt būtiski līdzvērtīgu aizsardzības līmeni). Patiešām būs situācijas, kad tikai ar tehniskiem pasākumiem iespējams aizkavēt vai padarīt neiespējamu trešo valstu valsts iestāžu piekļuvi persondatiem, jo īpaši uzraudzības nolūkos[52]. Šādās situācijās līgumiski vai organizatoriski pasākumi var papildināt tehniskos pasākumus un stiprināt vispārējo datu aizsardzības līmeni, piemēram, liekot šķēršļus valsts iestāžu mēģinājumiem piekļūt datiem veidā, kas neatbilst ES standartiem.

49. Attiecīgā gadījumā, sadarbojoties ar datu importētāju, varat aplūkot šādu (neizsmeļošu) faktoru uzskaitījumu, lai noteiktu, kuri papildinošie pasākumi visefektīvāk aizsargātu nosūtītos datus:

- nosūtāmo datu formāts (t. i., parastā tekstā / pseidonimizēti vai šifrēti);
- datu raksturs;
- datu apstrādes darbplūsmas ilgums un sarežģītība, apstrādē iesaistīto dalībnieku skaits un saistība starp tiem (piemēram, vai nosūtīšanā ir iesaistīti vairāki pārziņi vai arī gan pārziņi, gan apstrādātāji, vai arī tādu apstrādātāju iesaiste, kas nosūtīs datus no jums datu importētājam (ņemot vērā tiem piemērojamos attiecīgos noteikumus saskaņā ar galamērķa trešās valsts tiesību aktiem[53]));
- iespēja, ka dati var tikt nosūtīti tālāk tajā pašā trešā valstī vai pat uz citām trešām valstīm (piemēram, iesaistot datu importētāja apakšapstrādātājus[54]).

[50] Lieta C-311/18 (*Schrems* II), 96. punkts.
[51] VDAR 109. apsvērums un lieta C-311/18 (*Schrems* II), 133. punkts.
[52] Ja šāda piekļuve pārsniedz demokrātiskā sabiedrībā nepieciešamo un samērīgo; skatīt ES Pamattiesību hartas 47. un 52. pantu, VDAR 23. panta 1. punktu un EDAK Ieteikumus 02/2020 par Eiropas būtiskām garantijām uzraudzības pasākumiem, 2020. gada 10. novembris, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_lv.
[53] VDAR pārziņiem un apstrādātājiem ir noteikti atšķirīgi pienākumi. Nosūtīšana var būt no pārziņa pārzinim, starp kopīgajiem pārziņiem, no pārziņa apstrādātājam un, ja ir saņemta pārziņa atļauja, no apstrādātāja pārzinim vai no apstrādātāja apstrādātājam.
[54] Skatīt 25. zemsvītras piezīmi.

Papildinošo pasākumu piemēri

50. Daži tehnisko, līgumisko un organizatorisko pasākumu piemēri, kurus varētu apsvērt, atrodami neizsmeļošajos sarakstos 2. pielikumā.

***

51. Ja esat ieviesis efektīvus papildinošos pasākumus, kas apvienojumā ar jūsu izvēlēto VDAR 46. panta nosūtīšanas rīku sasniedz aizsardzības līmeni, kas tagad būtībā ir līdzvērtīgs EEZ garantētajam aizsardzības līmenim, jūs varat veikt nosūtīšanu.

52. Ja jūs nevarat atrast vai ieviest efektīvus papildinošos pasākumus, kas nodrošina nosūtītajiem persondatiem būtībā līdzvērtīgu aizsardzības līmeni[55], jūs nedrīkstat uzsākt persondatu nosūtīšanu uz attiecīgo trešo valsti, pamatojoties uz jūsu norādīto VDAR 46. panta nosūtīšanas rīku. Ja jūs jau veicat nosūtīšanu, jums ir jāaptur vai jāpārtrauc persondatu nosūtīšana[56] . Saskaņā ar jūsu norādītajā VDAR 46. panta nosūtīšanas rīkā ietvertajām garantijām, importētājam būtu jāatgriež vai pilnībā jāiznīcina dati, kurus esat jau nosūtījis uz šo trešo valsti, un to kopijas[57].

Piemērs: trešās valsts tiesību akti aizliedz jūsu norādītos papildinošos pasākumus (piemēram, aizliedz izmantot šifrēšanu) vai kā citādi kavē to efektivitāti. Jūs nedrīkstat uzsākt persondatu nosūtīšanu uz šo valsti vai arī ir jāpārtrauc esošā datu nosūtīšana uz šo valsti.

53. Ja jūs nolemjat turpināt nosūtīšanu, neskatoties uz to, ka importētājs nespēj izpildīt saistības saskaņā ar VDAR 46. panta nosūtīšanas rīku, jums par to būtu jāinformē kompetentā uzraudzības iestāde saskaņā ar īpašajiem noteikumiem, kas paredzēti attiecīgajā VDAR 46. panta nosūtīšanas rīkā[58]. Uzraudzības iestāde apturēs vai aizliegs datu nosūtīšanu tajos gadījumos, kad konstatēs, ka nav iespējams nodrošināt būtībā līdzvērtīgu aizsardzības līmeni[59].

54. Kompetentā uzraudzības iestāde var noteikt jebkuru citu koriģējošo pasākumu (piemēram, naudas sodu), ja, neskatoties uz to, ka trešā valstī nevarat pierādīt būtībā līdzvērtīgu aizsardzības līmeni, jūs uzsākat vai turpināt nosūtīšanu.

2.5 5. solis. Procesuālās darbības, ja esat identificējis efektīvus papildinošos pasākumus

55. Procesuālās darbības, kuras var nākties veikt gadījumā, kad esat identificējis ieviešamos efektīvus papildinošos pasākumus, var atšķirties atkarībā no jūsu izmantotā vai paredzētā VDAR 46. panta nosūtīšanas rīka.

---

[55] Ja šāda piekļuve pārsniedz demokrātiskā sabiedrībā nepieciešamo un samērīgo; skatīt ES Pamattiesību hartas 47. un 52. pantu, VDAR 23. panta 1. punktu un EDAK Ieteikumus 02/2020 par Eiropas būtiskām garantijām uzraudzības pasākumiem, 2020. gada 10. novembris, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_lv.

[56] Lieta C-311/18 (*Schrems* II), 135. punkts.

[57] Skatīt LSK Lēmuma 87/2010 pielikuma 12. klauzulu; skatīt (pēc izvēles) papildu izbeigšanas klauzulu LSK 2004/915/EK B pielikumā.

[58] Skatīt EDAK Bieži uzdotos jautājumus par Eiropas Savienības Tiesas spriedumu lietā C-311/18 *Data Protection Commissioner* pret *Facebook Ireland Ltd* un *Maximillian Schrems*, pieņemti 2020. gada 23. jūlijā, jo īpaši Bieži uzdotos jautājumus Nr. 5., 6. un 9. Skatīt arī Komisijas Lēmuma 2010/87/ES 4. klauzulas g) punktu, kā arī Komisijas Lēmuma 2001/497/EK 5. klauzulas a) punktu un Komisijas Lēmuma 2004/915/EK pielikuma II modeļa II. klauzulas c) punktu.

[59] Lieta C-311/18 (*Schrems* II), 113. un 121. punkts.

2.5.1 Standarta datu aizsardzības klauzulas (LSK) (VDAR 46. panta 2. punkta c) un d) apakšpunkts)

56. Ja plānojat ieviest papildinošos pasākumus papildus LSK, jums nav jāpieprasa atļauja no kompetentās UI, lai pievienotu šāda veida klauzulas vai papildu garantijas, ja vien identificētie papildinošie pasākumi nav tieši vai netieši pretrunā ar LSK un ir pietiekami, lai nodrošinātu, ka netiek apdraudēts VDAR garantētais aizsardzības līmenis[60]. Datu eksportētājam un importētājam jānodrošina, ka papildu klauzulas nav iespējams interpretēt veidā, kas ierobežotu LSK paredzētās tiesības un pienākumus vai kā citādi pazeminātu datu aizsardzības līmeni. Jums būtu jāspēj to, tostarp visu klauzulu nepārprotamību, pierādīt saskaņā ar pārskatatbildības principu, kā arī jūsu pienākumu nodrošināt pietiekamu datu aizsardzības līmeni. Kompetentajām uzraudzības iestādēm ir tiesības vajadzības gadījumā pārskatīt šīs papildinošās klauzulas (piemēram, sūdzības vai izmeklēšanas pēc pašu iniciatīvas gadījumā).

57. Ja pats plānojat modificēt standarta datu aizsardzības klauzulas vai ja pievienotie papildinošie pasākumi tieši vai netieši "ir pretrunā" ar LSK, vairs neuzskata, ka jūs atsaucaties uz līguma standartklauzulām[61], un jums ir jālūdz atļauja kompetentajā uzraudzības iestādē saskaņā ar VDAR 46. panta 3. punkta a) apakšpunktu.

2.5.2 SUN (VDAR 46. panta 2. punkta b) apakšpunkts)

58. Spriedumā lietā *Schrems* II izklāstītais pamatojums attiecas arī uz citiem nosūtīšanas instrumentiem saskaņā ar VDAR 46. panta 2. punktu, jo visiem šiem instrumentiem būtībā ir līgumisks raksturs, tāpēc tajos paredzētās garantijas un pušu uzņemtās saistības nav saistošas trešo valstu valsts iestādēm[62].

59. Spriedums lietā *Schrems* II skar persondatu nosūtīšanu, pamatojoties uz SUN, jo trešo valstu tiesību akti var ietekmēt šādu instrumentu sniegto aizsardzību. Konkrētā sprieduma lietā *Schrems* II ietekme uz SUN joprojām tiek apspriesta. EDAK sniegs WP256/257 atsaucēs sīkāku informāciju, tiklīdz tas būs iespējams, par to, vai SUN būtu jāiekļauj papildu saistības[63].

---

[60] VDAR 109. apsvērumā noteikts: "Iespējai, ka pārzinis vai apstrādātājs var izmantot Komisijas vai uzraudzības iestādes pieņemtās standarta datu aizsardzības klauzulas, nebūtu jāizslēdz ne tas, ka pārzinis vai apstrādātājs var iekļaut standarta datu aizsardzības klauzulas plašākā līgumā, piemēram, līgumā starp apstrādātāju un citu apstrādātāju, ne arī tas, ka pārzinis vai apstrādātājs var pievienot citas klauzulas vai papildu garantijas, ar noteikumu, ka tās tieši vai netieši nav pretrunā ar Komisijas vai uzraudzības iestādes pieņemtajām līguma standartklauzulām vai neierobežo datu subjekta pamattiesības vai brīvības." Līdzīgi noteikumi ir paredzēti LSK kopumos, kurus Eiropas Komisija pieņēmusi saskaņā ar Direktīvu 95/45/EK.

