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

Versija 2.0

Pieņemts 2021. gada 18. jūnijā

Versiju vēsture

Versija 2.0	2021. gada 18. jūnijs	Ieteikumu pieņemšana pēc sabiedriskās apspriešanas
Versija 1.0	2020. gada 10. novembris	Ieteikumu pieņemšana sabiedriskai apspriešanai

Kopsavilkums

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

Nesenajā spriedumā lietā C-311/18 (Schrems II) Eiropas Savienības Tiesa (EST) mums atgādina, ka personas datu aizsardzībai Eiropas Ekonomikas zonā (EEZ) ir jāiet līdzi datiem, lai kur tie nonāktu. Personas datu nosūtīšana uz trešajām valstīm nevar būt līdzeklis EEZ nodrošinātās aizsardzības apdraudēšanai vai mazināšanai. Tiesa to arī nosaka, paskaidrojot, ka aizsardzības līmenim trešajās valstīs nav jābūt identiskam EEZ garantētajam, bet būtībā līdzvērtīgam. Tiesa arī uzsver līguma standartklauzulu kā nosūtīšanas rīka spēkā esamību, kas var kalpot, lai ar līgumu nodrošinātu būtībā līdzvērtīgu uz trešajām 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 trešajā 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 personas datu apstrādi.

Lai palīdzētu eksportētājiem (pārziņiem vai apstrādātājiem, privātām vai publiskām struktūrām, kas personas datus 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 personas datu nosūtīšanas uz trešajām valstīm apzināšana var būt sarežģīts uzdevums. Tomēr ir jāzina, kur nonāk personas dati, 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 apstrādāti.

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 nosūtat 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, jums jāatsaucas uz kādu no VDAR 46. pantā uzskaitītajiem nosūtīšanas rīkiem. Tikai dažos gadījumos jūs varat atsaukties uz kādu no VDAR 49. pantā paredzētajām atkāpēm, ja atbilstat minētajiem nosacījumiem. Atkāpes nedrīkst kļūt par prakses "normu", tās jāierobežo līdz konkrētām situācijām.

Trešais solis ir **novērtēt**, vai trešās valsts spēkā esošajos tiesību aktos un/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 vispirms jāpievēršas trešo valstu tiesību aktiem, kas attiecas uz jūsu veikto nosūtīšanu, un VDAR 46. panta nosūtīšanas rīkam, uz kuru jūs atsaucaties. Pārbaudot arī trešās valsts publisko iestāžu praksi, jūs varēsiet pārbaudīt, vai nosūtīšanas rīkā ietvertie aizsardzības pasākumi praksē var nodrošināt nosūtīto personas datu efektīvu aizsardzību. Šīs prakses pārbaudīšana būs īpaši svarīga jūsu novērtējumam, ja:

(i.) trešās valsts tiesību akti, kas oficiāli atbilst ES standartiem, acīmredzami netiek piemēroti/panākti praksē;

(ii.) pastāv prakse, kas nav saderīga ar nosūtīšanas rīka saistībām, ja trešajā valstī trūkst attiecīgu tiesību aktu;

(iii.) jūsu nosūtītie dati un/vai importētājs ietilpst vai varētu ietilpt problemātisko tiesību aktu darbības jomā (t. i., skar nosūtīšanas rīka līgumā paredzēto garantiju būtībā līdzvērtīgam aizsardzības līmenim un neatbilst ES standartiem attiecībā uz pamattiesībām, nepieciešamību un proporcionalitāti).

Pirmajās divās situācijās, ja vēlaties turpināt nosūtīšanu, jums būs jāaptur nosūtīšana vai jāīsteno atbilstoši papildu pasākumi.

Trešajā situācijā, ņemot vērā neskaidrības par problemātisko tiesību aktu iespējamo piemērošanu jūsu nosūtīšanai, jūs varat nolemt apturēt nosūtīšanu, īstenot papildu pasākumus nosūtīšanas turpināšanai vai arī veikt nosūtīšanu, neīstenojot papildu pasākumus, ja uzskatāt, ka jums nav iemesla uzskatīt, ka attiecīgie un problemātiskie tiesību akti tiks interpretēti un/vai piemēroti praksē, lai aptvertu jūsu nosūtītos datus un importētāju, un ja jūs varat pierādīt un dokumentēt, ka jums nav pamata uzskatīt, ka attiecīgie tiesību akti tiks interpretēti un/vai piemēroti praksē.

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.