[61] Skatīt pēc analoģijas EDAK Atzinumu 17/2020 par Slovēnijas uzraudzības iestādes iesniegto līguma standartklauzulu projektu (VDAR 28. panta 8. punkts) par jau pieņemtajām 28. panta LSK ar līdzīgu noteikumu ("Turklāt Kolēģija atgādina, ka iespēja izmantot uzraudzības iestādes pieņemtās līguma standartklauzulas neliedz pusēm pievienot citus punktus vai papildu garantijas, ja vien tie tieši vai netieši nav pretrunā ar pieņemtajām līguma standartklauzulām vai neskar datu subjektu pamattiesības vai brīvības. Turklāt, ja tiek mainītas standarta datu aizsardzības klauzulas, vairs neuzskata, ka puses ir īstenojušas pieņemtās līguma standartklauzulas"), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_lv.pdf.

[62] EST spriedums lietā C-311/18 (*Schrems* II), 132. punkts.

[63] 29. panta darba grupa, Darba dokuments, kurā sniegta tabula ar elementiem un principiem, kas atrodami saistošajos uzņēmuma noteikumos, un kurš pēdējo reizi pārskatīts un pieņemts 2018. gada 6. februārī, WP 256 rev.01; 29. panta darba grupa, Darba dokuments, kurā sniegta tabula ar elementiem un principiem, kas atrodami saistošajos uzņēmuma noteikumos, un kurš pēdējo reizi pārskatīts un pieņemts 2018. gada 6. februārī, WP 257 rev.01.

60. Tiesa ir uzsvērusi, ka datu nosūtītāja un datu saņēmēja uzdevums ir novērtēt, vai attiecīgajā trešā valstī tiek ievērots ES tiesību aktos noteiktais aizsardzības līmenis, lai noteiktu, vai praksē ir iespējams ievērot LSK vai SUN sniegtās garantijas. Ja tas nav iespējams, jums būtu jānovērtē, vai varat veikt papildinošus pasākumus, lai nodrošinātu aizsardzības līmeni, kas pēc būtības ir līdzvērtīgs EEZ nodrošinātajam, un vai trešās valsts tiesību akti vai prakse neapdraud šos papildinošos pasākumus, mazinot to efektivitāti.

2.5.3 *Ad hoc* līgumu klauzulas (VDAR 46. panta 3. punkta a) apakšpunkts)

61. Spriedumā lietā *Schrems* II izklāstītais pamatojums attiecas arī uz citiem nosūtīšanas instrumentiem saskaņā ar VDAR 46. panta 2. punktu, jo visiem šiem instrumentiem būtībā ir līgumisks raksturs, tāpēc tajos paredzētās garantijas un pušu uzņemtās saistības nav saistošas trešo valstu valsts iestādēm[64]. Tādēļ spriedums lietā *Schrems* II skar persondatu nosūtīšanu, pamatojoties uz *ad hoc* līgumu klauzulām, jo trešo valstu tiesību akti var ietekmēt šādu instrumentu sniegto aizsardzību. Konkrētā sprieduma lietā *Schrems* II ietekme uz *ad hoc* līguma klauzulām joprojām tiek apspriesta. EDAK sniegs sīkāku informāciju, tiklīdz tas būs iespējams.

2.6 6. solis. Atkārtoti izvērtēt atbilstošos intervālos

62. Jums pastāvīgi un attiecīgā gadījumā sadarbībā ar datu importētājiem jāseko līdzi notikumiem trešā valstī, uz kuru esat nosūtījis persondatus, kas varētu ietekmēt jūsu sākotnējo aizsardzības līmeņa novērtējumu un lēmumus, ko esat attiecīgi pieņēmis saistībā ar jūsu veikto datu nosūtīšanu. Pārskatatbildība ir pastāvīgs pienākums (VDAR 5. panta 2. punkts).

63. Jums būtu jāievieš pietiekami stabili mehānismi, lai nodrošinātu, ka nekavējoties apturat vai pārtraucat nosūtīšanu šādos gadījumos:

- importētājs ir pārkāpis vai nespēj izpildīt saistības, ko uzņēmies saskaņā ar VDAR 46. panta nosūtīšanas rīku; vai
- papildinošie pasākumi šajā trešā valstī vairs nav efektīvi.

3 SECINĀJUMS

64. VDAR ir paredzēti noteikumi par persondatu apstrādi EEZ, tādējādi nodrošinot brīvu persondatu plūsmu EEZ ietvaros. VDAR V nodaļā ir reglamentēta persondatu nosūtīšana uz trešām valstīm un noteikta augsta latiņa — nosūtīšana nedrīkst samazināt fizisko personu aizsardzības līmeni, ko garantē VDAR (VDAR 44. pants). EST spriedumā lietā C-311/18 (*Schrems* II) uzsvērta nepieciešamība nodrošināt uz trešo valsti nosūtītiem persondatiem VDAR garantētā aizsardzības līmeņa nepārtrauktību[65].

65. Lai nodrošinātu būtībā līdzvērtīgu datu aizsardzības līmeni, jums vispirms ir rūpīgi jāpārzina jūsu veiktā nosūtīšana. Jums arī jāpārbauda, vai nosūtītie dati ir adekvāti, atbilstīgi un ietver tikai to, kas nepieciešams saistībā ar nolūkiem, kuriem tie tiek nosūtīti un apstrādāti trešā valstī.

66. Jums arī jāidentificē nosūtīšanas rīks, uz kuru jūs atsaucaties nosūtīšanas īstenošanai. Ja nosūtīšanas rīks nav lēmums par aizsardzības līmeņa pietiekamību, jums katrā gadījumā jāpārbauda, vai galamērķa trešās valsts tiesību akti vai prakse nemazina VDAR 46. panta nosūtīšanas rīkā ietvertās garantijas saistībā ar jūsu veikto nosūtīšanu. Ja tikai ar VDAR 46. panta nosūtīšanas rīku jūsu nosūtītajiem

[64] EST spriedums lietā C-311/18 (*Schrems* II), 132. punkts.
[65] Lieta C-311/18 (*Schrems* II), 93. punkts.

persondatiem nav iespējams nodrošināt būtībā līdzvērtīgu aizsardzības līmeni, nepilnības var novērst ar papildinošiem pasākumiem.

67. Ja nevarat atrast vai ieviest efektīvus papildinošos pasākumus, kas nodrošina nosūtītajiem persondatiem būtībā līdzvērtīgu aizsardzības līmeni, jūs nedrīkstat uzsākt persondatu nosūtīšanu uz attiecīgo trešo valsti, pamatojoties uz jūsu izvēlēto nosūtīšanas rīku. Ja jūs jau veicat nosūtīšanu, jums ir nekavējoties jāaptur vai jāpārtrauc persondatu nosūtīšana.

68. Kompetentajai uzraudzības iestādei ir pilnvaras apturēt vai pārtraukt persondatu nosūtīšanu uz trešo valsti, ja netiek nodrošināta ES tiesību aktos paredzētā nosūtīto datu aizsardzība, jo īpaši VDAR 45. un 46. pantā un Pamattiesību hartā paredzētā.

Eiropas Datu aizsardzības kolēģijas vārdā

priekšsēdētāja

(*Andrea Jelinek*)

1. PIELIKUMS DEFINĪCIJAS

- “Trešā valsts” ir jebkura valsts, kas nav EEZ dalībvalsts.
- “EEZ” ir Eiropas Ekonomikas zona, un tajā ietilpst Eiropas Savienības dalībvalstis, kā arī Islande, Norvēģija un Lihtenšteina. VDAR piemēro pēdējām minētajām valstīm saskaņā ar EEZ līgumu, jo īpaši ar tā XI pielikumu un 37. protokolu.
- VDAR ir Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula).
- “Harta” ir Eiropas Savienības Pamattiesību harta, OV C 326, 26.10.2012., 391.–407. lpp.
- “EST” vai “Tiesa” ir Eiropas Savienības Tiesa. Šī ir Eiropas Savienības tiesu iestāde, un tā sadarbībā ar dalībvalstu tiesām nodrošina vienotu ES tiesību piemērošanu un interpretāciju.
- “Datu eksportētājs” ir pārzinis vai apstrādātājs EEZ, kurš persondatus nosūta pārzinim vai apstrādātājam trešā valstī.
- “Datu importētājs” ir pārzinis vai apstrādātājs trešā valstī, kurš saņem vai piekļūst persondatiem, kas nosūtīti no EEZ.
- “VDAR 46. panta nosūtīšanas rīks” ir VDAR 46. pantā ietvertās garantijas, kuras datu eksportētāji ievieš, nosūtot persondatus uz trešo valsti, ja nav lēmuma par aizsardzības līmeņa pietiekamību saskaņā ar VDAR 45. panta 3. punktu. VDAR 46. panta 2. un 3. punktā sniegts to VDAR 46. panta nosūtīšanas rīku uzskaitījums, kurus pārziņi un apstrādātāji var izmantot.
- “LSK” ir standarta datu aizsardzības klauzulas (jeb “līguma standartklauzulas”), ko Eiropas Komisija ir pieņēmusi persondatu nosūtīšanai starp pārziņiem vai apstrādātājiem EEZ un pārziņiem vai apstrādātājiem ārpus EEZ. Eiropas Komisijas pieņemtās līguma standartklauzulas saskaņā ar VDAR ir nosūtīšanas rīks saskaņā ar VDAR 46. panta 2. punkta c) apakšpunktu un 5. punktu.

2. PIELIKUMS. PAPILDINOŠO PASĀKUMU PIEMĒRI

69. Turpmāk uzskaitīti to papildinošo pasākumu piemēri, kurus jūs varētu apsvērt 4. solī "Pieņemt papildinošus pasākumus". Šis uzskaitījums nav izsmeļošs. Viena vai vairāku šo pasākumu izvēle un ieviešana ne vienmēr un sistemātiski nenodrošina, ka jūsu veiktā nosūtīšana atbilst būtiskas līdzvērtības standartiem, ko pieprasa ES tiesību akti. Jums būtu jāizvēlas tādi papildinoši pasākumi, kas var efektīvi garantēt šādu aizsardzības līmeni jūsu nosūtīšanai.

70. Jebkuru papildinošu pasākumu var uzskatīt par efektīvu EST sprieduma lietā *Schrems* II izpratnē tikai tad un tiktāl, ciktāl tas novērš konkrētās nepilnības, kas konstatētas, izvērtējot tiesisko situāciju trešā valstī. Ja galu galā jūs nevarat nodrošināt būtībā līdzvērtīgu aizsardzības līmeni, jūs nedrīkstat nosūtīt persondatus.

71. Uz jums kā pārzini vai apstrādātāju jau var attiekties prasība veikt noteiktus šajā pielikumā aprakstītos pasākumus, pat ja uz jūsu datu importētāju attiecas lēmums par aizsardzības līmeņa pietiekamību, tāpat kā jums, iespējams, tie jāievieš, kad apstrādājat datus EEZ[66]

Tehniskie pasākumi

72. Šajā sadaļā sniegts neizsmeļošs tādu tehnisko pasākumu piemēru uzskaitījums, ar ko var papildināt VDAR 46. pantā minētās garantijas, lai nodrošinātu atbilstību ES tiesību aktos noteiktajam aizsardzības līmenim saistībā ar persondatu nosūtīšanu uz trešo valsti. Šie pasākumi jo īpaši nepieciešami, ja attiecīgās valsts tiesību akti uzliek datu importētājam pienākumus, kas ir pretrunā VDAR 46. panta nosūtīšanas rīku garantijām un var jo īpaši ietekmēt pēc būtības līdzvērtīga aizsardzības līmeņa pret šīs trešās valsts valsts iestāžu piekļuvi šiem datiem līgumiskās garantijas[67].

73. Skaidrības labad jānorāda, ka šajā sadaļā vispirms ir norādīti tehniskie pasākumi, kas varētu būt efektīvi noteiktos scenārijos / lietošanas gadījumos, lai nodrošinātu būtībā līdzvērtīgu aizsardzības līmeni. Sadaļā tālāk aprakstīti daži scenāriji / lietošanas gadījumi, kuros nav iespējams identificēt tehniskus pasākumus, kas nodrošinātu šo aizsardzības līmeni.

Scenāriji, kuriem var atrast *efektīvus* pasākumus

74. Turpmāk uzskaitīto pasākumu mērķis ir nodrošināt, ka trešo valstu valsts iestāžu piekļuve nosūtītajiem datiem neietekmē VDAR 46. panta nosūtīšanas rīkos ietverto atbilstošo garantiju efektivitāti. Šie pasākumi piemērojami arī tad, ja valsts iestāžu piekļuve atbilst importētāja valsts tiesību aktiem gadījumos, kad šāda piekļuve pārsniedz demokrātiskā sabiedrībā nepieciešamo un samērīgo[68]. Šo pasākumu mērķis ir novērst iespējami tiesības aizskarošu piekļuvi, liedzot iestādēm identificēt datu subjektus, izsecināt informāciju par tiem, izdalīt tos citā kontekstā vai sasaistīt nosūtītos datus ar citām to rīcībā esošajām datu kopām, kas cita starpā var saturēt tiešsaistes identifikatorus, kurus nodrošina ierīces, lietojumprogrammas, rīki un protokoli, ko datu subjekti izmanto citos kontekstos.

75. Trešo valstu valsts iestādes var censties piekļūt nosūtītajiem datiem

[66] VDAR 5. panta 2. punkts un 32. pants.
[67] Lieta C-311/18 (*Schrems* II), 135. punkts.
[68] Skatīt ES Pamattiesību hartas 47. un 52. pantu, VDAR 23. panta 1. punktu un EDAK Ieteikumus par Eiropas būtiskām garantijām uzraudzības pasākumiem.

a) tranzītā, piekļūstot sakaru līnijām, kuras izmanto datu nosūtīšanai saņēmējai valstij. Šāda piekļuve var būt pasīva, tādā gadījumā saziņas saturs, iespējams, pēc atlases procesa tiek vienkārši nokopēts. Piekļuve tomēr var būt aktīva arī tādā nozīmē, ka valsts iestādes iejaucas sakaru procesā, ne tikai lasot saturu, bet arī manipulējot vai anulējot tā daļas.

b) datiem esot pie paredzētā datu saņēmēja, piekļūstot apstrādes iekārtām, vai arī pieprasot datu saņēmējam atrast un izgūt interesējošos datus un nodot tos iestādēm.

76. Šajā sadaļā aplūkoti scenāriji, kuros tiek piemēroti abos gadījumos efektīvi pasākumi. Var tikt piemēroti dažādi papildinošie pasākumi, un tie var būt pietiekami konkrētā nosūtīšanas gadījumā, ja saņēmējas valsts tiesību aktos ir paredzēts tikai viens piekļuves veids. Tādēļ datu eksportētājam ar datu importētāja atbalstu ir rūpīgi jāizanalizē tam uzliktie pienākumi.

Piemēram, ASV datu importētājiem, uz kuriem attiecas *USC* 50. sadaļas 1881.a pants (*FISA* 702. pants), ir tiešs pienākums piešķirt piekļuvi viņu rīcībā, glabāšanā vai kontrolē esošiem importētiem persondatiem. Tas var ietvert jebkādas šifrēšanas atslēgas, kas nepieciešamas, lai dati būtu nolasāmi.

77. Scenārijos aprakstīti konkrēti apstākļi un veiktie pasākumi. Jebkuras izmaiņas scenārijos var novest pie atšķirīgiem secinājumiem.

78. Pārziņiem, iespējams, būs jāizmanto noteikti vai visi šeit aprakstītie pasākumi neatkarīgi no datu importētājam piemērojamajos tiesību aktos paredzētā aizsardzības līmeņa, jo tie ir nepieciešami, lai izpildītu VDAR 25. un 32. pantu prasības konkrētos nosūtīšanas apstākļos. Citiem vārdiem sakot, uz eksportētāju jau var attiekties prasība ieviest noteiktus šajā dokumentā aprakstītos pasākumus, pat ja uz viņu datu importētājiem attiecas lēmums par aizsardzības līmeņa pietiekamību, tāpat kā pārziņiem un apstrādātājiem, iespējams, tie jāievieš, apstrādājot datus EEZ

1. lietošanas gadījums. Datu glabāšana dublēšanai un citiem nolūkiem, kuriem nav nepieciešama piekļuve nekodētiem datiem

79. Datu eksportētājs izmanto mitināšanas pakalpojumu sniedzēju trešā valstī persondatu glabāšanai, piemēram, dublēšanas nolūkos.

Ja

1. persondati pirms nosūtīšanas ir apstrādāti, izmantojot spēcīgu šifrēšanu,
2. šifrēšanas algoritms un tā parametru noteikšana (piemēram, atslēgas garums, darbības režīms, ja atbilstoši) atbilst jaunākajiem tehnikas sasniegumiem, un tos var uzskatīt par noturīgiem pret saņēmējvalsts iestāžu veiktu kriptoanalīzi, ņemot vērā tām pieejamos resursus un tehniskās iespējas (piemēram, datošanas jauda pārlases uzbrukumiem),
3. šifrēšanas stiprumā ņemts vērā konkrētais laika periods, kurā jāsaglabā šifrēto persondatu konfidencialitāte,
4. šifrēšanas algoritms ir nevainojami ieviests, izmantojot pienācīgi uzturētu programmatūru, kuras atbilstība izvēlētā algoritma specifikācijai ir pārbaudīta, piemēram, ar sertifikāciju,
5. atslēgas tiek droši pārvaldītas (ģenerētas, administrētas, glabātas, ja atbilstoši, piesaistītas paredzētā saņēmēja identitātei un atsauktas), un
6. atslēgas kontrolē tikai datu eksportētājs vai cita struktūra, kam uzticēts šis uzdevums, kas atrodas EEZ vai trešā valstī, teritorijā vai vienā vai vairākos noteiktos sektoros trešā valstī, vai starptautiskā organizācijā, attiecībā uz ko Komisija saskaņā ar VDAR 45. pantu ir noteikusi, ka ir nodrošināts pietiekams aizsardzības līmenis,

tad EDAK uzskata, ka veiktā šifrēšana ir efektīvs papildinošais pasākums.

2. lietošanas gadījums. Pseidonimizētu datu nosūtīšana

80. Datu eksportētājs vispirms pseidonimizē tā rīcībā esošos datus un pēc tam tos nosūta uz trešo valsti analīzei, piemēram, pētniecības vajadzībām.

Ja

1. datu eksportētājs nosūta apstrādātos persondatus tādā veidā, ka persondatus vairs nevar sasaistīt ar konkrētu datu subjektu, kā arī tos nevar izmantot, lai izdalītu datu subjektu lielākā grupā, bez papildu informācijas izmantošanas[69],
2. šo papildu informāciju glabā tikai datu eksportētājs, un tā tiek turēta atsevišķi dalībvalstī vai trešā valstī, teritorijā vai vienā vai vairākās noteiktās nozarēs trešā valstī, vai starptautiskā organizācijā, attiecībā uz ko Komisija saskaņā ar VDAR 45. pantu ir noteikusi, ka ir nodrošināts pietiekams aizsardzības līmenis,
3. šīs papildu informācijas izpaušanu vai neatļautu izmantošanu liedz atbilstošas tehniskas un organizatoriskas garantijas, tiek nodrošināts, ka datu eksportētājs vienpersoniski kontrolē algoritmu vai repozitoriju, kas ļauj atkārtoti identificēt, izmantojot papildu informāciju, un
4. pārzinis, veicot rūpīgu attiecīgo datu analīzi, ir noteicis, ņemot vērā visu informāciju, kas var būt saņēmējvalsts iestāžu rīcībā, ka pseidonimizētus persondatus nevar sasaistīt ar identificētu vai identificējamu fizisku personu, pat izmantojot savstarpējas atsauces ar šādu informāciju,

tad EDAK uzskata, ka veiktā pseidonimizācija ir efektīvs papildinošais pasākums.

81. Ņemiet vērā, ka daudzās situācijās faktori, kas raksturīgi fiziskas personas fiziskai, fizioloģiskai, ģenētiskai, garīgai, ekonomiskai, kultūras vai sociālai identitātei, fiziskai atrašanās vietai vai saskarei ar interneta pakalpojumu noteiktā brīdī[70], var ļaut identificēt šo personu, pat ja nav norādīts tās vārds, adrese vai citi skaidri identificējami dati.

82. Tas jo īpaši attiecas uz gadījumiem, kad dati skar informācijas pakalpojumu izmantošanu (piekļuves laiks, izmantoto funkciju secība, izmantotās ierīces raksturojums u. c.). Šiem pakalpojumiem tāpat kā persondatu importētājam varētu būt pienākums piešķirt piekļuvi tām pašām valsts iestādēm viņu jurisdikcijā, kuru rīcībā pēc tam, visticamāk, būs dati par to, kā viņu izvēlētā(-ās) persona(-as) izmanto šos informācijas pakalpojumus.

83. Turklāt, ņemot vērā to, ka daži informācijas pakalpojumi pēc būtības ir publiski vai arī tos var izmantot puses ar ievērojamiem resursiem, pārziņiem būs jāpiemēro īpaša piesardzība, ņemot vērā, ka viņu jurisdikcijā esošajām valsts iestādēm, iespējams, ir dati par to, kā viņu izvēlētā persona izmanto informācijas pakalpojumus.

---

[69] Saskaņā ar VDAR 4. panta 5. punktu: ""pseidonimizācija" ir persondatu apstrāde, ko veic tādā veidā, lai persondatus vairs nav iespējams saistīt ar konkrētu datu subjektu bez papildu informācijas izmantošanas, ar noteikumu, ka šāda papildu informācija tiek turēta atsevišķi un tai piemēro tehniskus un organizatoriskus pasākumus, lai nodrošinātu, ka persondati netiek saistīti ar identificētu vai identificējamu fizisku personu;".

[70] VDAR 4. panta 1. punkts: ""persondati" ir jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu ("datu subjektu"); identificējama fiziska persona ir tāda, kuru var tieši vai netieši identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, minētās personas vārdu, uzvārdu, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem;".

3. lietošanas gadījums. Šifrēti dati tikai šķērso trešās valstis

84. Datu eksportētājs vēlas nosūtīt datus uz galamērķi, par kuru pieņemts lēmums, ka tas nodrošina pietiekamu aizsardzību saskaņā ar VDAR 45. pantu. Dati šķērso trešo valsti.

Ja

1. datu eksportētājs nosūta persondatus datu importētājam jurisdikcijā, kas nodrošina pietiekamu aizsardzību, dati tiek transportēti internetā, un dati var ģeogrāfiski šķērsot trešo valsti, kurā netiek nodrošināts būtībā līdzvērtīgs aizsardzības līmenis,
2. tiek izmantota pārsūtīšanas šifrēšana, kurai tiek nodrošināts, ka izmantotie šifrēšanas protokoli ir vismodernākie un nodrošina efektīvu aizsardzību pret aktīviem un pasīviem uzbrukumiem, izmantojot tādus resursus, par kuriem zināms, ka tie ir pieejami valsts iestādēm trešā valstī,
3. atšifrēšana ir iespējama tikai ārpus attiecīgās trešās valsts,
4. saziņā iesaistītās puses vienojas par uzticamu publiskās atslēgas sertifikācijas iestādi vai infrastruktūru,
5. pret aktīviem un pasīviem uzbrukumiem šifrētai pārsūtīšanai tiek izmantoti īpaši aizsardzības pasākumi, kas atbilst jaunākajiem tehnikas sasniegumiem.
6. ja pārsūtīšanas šifrēšana pati par sevi nenodrošina atbilstošu drošību, ņemot vērā pieredzi ar infrastruktūru vai izmantotās programmatūras ievainojamību, persondatus pilnībā šifrē lietojumslānī, izmantojot vismodernākās šifrēšanas metodes,
7. šifrēšanas algoritms un tā parametru noteikšana (piemēram, atslēgas garums, darbības režīms, ja atbilstoši) atbilst jaunākajiem tehnikas sasniegumiem, un tos var uzskatīt par noturīgiem pret tranzīta valsts iestāžu veiktu kriptoanalīzi, ņemot vērā tām pieejamos resursus un tehniskās iespējas (piemēram, datošanas jauda pārlases uzbrukumiem),
8. šifrēšanas stiprumā ņemts vērā konkrētais laika periods, kurā jāsaglabā šifrēto persondatu konfidencialitāte,
9. šifrēšanas algoritms ir nevainojami ieviests, izmantojot pienācīgi uzturētu programmatūru, kuras atbilstība izvēlētā algoritma specifikācijai ir pārbaudīta, piemēram, ar sertifikāciju,
10. ir izslēgtas (aparatūras vai programmatūras) apiešanas iespējas,
11. atslēgas droši pārvalda (ģenerē, administrē, glabā, ja atbilstoši, sasaista ar paredzētā saņēmēja identitāti un atsauc) eksportētājs vai eksportētāja uzticama struktūra jurisdikcijā, kas nodrošina būtībā līdzvērtīgu aizsardzības līmeni,

tad EDAK uzskata, ka pārsūtīšanas šifrēšana, attiecīgā gadījumā kopā ar satura pilnīgu šifrēšanu, ir efektīvs papildinošais pasākums.

4. lietošanas gadījums. Aizsargāts saņēmējs

85. Datu eksportētājs nosūta persondatus datu importētājam trešā valstī, kas īpaši aizsargāts šīs valsts tiesību aktos, piemēram, nolūkā sniegt pacientam ārstēšanu vai klientam juridiskus pakalpojumus.

Ja

1. saskaņā ar trešās valsts tiesību aktiem tās rezidents-datu importētājs ir atbrīvots no pienākuma sniegt iespējami tiesības aizskarošu piekļuvi datiem, kas ir šī saņēmēja rīcībā konkrētā nolūkā, piemēram, balstoties uz pienākumu glabāt dienesta noslēpumu, kas attiecas uz datu importētāju,
2. šis atbrīvojums attiecas uz jebkādu informāciju, kas ir datu importētāja rīcībā un ko var izmantot, lai apietu konfidenciālas informācijas aizsardzību (šifrēšanas atslēgas, paroles, citi akreditācijas dati u. c.),

3. datu importētājs neizmanto apstrādātāja pakalpojumus tādā veidā, kas ļauj valsts iestādēm piekļūt datiem, kamēr tie ir apstrādātāja rīcībā, kā arī datu importētājs nenosūta datus citai, neaizsargātai struktūrai, pamatojoties uz VDAR 46. panta nosūtīšanas rīkiem,
4. persondati pirms to nosūtīšanas tiek šifrēti, izmantojot jaunākajiem tehnikas sasniegumiem atbilstošu metodi, kas garantē, ka atšifrēšana nebūs iespējama, nezinot atšifrēšanas atslēgu (pilnīga šifrēšana) visā obligātajā datu aizsardzības periodā,
5. atšifrēšanas atslēga atrodas tikai aizsargātā datu importētāja pārziņā un ir atbilstoši aizsargāta pret nesankcionētu izmantošanu vai izpaušanu, izmantojot tehniskus un organizatoriskus pasākumus, kas atbilst jaunākajiem tehnikas sasniegumiem, un
6. datu eksportētājs ir droši konstatējis, ka šifrēšanas atslēga, kuru tas plāno izmantot, atbilst saņēmēja rīcībā esošajai atšifrēšanas atslēgai,

tad EDAK uzskata, ka veiktā pārsūtīšanas šifrēšana ir efektīvs papildinošais pasākums.

5. lietošanas gadījums. Dalīta vai daudzpusēja apstrāde

86. Datu eksportētājs vēlas, lai persondatus kopīgi apstrādātu divi vai vairāki neatkarīgi apstrādātāji, kas atrodas dažādās jurisdikcijās, neizpaužot tiem datu saturu. Pirms nosūtīšanas tas datus sadala tā, ka neviena katra apstrādātāja saņemtā daļa nav pietiekama, lai pilnībā vai daļēji rekonstruētu persondatus. Datu eksportētājs saņem apstrādes rezultātus no katra apstrādātāja atsevišķi un apvieno saņemtās daļas, lai iegūtu gala rezultātu, kas var būt persondati vai apkopoti dati.

Ja

1. datu eksportētājs apstrādā persondatus tā, ka tie ir sadalīti divās vai vairākās daļās un nevienu no tām vairs nav iespējams interpretēt vai sasaistīt konkrētu datu subjektu bez papildu informācijas izmantošanas,
2. katra daļa tiek nodota atsevišķam apstrādātājam, kas atrodas citā jurisdikcijā,
3. apstrādātāji pēc izvēles datus apstrādā kopīgi, piemēram, izmantojot drošu daudzpusēju datošanu tā, lai nevienam no tiem netiktu izpausta informācija, kas nav bijusi to rīcībā pirms datošanas,
4. kopīgai datošanai izmantotais algoritms ir aizsargāts pret aktīviem ienaidnieku uzbrukumiem,
5. nav pierādījumu par sadarbību starp valsts iestādēm, kuras atrodas katra apstrādātāja attiecīgajās jurisdikcijās, kas tām ļautu piekļūt visiem apstrādātāju rīcībā esošajiem persondatiem un ļautu atjaunot un izmantot persondatu saturu nekodētā formā apstākļos, kad šāda izmantošana neievērotu datu subjektu pamattiesību un brīvību būtību. Tāpat jebkuras valsts valsts iestādēm nevajadzētu būt pilnvarām piekļūt persondatiem, kas ir apstrādātāju rīcībā visās skartajās jurisdikcijās.
6. pārzinis, veicot rūpīgu attiecīgo datu analīzi, ir noteicis, ņemot vērā visu informāciju, kas var būt saņēmējvalstu iestāžu rīcībā, ka persondatu daļas, kuras tas nosūta apstrādātājiem, nevar sasaistīt ar identificētu vai identificējamu fizisku personu, pat izmantojot savstarpējas atsauces ar šādu informāciju,

tad EDAK uzskata, ka veiktā dalītā apstrāde ir efektīvs papildinošais pasākums.

Scenāriji, kuriem nevar atrast *efektīvus* pasākumus

87. Atsevišķos scenārijos turpmāk aprakstītie pasākumi nebūtu efektīvi, nodrošinot būtībā līdzvērtīgu aizsardzības līmeni datu nosūtīšanai uz trešām valstīm. Tādēļ tie nebūtu kvalificējami kā papildinošie pasākumi.

6. lietošanas gadījums. Nosūtīšana mākoņpakalpojumu sniedzējiem vai citiem apstrādātājiem, kuriem nepieciešama piekļuve nekodētiem datiem

88. Datu eksportētājs izmanto mākoņpakalpojumu sniedzēju vai citu apstrādātāju persondatu apstrādei saskaņā ar tā norādījumiem trešā valstī.

Ja

1. pārzinis nosūta datus mākoņpakalpojumu sniedzējam vai citam apstrādātājam,
2. mākoņpakalpojumu sniedzējam vai citam apstrādātājam ir nepieciešama piekļuve nekodētiem datiem, lai izpildītu uzticēto uzdevumu, un
3. saņēmējvalsts iestādēm piešķirtās pilnvaras piekļūt nosūtītajiem datiem pārsniedz to, kas nepieciešami un samērīgi demokrātiskā sabiedrībā[71],

tad EDAK, ņemot vērā pašreizējo tehnikas līmeni, nespēj paredzēt efektīvu tehnisku pasākumu, kas nepieļautu datu subjekta tiesību pārkāpumu šādas piekļuves rezultātā. EDAK neizslēdz, ka, tehnoloģijai turpmāk attīstoties, var tikt piedāvāti pasākumi, kas sasniedz iecerētos uzņēmējdarbības mērķus bez piekļuves nekodētiem datiem.

89. Aprakstītajos scenārijos, kad nešifrēti persondati ir tehniski nepieciešami apstrādātājam pakalpojuma sniegšanai, pārsūtīšanas šifrēšana un neaktīvo datu miera šifrēšana pat kopā ņemot, nav uzskatāmas par papildinošu pasākumu, kas nodrošina būtībā līdzvērtīgu aizsardzības līmeni, ja datu importētāja rīcībā ir šifrēšanas atslēgas.

7. lietošanas gadījums. Attālināta piekļuve datiem uzņēmējdarbības nolūkos

90. Datu eksportētājs dara persondatus pieejamus trešās valsts uzņēmumiem, lai tos izmantotu kopīgos uzņēmējdarbības nolūkos. Tipisks salikums var būt pārzinis vai apstrādātājs, kas reģistrēts dalībvalsts teritorijā, nosūta persondatus pārzinim vai apstrādātājam trešā valstī, kas pieder tai pašai uzņēmumu grupai vai uzņēmējsabiedrību grupai, kas iesaistīta kopīgā saimnieciskā darbībā. Datu importētājs, piemēram, var izmantot saņemtos datus, lai sniegtu personāla pakalpojumus datu eksportētājam, un šim nolūkam tam nepieciešami cilvēkresursu dati, vai lai sazinātos ar datu eksportētāja klientiem, kuri dzīvo Eiropas Savienībā, pa tālruni vai e-pastu.

Ja

1. datu eksportētājs nosūta persondatus datu importētājam trešā valstī, padarot tos pieejamus plaši izmantotā informācijas sistēmā veidā, kas ļauj importētājam tieši piekļūt datiem pēc paša izvēles, vai nosūtot tos tieši, atsevišķi vai vairumā izmantojot sakaru pakalpojumu,

[71] Skatīt ES Pamattiesību hartas 47. un 52. pantu, VDAR 23. panta 1. punktu un EDAK Ieteikumus par Eiropas būtiskām garantijām uzraudzības pasākumiem.

2. importētājs izmanto nekodētos datus savām vajadzībām,
3. saņēmējvalsts iestādēm piešķirtās pilnvaras piekļūt nosūtītajiem datiem pārsniedz to, kas nepieciešami un samērīgi demokrātiskā sabiedrībā,

tad EDAK nespēj paredzēt efektīvu tehnisku pasākumu, kas nepieļautu datu subjekta tiesību pārkāpumu šādas piekļuves rezultātā.

91. Aprakstītajos scenārijos, kad nešifrēti persondati ir tehniski nepieciešami apstrādātājam pakalpojuma sniegšanai, pārsūtīšanas šifrēšana un neaktīvo datu miera šifrēšana pat kopā ņemot, nav uzskatāmas par papildinošu pasākumu, kas nodrošina būtībā līdzvērtīgu aizsardzības līmeni, ja datu importētāja rīcībā ir šifrēšanas atslēgas.

Papildu līgumiskie pasākumi

92. Šie pasākumi parasti sastāv no vienpusējām, divpusējām vai daudzpusējām[72] līgumsaistībām[73]. Ja tiek izmantots VDAR 46. panta nosūtīšanas rīks, tas lielākajā daļā gadījumu jau satur vairākas datu eksportētāja un datu importētāja saistības (galvenokārt līgumiskas), kuru mērķis ir aizsargāt persondatus[74].

93. Dažās situācijās šie pasākumi var papildināt un pastiprināt nosūtīšanas instrumentā un attiecīgajos trešās valsts tiesību aktos paredzētās garantijas, ja, ņemot vērā nosūtīšanas apstākļus, tās neatbilst visiem būtībā līdzvērtīgam ES garantētajam aizsardzības līmenim nepieciešamajiem nosacījumiem. Tā kā līgumisko pasākumu raksturs parasti nav saistošs šīs trešās valsts iestādēm, ja vien tās nav līgumslēdzējas puses[75], šie pasākumi būtu jāapvieno ar citiem tehniskiem un organizatoriskiem pasākumiem, lai nodrošinātu nepieciešamo datu aizsardzības līmeni. Viena vai vairāku šo pasākumu izvēle un ieviešana ne vienmēr un sistemātiski nenodrošina, ka jūsu veiktā nosūtīšana atbilst būtiskas līdzvērtības standartiem, ko pieprasa ES tiesību akti.

94. Atkarībā no tā, kādi līgumiskie pasākumi jau ir iekļauti VDAR 46. panta nosūtīšanas rīkā, uz kuru atsaucaties, papildu līgumiskie pasākumi var būt lietderīgi, informējot EEZ datu eksportētājus par jaunām norisēm, kas skar uz trešām valstīm nosūtīto datu aizsardzību.

95. Kā minēts, līgumiskie pasākumi neizslēgs tādas trešās valsts tiesību aktu piemērošanu, kas neatbilst EDAK Eiropas būtisko garantiju standartam gadījumos, kad tiesību akti uzliek importētājiem pienākumu izpildīt no valsts iestādēm saņemtos rīkojumus izpaust saņemtos datus[76].

96. Daži šo iespējamo līgumisko pasākumu piemēri ir uzskaitīti turpmāk un klasificēti atbilstoši to būtībai:

[72] Piemēram, SUN ietvaros, kam jebkurā gadījumā būtu jāregulē noteikti turpmāk uzskaitītie pasākumi.

[73] Tiem būs privāts raksturs, un tos neuzskatīs par starptautiskiem nolīgumiem saskaņā ar starptautiskām publiskām tiesībām. Attiecīgi tie parasti neuzliek saistības trešās valsts iestādei kā līgumslēdzējai pusei, ja tie tiek noslēgti ar privātām struktūrām trešās valstīs, kā Tiesa to uzsvēra spriedumā lietā C-311/18 (*Schrems* II), 125. punkts.

[74] Skatīt sprieduma lietā C-311/18 (*Schrems* II) 137. punktu, kurā Tiesa rezultātā atzina, ka LSK satur "efektīvus mehānismus, kas praksē ļauj nodrošināt, ka tiek ievērots Savienības tiesībās prasītais aizsardzības līmenis un ka, pamatojoties uz šīm klauzulām īstenotā persondatu pārsūtīšana šo klauzulu pārkāpuma gadījumā tiek apturēta vai aizliegta" (skatīt arī 148. punktu).

[75] Lieta C-311/18 (*Schrems* II), 125. punkts.

[76] EST spriedums lietā C-311/18 (*Schrems* II), 132. punkts.

Paredzēt līgumsaistības, izmantojot konkrētus tehniskus pasākumus

97. ***Atkarībā no konkrētajiem nosūtīšanas apstākļiem līgumā, iespējams, jāparedz, ka nosūtīšanas īstenošanai jāievieš konkrēti tehniskie pasākumi (skatīt iepriekš piedāvātos tehniskos pasākumus).***

98. ***Efektivitātes nosacījumi:***

- Šī klauzula varētu būt efektīva tajās situācijās, kad eksportētājs ir identificējis tehnisko pasākumu nepieciešamību. Tad tas būtu jāparedz juridiski, lai nodrošinātu, ka arī importētājs apņemas nepieciešamības gadījumā ieviest nepieciešamos tehniskos pasākumus.

Pārredzamības pienākumi:

99. ***Eksportētājs var pievienot līgumam pielikumus ar informāciju, ko importētājs, pieliekot visas pūles, nodrošinās attiecībā uz valsts iestāžu piekļuvi datiem, tostarp izlūkošanas jomā, ja tiesību akti galamērķa valstī atbilst EDAK Eiropas būtiskajām garantijām. Tas varētu palīdzēt datu eksportētājam izpildīt pienākumu dokumentēt aizsardzības līmeņa novērtējumu trešā valstī.***

100. Importētājam var izvirzīt, piemēram, šādas prasības:

(1) uzskaitīt normatīvos aktus galamērķa valstī, kas piemērojami importētājam vai tā (apakš)apstrādātājiem, saskaņā ar kuriem valsts iestādes varētu piekļūt nosūtāmajiem persondatiem, jo īpaši izlūkošanas, tiesībaizsardzības, administratīvās un regulatīvās uzraudzības jomās, kas piemērojamas nosūtītajiem datiem;
(2) ja nav tiesību aktu, kas regulē valsts iestāžu piekļuvi datiem, sniegt informāciju un statistiku, pamatojoties uz importētāja pieredzi vai informāciju no dažādiem avotiem (piemēram, partneriem, atvērtiem avotiem, valsts tiesu praksi un uzraudzības struktūru lēmumiem) par valsts iestāžu piekļuvi attiecīgajai nosūtīšanai paredzēto persondatu veidam (t. i., konkrētajā regulatīvajā jomā; attiecībā uz struktūru veidu, kam pieder datu importētājs; ....)
(3) norādīt, kādi pasākumi tiek veikti, lai novērstu piekļuvi nosūtītajiem datiem (ja tādi ir);
(4) sniegt pietiekami sīku informāciju par visiem valsts iestāžu pieprasījumiem piekļūt persondatiem, kurus importētājs ir saņēmis noteiktā laika posmā[77], jo īpaši iepriekš 1. punktā minētajās jomās, un iekļaut informāciju par saņemtajiem pieprasījumiem, pieprasītajiem datiem, pieprasītāju iestādi un izpaušanas juridisko pamatu, kā arī to, cik lielā mērā importētājs ir izpaudis pieprasītos datus[78];
(5) precizēt, vai un cik lielā mērā importētājam ir likumīgi aizliegts sniegt iepriekš 1.–5. punktā minēto informāciju.

101. Šo informāciju varētu sniegt, izmantojot strukturētas anketas, kuras importētājs aizpilda un paraksta, un to papildina importētāja līgumsaistības noteiktā laika posmā informēt par jebkādām iespējamām izmaiņām šajā informācijā, kā to paredz spēkā esošā pienācīgas rūpības procedūras prakse.

[77] Perioda ilgumam vajadzētu būt atkarīgam no datu subjektu, kuru datus paredzēts nosūtīt, tiesībām un brīvībām, piemēram, pēdējais gads pirms datu eksportēšanas instrumenta noslēgšanas ar datu eksportētāju.
[78] Šī pienākuma izpilde pati par sevi nenozīmē pienācīga aizsardzības līmeņa nodrošināšanu. Tajā pašā laikā jebkura neatbilstoša izpaušana, kas faktiski ir notikusi, rada nepieciešamību ieviest papildinošus pasākumus.

102. ***Efektivitātes nosacījumi:***

- Importētājam jāspēj sniegt eksportētājam šāda veida informācija, ciktāl tam tā ir zināma, kad ir pieliktas visas pūles tās iegūšanā[79].
- Šis importētājam uzliktais pienākums ļauj nodrošināt, ka eksportētājs tiek un joprojām ir informēts par riskiem, kas saistīti ar datu nosūtīšanu uz trešo valsti. Tādējādi eksportētājs varēs atteikties no līguma noslēgšanas vai, ja informācija mainās pēc tā noslēgšanas, izpildīt savu pienākumu apturēt nosūtīšanu un/vai izbeigt līgumu, ja trešās valsts tiesību akti, izmantotajā VDAR 46. panta nosūtīšanas rīkā ietvertās garantijas un jebkādi tā pieņemtie papildu aizsardzības pasākumi vairs nespēj nodrošināt aizsardzības līmeni, kas būtībā ir līdzvērtīgs ES paredzētajam. Tomēr šis pienākums nevar nedz attaisnot importētāja persondatu izpaušanu, nedz radīt cerības, ka turpmāk netiks saņemti piekļuves pieprasījumi.

***

103. ***Eksportētājs var pievienot arī klauzulas, ar kurām importētājs apliecina, ka 1) nav mērķtiecīgi izveidojis apiešanas iespējas vai līdzīgu programmatūru, ko varētu izmantot, lai piekļūtu sistēmai un/vai persondatiem; 2) nav mērķtiecīgi izveidojis vai mainījis savus uzņēmējdarbības procesus veidā, kas atvieglo piekļuvi persondatiem vai sistēmām; un 3) ka valsts tiesību akti vai valdības politika neprasa, lai importētājs izveido vai uztur apiešanas iespējas vai arī atvieglo piekļuvi persondatiem vai sistēmām, vai lai importētāja valdījumā būtu šifrēšanas atslēga, vai arī tam būtu pienākums to nodot[80].***

104. ***Efektivitātes nosacījumi:***

- Tādi tiesību akti vai valdības politika, kas neļauj importētājiem izpaust šo informāciju, var padarīt šo klauzulu neefektīvu. Tādējādi importētājs nevarēs noslēgt līgumu vai arī tam būs jāinformē eksportētājs par nespēju turpināt pildīt savas līgumsaistības[81].
- Līgumā jāiekļauj soda sankcijas un/vai eksportētājam iespēja īsā laikā izbeigt līgumu gadījumos, kad importētājs nav izpaudis apiešanas iespējas vai līdzīgas programmatūras, vai mainījis uzņēmējdarbības procesus vai jebkādas prasības ieviest kādu no šiem pasākumiem, vai nav nekavējoties informējis eksportētāju, tiklīdz par to esību ir uzzinājis.

***

105. ***Eksportētājs var nostiprināt savas tiesības uz vietas un/vai attālināti veikt importētāja datu apstrādes iekārtu revīziju[82] vai pārbaudi, lai pārbaudītu, vai dati nav izpausti valsts iestādēm un ar kādiem nosacījumiem (piekļuve nepārsniedz to, kas nepieciešams un samērīgs demokrātiskā sabiedrībā), piemēram, paredzot īsu laiku un mehānismus, kas nodrošina ātru pārbaudes struktūru intervenci, kā arī nostiprina eksportētāja autonomiju pārbaudes struktūru izvēlē.***

[79] Skatīt iepriekš 32.5. punktu.

[80] Šī klauzula ir būtiska, lai garantētu pienācīgu nosūtīto persondatu aizsardzības līmeni, un tā parasti būtu obligāti jāiekļauj.

[81] Skatīt iepriekš 32.5. punktu.

[82] Skatīt, piemēram, Lēmuma 2010/87/ES par LSK starp pārziņiem un apstrādātājiem 5. klauzulas f) punktu — revīzijas varētu paredzēt arī rīcības kodeksā vai ar sertifikācijas palīdzību.

106. ***Efektivitātes nosacījumi:***

- Lai revīzija būtu pilnībā efektīva, tās tvērumam juridiski un tehniski būtu jāattiecas uz jebkādu importētāja apstrādātāju vai apakšapstrādātāju veikto persondatu apstrādi trešā valstī.
- Piekļuves žurnāliem un citām līdzīgām pēdām vajadzētu būt aizsargātām pret manipulācijām, lai revidenti varētu atrast izpaušanas pierādījumus. Piekļuves žurnālos un citās līdzīgās pēdās būtu jānošķir arī piekļuves, kas saistītas ar parasto uzņēmējdarbību, un piekļuves, kas saistītas ar pasūtījumiem vai piekļuves pieprasījumiem.

***

107. ***Ja sākotnēji tikuši novērtēti importētāja trešās valsts tiesību akti un prakse un ticis uzskatīts, ka tie eksportētāja nosūtītajiem datiem nodrošina būtībā līdzvērtīgu aizsardzības līmeni ES paredzētajam, eksportētājs joprojām var nostiprināt datu importētāja pienākumu nekavējoties informēt datu eksportētāju, ja tas nespēj izpildīt līgumā noteiktās saistības un līdz ar to prasīto "būtībā līdzvērtīga datu aizsardzības līmeņa" standartu[83].***

108. Šī nespēja nodrošināt atbilstību var rasties sakarā ar izmaiņām trešās valsts tiesību aktos vai praksē[84]. Klauzulās var noteikt konkrētus un stingrus laika ierobežojumus un procedūras ātrai datu nosūtīšanas apturēšanai un/vai līguma izbeigšanai, un saņemto datu atgriešanai vai dzēšanai, ko veic importētājs. Saņemto pieprasījumu, to tvēruma un to novēršanai pieņemto pasākumu efektivitātes uzskaitei būtu jāsniedz eksportētājam pietiekamas norādes, lai tas varētu izpildīt pienākumu apturēt vai pārtraukt nosūtīšanu un/vai izbeigt līgumu.

109. ***Efektivitātes nosacījumi:***

- Paziņojums jāsniedz, pirms datiem tiek piešķirta piekļuve. Pretējā gadījumā līdz brīdim, kad eksportētājs saņem paziņojumu, iespējams, ka personas tiesības jau ir pārkāptas, ja pieprasījums ir balstīts šīs trešās valsts tiesību aktos, kas pārsniedz ES tiesību aktos atļauto datu aizsardzības līmeni. Paziņojums tomēr var palīdzēt novērst turpmākus pārkāpumus un ļaut eksportētājam izpildīt pienākumu apturēt persondatu nosūtīšanu uz trešo valsti un/vai izbeigt līgumu.
- Datu importētājam jāseko līdzi visām juridiskām vai politiskām norisēm, kuru rezultātā tas var zaudēt spēju izpildīt savas saistības, un nekavējoties jāinformē datu eksportētājs par jebkādām šādām izmaiņām un notikumiem un, ja iespējams, pirms to ieviešanas, lai datu eksportētājs varētu atgūt datus no datu importētāja.
- Klauzulās būtu jāparedz ātrs mehānisms, ar kuru datu eksportētājs pilnvaro datu importētāju nekavējoties nodrošināt datus vai tos atgriezt datu eksportētājam vai, ja tas nav iespējams, dzēst vai droši šifrēt datus, negaidot eksportētāja norādījumus, ja ir pārkāpts konkrēts slieksnis, par kuru datu eksportētājs un datu importētājs ir vienojušies. Importētājam šis mehānisms

[83] LSK Lēmuma 2010/87/ES 5. klauzulas a) punkta un d) punkta i) apakšpunkts.

[84] Skatīt sprieduma lietā C-311/18 (*Schrems* II) 139. punktu, kurā Tiesa apgalvo, ka "lai gan 5. klauzulas d) punkta i) apakšpunkts ļauj persondatu saņēmējam gadījumā, kad piemērojams tiesiskais regulējums, kas tam nodrošina aizstāvību, kāds, piemēram, ir krimināltiesībās paredzētais aizliegums nolūkā saglabāt tiesībaizsardzības iestāžu veiktās izmeklēšanas konfidencialitāti, nepaziņot Savienībā reģistrētajam persondatu pārzinim par tiesībaizsardzības iestādes saistošu pieprasījumu izpaust persondatus, viņam tomēr atbilstoši LSK lēmuma pielikuma 5. klauzulas a) punktam ir jāinformē persondatu pārzinis par neiespējamību izpildīt datu aizsardzības standartklauzulu prasības".

būtu jāievieš no datu nosūtīšanas sākuma un regulāri jāpārbauda, lai nodrošinātu, ka to var piemērot īsā laikā.

- Citās klauzulās var paredzēt eksportētājam iespēju kontrolēt, vai importētājs ievēro šīs saistības, veicot revīzijas, pārbaudes un citus pārbaudes pasākumus, un panākt saistību izpildi ar sodu piemērošanu importētājam un/vai iespēju eksportētājam apturēt nosūtīšanu un/vai nekavējoties izbeigt līgumu.

***

110. ***Ciktāl to pieļauj attiecīgās trešās valsts tiesību akti, līgumā var nostiprināt importētājam pārredzamības nodrošināšanas pienākumus, paredzot "Warrant Canary" metodi, saskaņā ar kuru importētājs apņemas regulāri publicēt (piemēram, vismaz reizi 24 stundās) kriptogrāfiski parakstītu ziņojumu, ar kuru informē eksportētāju, ka noteiktā datumā un laikā nav saņēmis rīkojumu izpaust persondatus vai tamlīdzīgi. Ja šis paziņojums netiek atjaunināts, tā ir norāde eksportētājam, ka importētājs, iespējams, ir saņēmis rīkojumu.***

111. ***Efektivitātes nosacījumi:***

- Trešās valsts noteikumiem jāļauj datu importētājam sniegt eksportētājam šāda veida pasīvo paziņojumu.
- Datu eksportētājam automātiski jāuzrauga *Warrant Canary* rīkojumi.
- Datu importētājam ir jānodrošina, ka tā privātā atslēga, ar ko paraksta *Warrant Canary*, tiek glabāta drošībā un to nevar piespiest izdot viltus *Warrant Canary* atbilstīgi trešo valstu noteikumiem. Šajā nolūkā var būt lietderīgi izmantot vairākus dažādu personu parakstus un/vai, ka *Warrant Canary* izsniedz persona, kura ir ārpus trešās valsts jurisdikcijas.

Pienākums veikt konkrētas darbības

112. ***Importētājs saskaņā ar galamērķa valsts tiesību aktiem var apņemties pārbaudīt jebkura rīkojuma par datu izpaušanu likumību, jo īpaši, vai nav pārkāptas pieprasītājai valsts iestādei piešķirtās pilnvaras, un apstrīdēt rīkojumu, ja pēc rūpīgas izvērtēšanas tas secina, ka saskaņā ar galamērķa valsts tiesību aktiem ir pamats šādi rīkoties. Apstrīdot rīkojumu, datu importētājam būtu jālūdz pagaidu tiesiskās aizsardzības pasākumi, lai apturētu rīkojuma darbību, kamēr tiesa nav pieņēmusi lēmumu pēc būtības. Importētājam būtu pienākums neizpaust pieprasītos persondatus, ja tas nav obligāti saskaņā ar piemērojamiem procesuālajiem noteikumiem. Datu importētājs arī apņemta sniegt minimālo pieļaujamo informācijas daudzumu, atbildot uz rīkojumu, balstoties uz pamatotu rīkojuma interpretāciju.***

113. ***Efektivitātes nosacījumi:***

- Trešās valsts tiesiskajā regulējumā jābūt efektīviem tiesiskajiem ceļiem, kā apstrīdēt rīkojumus par datu izpaušanu.
- Šajā klauzulā jebkurā gadījumā tiks sniegta ļoti ierobežota papildu aizsardzība, jo rīkojums par datu izpaušanu var būt likumīgs saskaņā ar trešās valsts tiesisko regulējumu, taču šāds tiesiskais regulējums var neatbilst ES standartiem. Šis līgumiskais pasākums noteikti jāpapildina ar citiem papildinošiem pasākumiem.
- Rīkojumu apstrīdēšanai saskaņā ar trešās valsts tiesību aktiem ir jābūt apturošam efektam. Pretējā gadījumā valsts iestādēm joprojām būs piekļuve personu datiem, un jebkurai izrietošai

prasībai par labu indivīdam būtu ierobežota ietekme uz viņa/viņas kaitējuma atlīdzības par datu izpaušanas negatīvajām sekām pieprasījumu.

- Importētājam jāspēj dokumentēt un eksportētājam pierādīt darbības, kuras tas ir veicis, pieliekot visas pūles, lai izpildītu šīs saistības.

***

114. ***Tādā pašā situācijā, kā aprakstīts iepriekš, importētājs var apņemties informēt pieprasījuma iesniedzēju valsts iestādi par pasūtījuma neatbilstību VDAR 46. panta nosūtīšanas rīkā[85] ietvertajām garantijām un no tā izrietošo importētāja pienākumu konfliktu. Importētājs par to vienlaicīgi un pēc iespējas ātrāk informē eksportētāju un/vai EEZ kompetento uzraudzības iestādi, ciktāl tas iespējams saskaņā ar trešās valsts tiesisko regulējumu.***

115. ***Efektivitātes nosacījumi:***

- Šādai informācijai par ES tiesību aktos piešķirto aizsardzību un pienākumu konfliktam vajadzētu būt zināmai juridiskai ietekmei trešās valsts tiesiskajā regulējumā, piemēram, rīkojuma vai piekļuves pieprasījuma tiesiskai vai administratīvai pārskatīšana, tiesas ordera nepieciešamība un/vai pagaidu rīkojuma apturēšana, lai datiem nodrošinātu zināmu aizsardzību.
- Valsts tiesību sistēma nedrīkst liegt importētājam informēt eksportētāju vai vismaz EEZ kompetento uzraudzības iestādi par saņemto rīkojumu vai piekļuves pieprasījumu.
- Importētājam jāspēj dokumentēt un eksportētājam pierādīt darbības, kuras tas ir veicis, pieliekot visas pūles, lai izpildītu šīs saistības.

Datu subjekta iespējas īstenot savas tiesības

116. ***Līgumā var paredzēt, ka persondatiem, kas parastās uzņēmējdarbības laikā (tostarp atbalsta sniegšanas gadījumos) nosūtīti kā parasts teksts, var piekļūt tikai ar eksportētāja un/vai datu subjekta skaidru vai netiešu piekrišanu.***

117. ***Efektivitātes nosacījumi:***

- Šī klauzula varētu būt efektīva situācijās, kad importētāji saņem valsts iestāžu pieprasījumus sadarboties pēc brīvprātības principa, atšķirībā no, piemēram, valsts iestāžu piekļuves datiem, kas tiek veikta bez datu importētāja ziņas vai pretēji tā gribai.
- Dažās situācijās datu subjekts, iespējams, nevar iebilst pret piekļuvi vai sniegt piekrišanu, kas atbilst visiem ES tiesību aktos paredzētajiem nosacījumiem (brīvi sniegta, konkrēta, informēta un nepārprotama) (piemēram, ja runa ir par darbiniekiem)[86].
- Valsts noteikumi vai politika, kas uzliek importētājam pienākumu neizpaust piekļuves rīkojuma faktu, var padarīt šo klauzulu neefektīvu, ja to nevar papildināt ar tehniskām

[85] *Piemēram, LSK paredzēts, ka datu apstrāde, tostarp to nosūtīšana, tiek un arī turpmāk tiks veikta saskaņā ar "piemērojamajiem tiesību aktiem datu aizsardzības jomā". Šis likums ir definēts kā "tiesību akti, kas aizsargā personu pamattiesības un pamatbrīvības, un jo īpaši viņu tiesības uz privāto dzīvi attiecībā uz persondatu apstrādi, un kas attiecas uz atbildīgo par datu apstrādi dalībvalstī, kurā datu nosūtītājs ir reģistrēts".* EST apstiprina, ka VDAR noteikumi, lasot tos kopā ar ES Pamattiesību hartu, ir daļa no šiem tiesību aktiem, skatīt EST spriedumu lietā C-311/18 (*Schrems* II), 138. punkts.

[86] VDAR 4. panta 11. punkts.

metodēm, kas prasa eksportētāja vai datu subjekta iejaukšanos, lai parastā tekstā sūtītie dati būtu pieejami. Šādus tehniskus pasākumus piekļuves ierobežošanai var paredzēt jo īpaši, ja piekļuve tiek piešķirta tikai īpašos atbalsta vai apkopes gadījumos, bet paši dati tiek glabāti EEZ.

***

118. ***Līgumā var paredzēt importētājam un/vai eksportētājam pienākumu nekavējoties informēt datu subjektu par pieprasījumu vai rīkojumu, kas saņemts no trešās valsts iestādēm, vai par importētāja nespēju izpildīt līgumā noteiktās saistības, lai datu subjekts varētu lūgt informāciju un efektīvu tiesisko aizsardzību (piemēram, iesniedzot prasību kompetentai uzraudzības iestādei un/vai tiesu iestādei un pierādot savas tiesības celt prasību trešās valsts tiesās).***

119. ***Efektivitātes nosacījumi:***

- Ar šādu paziņojumu varētu brīdināt datu subjektu par iespējamu trešo valstu valsts iestāžu piekļuvi tā datiem. Tādējādi tas varētu sniegt datu subjektam iespēju lūgt papildu informāciju no eksportētājiem un iesniegt prasību kompetentai uzraudzības iestādei. Ar šo klauzulu var risināt arī dažas grūtības, ar kurām indivīds var saskarties, pierādot savas tiesības celt prasību (*locus standi*) trešo valstu tiesās, apstrīdot valsts iestāžu piekļuvi viņa datiem.
- Valsts noteikumi un politika var liegt sniegt datu subjektam šo paziņojumu. Tomēr eksportētājs un importētājs var apņemties informēt datu subjektu, tiklīdz tiek atcelti ierobežojumi attiecībā uz datu izpaušanu, un pielikt visas pūles, lai panāktu atbrīvojumu no šī izpaušanas aizlieguma. Eksportētājs vai kompetentā uzraudzības iestāde vismaz var informēt datu subjektu par tā persondatu nosūtīšanas apturēšanu vai izbeigšanu sakarā ar to, ka importētājs nespēj izpildīt savas līgumsaistības piekļuves pieprasījuma saņemšanas rezultātā.

***

120. ***Līgumā var paredzēt eksportētājam un importētājam pienākumu palīdzēt datu subjektam īstenot savas tiesības trešās valsts jurisdikcijā, izmantojot ad hoc tiesiskās aizsardzības mehānismus un juridiskas konsultācijas.***

121. ***Efektivitātes nosacījumi***

- Valsts noteikumos un politikā var būt nosacījumi, kas mazinātu paredzēto *ad hoc* tiesiskās aizsardzības mehānismu efektivitāti.
- Juridiskās konsultācijas datu subjektam var būt noderīgas, jo īpaši ņemot vērā, cik sarežģīti un dārgi datu subjektam var būt izprast trešās valsts tiesību sistēmu un celt juridiskas prasības no ārvalstīm, iespējams, svešvalodā. Tomēr šī klauzula visos gadījumos nodrošinās ierobežotu papildu aizsardzību, jo palīdzības un juridisko konsultāciju sniegšana datu subjektiem pati par sevi nevar aizsargāt pret trešās valsts tiesisko regulējumu, ja netiek nodrošināts būtībā ES garantētajam līdzvērtīgs aizsardzības līmenis. Šis līgumiskais pasākums noteikti jāpapildina ar citiem papildinošiem pasākumiem.

Šis papildinošais pasākums būtu efektīvs tikai ar nosacījumu, ka trešās valsts tiesību akti paredz tiesisko aizsardzību savas valsts tiesās vai pastāv *ad hoc* tiesiskās aizsardzības mehānisms. Jebkurā gadījumā tas tomēr nebūtu efektīvs papildinošais pasākums pret uzraudzības pasākumiem, ja nepastāv tiesiskās aizsardzības mehānisms.

Organizatoriski pasākumi

122. Papildu organizatoriski pasākumi var būt iekšējā politika, organizatoriskās metodes un standarti, kurus pārziņi un apstrādātāji var piemērot paši sev, kā arī datu importētājiem trešās valstīs. Tie var palīdzēt nodrošināt konsekvenci persondatu aizsardzībā visā apstrādes ciklā. Organizatoriski pasākumi var arī uzlabot eksportētāju izpratni par risku un mēģinājumiem piekļūt datiem trešās valstīs, kā arī viņu spēju reaģēt uz tiem. Viena vai vairāku šo pasākumu izvēle un ieviešana ne vienmēr un sistemātiski nenodrošina, ka jūsu veiktā nosūtīšana atbilst būtiskas līdzvērtības standartiem, ko pieprasa ES tiesību akti. Atkarībā no konkrētajiem nosūtīšanas apstākļiem un veiktā trešās valsts tiesību aktu novērtējuma var būt nepieciešami organizatoriski pasākumi, lai papildinātu līgumiskos un/vai tehniskos pasākumus nolūkā nodrošināt persondatu aizsardzības līmeni, kas būtībā līdzvērtīgs ES garantētajam.

123. Vispiemērotāko pasākumu novērtējumu veic katrā gadījumā atsevišķi, paturot prātā, ka pārziņiem un apstrādātājiem ir jāievēro pārskatatbildības princips. Turpmāk EDAK sniedz dažus organizatorisko pasākumu piemērus, kurus eksportētāji var ieviest, taču šis uzskaitījums nav izsmeļošs, un var būt piemēroti arī citi pasākumi:

Iekšējā politika nosūtīšanas pārvaldībai, īpaši uzņēmējsabiedrību grupām

124. ***Pienācīgas iekšējās politikas pieņemšana, ietverot skaidru pienākumu sadali attiecībā uz datu nosūtīšanu, ziņošanas kanālus un standarta darbības procedūras gadījumos, ja valsts iestādes slēpti vai oficiāli pieprasa piekļuvi datiem. Īpaši gadījumos, kad tiek veikta nosūtīšana starp uzņēmējsabiedrību grupām, šādā politikā cita starpā var ietvert īpašas EEZ bāzētas komandas iecelšanu, kuru veido IT, datu aizsardzības un privātuma tiesību eksperti, pieprasījumu, kuri skar no ES nosūtīto persondatu, izskatīšanai; paziņojumu sniegšanu augstākajam juridiskās un korporatīvās vadības līmenim un datu eksportētājam pēc šādu pieprasījumu saņemšanas; procesuālās darbības, apstrīdot nesamērīgus vai nelikumīgus pieprasījumus, un pārredzamu informācijas sniegšanu datu subjektiem.***

125. Jāizstrādā īpašas apmācības procedūras personālam, kurš atbild par valsts iestāžu pieprasījumu par piekļuvi persondatiem pārvaldību, un tās periodiski jāatjaunina, lai atspoguļotu jaunākās likumdošanas un tiesu prakses tendences gan trešā valstī, gan EEZ. Apmācības procedūrās būtu jāiekļauj ES tiesību aktu prasības par valsts iestāžu piekļuvi persondatiem, joīpaši saskaņā ar Pamattiesību hartas 52. panta 1. punktu. Personāla informētība jo īpaši būtu jāveicina, novērtējot valsts iestāžu datu piekļuves pieprasījumu praktiskos piemērus un šādiem praktiskiem piemēriem piemērojot Pamattiesību hartas 52. panta 1. punktā noteikto standartu. Šādās apmācībās būtu jāņem vērā datu importētāja īpašā situācija, piemēram, tās trešās valsts tiesību akti un noteikumi, ko piemēro datu importētājam, un, ja iespējams, būtu jāizstrādā sadarbībā ar datu eksportētāju.

126. ***Efektivitātes nosacījumi:***

- Šīs politikas ir izskatāmas tikai tajos gadījumos, kad trešās valsts valsts iestāžu pieprasījums ir saderīgs ar ES tiesību aktiem[87]. Ja pieprasījums nav saderīgs, ar šo politiku nepietiks, lai nodrošinātu līdzvērtīgu persondatu aizsardzības līmeni, un, kā minēts iepriekš, nosūtīšana ir jāpārtrauc vai jāievieš atbilstoši papildinošie pasākumi, lai novērstu no piekļuvi.

[87] Skatīt spriedumu lietā C-362/14 (*Schrems* I), 94. punkts; spriedumu lietā C-311/18 (*Schrems* II), 168.,174., 175. un 176. punkts.

Pārredzamības un pārskatatbildības pasākumi

127. ***Dokumentēt un reģistrēt no valsts iestādēm saņemtos piekļuves pieprasījumus un sniegto atbildi, kā arī juridisko pamatojumu un iesaistītās personas (piemēram, vai eksportētājs ir informēts un tā atbilde, komandas, kura atbild par šādu pieprasījumu izskatīšanu, novērtējums u. c.) Šie ieraksti būtu jādara pieejami datu eksportētājam, kuram savukārt tie nepieciešamības gadījumā jāsniedz attiecīgajiem datu subjektiem.***

128. ***Efektivitātes nosacījumi:***

- Trešās valsts tiesību akti var liegt izpaust pieprasījumus vai būtisku informāciju un tādējādi padarīt šo praksi neefektīvu. Datu importētājam būtu jāinformē eksportētājs, ja tas nespēj iesniegt šādus dokumentus un uzskaiti, tādējādi sniedzot eksportētājam iespēju pārtraukt nosūtīšanu, ja šāda nespēja novestu pie aizsardzības līmeņa pazemināšanās.

***

129. ***Regulāra pārredzamības ziņojumu vai kopsavilkumu publicēšana par valsts iestāžu pieprasījumiem nodrošināt piekļuvi datiem un sniegtās atbildes veidu, ciktāl vietējie tiesību akti to atļauj publicēt.***

130. ***Efektivitātes nosacījumi:***

- Sniegtajai informācijai vajadzētu būt būtiskai, skaidrai un pēc iespējas sīkāk izstrādātai. Trešās valsts tiesību akti var liegt izpaust sīkāku informāciju. Šādos gadījumos datu importētājam būtu jāpieliek visas pūles, lai publicētu statistikas informāciju vai līdzīga veida apkopotu informāciju.

Organizatoriskās metodes un datu minimizēšanas pasākumi

131. ***Saistībā ar datu nosūtīšanu jau esošās organizatoriskās prasības saskaņā ar pārskatatbildības principu var būt noderīgas, piemēram, stingras un detalizētas piekļuves datiem, konfidencialitātes politikas un paraugprakses pieņemšana, kas balstīta vajadzības pēc informācijas principā, ko uzrauga, veicot regulāru revīziju, un panāk ar disciplinārsodiem. Šajā sakarā būtu jāapsver datu minimizēšana, lai ierobežotu nesankcionētas piekļuves iespēju persondatiem. Piemēram, dažos gadījumos varbūt nav nepieciešams nosūtīt noteiktus datus (piemēram, attālinātās piekļuves gadījumā EEZ datiem, piemēram, atbalsta gadījumos, kad pilnīgas piekļuves vietā tiek piešķirta ierobežota piekļuve; vai ja pakalpojuma sniegšanai nepieciešams nosūtīt tikai ierobežotu datu kopu, nevis visu datu bāzi).***

132. ***Efektivitātes nosacījumi:***

- Jābūt regulārām revīzijām un stingriem disciplināriem pasākumiem, lai uzraudzītu un nodrošinātu datu minimizēšanas pasākumu ievērošanu saistībā ar nosūtīšanu.
- Datu eksportētājs pirms nosūtīšanas veic tā rīcībā esošo persondatu novērtējumu, lai identificētu tās datu kopas, kuras nav nepieciešamas nosūtīšanas mērķiem un tāpēc netiks kopīgotas ar datiem importētājs.
- Datu minimizēšanas pasākumi būtu jāpapildina ar tehniskiem pasākumiem, lai nodrošinātu, ka datiem nav iespējama nesankcionēta piekļuve. Piemēram, drošu daudzpusēju datošanas mehānismu ieviešana un šifrētu datu kopu izplatīšana starp dažādām uzticamām struktūrām

integrēti var novērst to, ka jebkuras vienpusējas piekļuves rezultātā tiktu izpausti identificējami dati.

***

133. ***Paraugprakses izstrāde, lai atbilstoši un savlaicīgi iesaistītu un nodrošinātu piekļuvi informācijai datu aizsardzības speciālistam, ja tāds pastāv, kā arī juridiskās un iekšējās revīzijas dienestiem attiecībās uz jautājumiem, kas saistīti ar persondatu starptautisku nosūtīšanu.***

134. ***Efektivitātes nosacījumi:***

- Datu aizsardzības speciālistam, ja tāds ir, un juridiskās un iekšējās revīzijas grupai pirms nosūtīšanas tiek sniegta visa attiecīgā informācija, un ar viņiem konsultējas par nosūtīšanas nepieciešamību un papildu garantijām, ja tādas ir.
- Attiecīgajā informācijā būtu jāietver, piemēram, konkrēto persondatu nosūtīšanas nepieciešamības novērtējums, pārskats par piemērojamiem trešās valsts tiesību aktiem un garantijām, kuras importētājs apņēmies ieviest.

Standartu un paraugprakses pieņemšana

135. ***Stingras datu drošības un datu konfidencialitātes politikas pieņemšana, pamatojoties uz ES sertifikāciju vai rīcības kodeksiem, vai starptautiskajiem standartiem (piemēram, ISO normām) un paraugpraksi (piemēram, ENISA), pienācīgi ņemot vērā jaunākos tehnikas sasniegumus, atbilstīgi apstrādāto datu kategoriju riskam un iespējamībai, ka valsts iestādes mēģinās datiem piekļūt.***

Citi

136. ***Iekšējās politikas pieņemšana un regulāra pārskatīšana, lai novērtētu īstenoto papildinošo pasākumu piemērotību un vajadzības gadījumā identificētu un ieviestu papildu vai alternatīvus risinājumus nolūkā nodrošināt, ka tiek saglabāts ES garantētajam līdzvērtīgs nosūtīto persondatu aizsardzības līmenis.***

***

137. ***Datu importētāja apņemšanās neveikt persondatu tālāku nosūtīšanu tās pašas trešās valsts ietvaros vai uz citu trešo valsti vai pārtraukt esošu nosūtīšanu, ja trešā valstī nav iespējams garantēt ES nodrošinātajam līdzvērtīgu persondatu aizsardzības līmeni[88].***

[88] Lieta C-311/18 (*Schrems* II), 135. un 137. punkts.

3. PIELIKUMS IESPĒJAMIE INFORMĀCIJAS AVOTI TREŠĀS VALSTS NOVĒRTĒJUMAM

138. Jūsu datu importētājam būtu jāspēj norādīt attiecīgos avotus un informāciju par trešo valsti, kurā tas ir reģistrēts, un tam piemērojamiem tiesību aktiem. Jūs varat atsaukties arī uz vairākiem informācijas avotiem, piemēram, uz tiem, kas turpmāk sniegti neizsmeļošajā uzskaitījumā.

- Eiropas Savienības Tiesas (EST) un Eiropas Cilvēktiesību tiesas (ECT)[89] judikatūra, kā minēts Eiropas būtisko garantiju ieteikumos[90];
- Lēmumi par aizsardzības līmeņa pietiekamību galamērķa valstī, ja nosūtīšana balstīta uz citu juridisko pamatu[91];
- Starpvaldību organizāciju, piemēram, Eiropas Padomes[92], citu reģionālo struktūru[93] rezolūcijas un ziņojumi; un ANO struktūras un aģentūras (piemēram, ANO Cilvēktiesību padome[94], Cilvēktiesību komiteja[95]);
- Valsts judikatūra vai lēmumi, ko pieņēmušas neatkarīgas tiesu vai administratīvās iestādes, kas ir kompetentas datu privātuma un trešo valstu datu aizsardzības jomā;
- Akadēmisko institūciju un pilsoniskās sabiedrības organizāciju (piemēram, NVO un tirdzniecības asociāciju) ziņojumi.

[89] Skatīt ECT judikatūras par masu novērošanu faktu lapu: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf.

[90] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions.

[91] Lieta C-311/18 (*Schrems* II), 141. punkts; skatīt lēmumus par aizsardzības līmeņa pietiekamību vietnē https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[92] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions.

[93] Skatīt, piemēram, Amerikas Cilvēktiesību komisijas (*IACHR*) valstu ziņojumus, https://www.oas.org/en/iachr/reports/country.asp.

[94] Skatīt https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx.

[95] skatīt: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5.