Šis novērtējums būtu jāveic ar pienācīgu rūpību un rūpīgi jādokumentē. Jūsu kompetentās uzraudzības un/vai tiesu iestādes to var pieprasīt un saukt jūs pie atbildības par jebkuru lēmumu, ko pieņemat, 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 un/vai prakse 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 visās. Jūs būsiet atbildīgs par to efektivitātes novērtēšanu attiecībā uz nosūtīšanu, ņemot vērā trešo valstu tiesību aktus un praksi un nosūtīšanas rīku, uz kuru atsaucaties, un jūs būsiet atbildīgs par lēmumu, ko pieņemat uz šā pamata. Šim nolūkam var būt nepieciešams apvienot vairākus papildinošos pasākumus. Jūs galu galā varat secināt, ka neviens papildinošais pasākums nevar nodrošināt 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 personas datu 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 dažas no šīm formalitātēm. Jums var būt jāapspriežas ar kompetentām uzraudzības iestādēm par dažām no šīm darbībām.

Sestais un pēdējais solis būs atbilstošā laika intervālā **atkārtoti novērtēt** personas datiem, kurus nosūtat uz trešajām valstīm, nodrošināto aizsardzības līmeni un uzraudzīt, vai ir bijuši vai būs kādi notikumi, kas tos varētu ietekmēt. Pārskatatbildības princips prasa nepārtrauktu modrību attiecībā uz personas datu 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 Tiesa atgādina, uzraudzības iestādes pēc izmeklēšanas vai sūdzības saņemšanas aptur vai aizliedz datu

nosūtīšanu gadījumos, kad tās konstatē, 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 personas datu 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 personas dati 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 personas dati tiek nosūtīti uz trešo valsti. V nodaļas noteikumu mērķis ir nodrošināt šī augsta līmeņa aizsardzības nepārtrauktību, ja personas dati 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

[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.

ar papildinošiem pasākumiem, lai nodrošinātu atbilstību ES tiesību aktos noteiktajam aizsardzības 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 personas datu aizsardzības līmenis atbilstīgi ES tiesību aktiem personas datiem, kas nosūtīti saskaņā ar standarta datu aizsardzības klauzulām, vajadzības gadījumā paredzot papildus pasākumus tiem, kas piedāvāti šajās klauzulās[5].

(6) Ja Eiropas Savienībā reģistrēts pārzinis vai apstrādātājs nespēj veikt atbilstošus papildus 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 personas datu 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 trešajā 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 papildus pasākumus. Šo ieteikumu mērķis ir nodrošināt metodiku eksportētājiem, nosakot, vai un kādi papildus 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 personas datu 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 līdzvērtīgs ES garantētajam aizsardzības līmenim, lai nodrošinātu, ka gan nosūtīšanas laikā, gan pēc tās 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 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 trešajām 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 personas dati tiek nosūtīti uz trešo valsti[15].

5. Spriedumā lietā Schrems II Tiesa uzsvēra eksportētāju un importētāju pienākumu nodrošināt, ka personas datu 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

---

[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.

saņemto personas datu aizsardzības līmeni[17]. Šie pienākumi ir VDAR pārskatatbildības principa piemērošana datu nosūtīšanai[18].

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 papildus pasākumi likumīgai datu nosūtīšanai ārpus EEZ. "Jūs" šajā dokumentā nozīmē pārzini vai apstrādātāju, kas darbojas kā datu eksportētājs un apstrādā personas datus VDAR piemērošanas jomas ietvaros, tostarp veic datu apstrādi kā privātpersonas un valsts pārvaldes struktūras, nosūtot datus privātām struktūrām[19]. Kas attiecas uz personas datu 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 personas datu nosūtīšanai starp EEZ un ārpus EEZ esošām valsts iestādēm un struktūrām[20].

7. Jums atbilstoši jādokumentē šis novērtējums un izvēlētie un īstenotie papildus 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 personas datu nosūtīšanu[22], vispirms ir jāpārliecinās, ka jūs pilnībā pārzināt savu datu nosūtīšanu (apzināt savu datu nosūtīšanu). Visas nosūtīšanas reģistrēšana un apzināšana var būt sarežģīts uzdevums uzņēmumiem, kuru veiktā datu nosūtīšana uz trešajām 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 veikt, rīkojoties kā pārzinim vai apstrādātājam saskaņā ar VDAR 30. pantu[23]. Jums var palīdzēt arī iepriekšējās darbības, kas veiktas nolūkā izpildīt pienākumu

---

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

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

[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_en

[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

informēt datu subjektus saskaņā ar VDAR 13. panta 1. punkta f) apakšpunktu un 14. panta 1. punkta f) apakšpunktu par viņu personas datu nosūtīšanu uz trešajām valstīm[24].

10. Apzinot nosūtīšanu, neaizmirstiet apsvērt arī tālāku nosūtīšanu, piemēram, vai jūsu apstrādātāji ārpus EEZ nosūta personas datus, 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 saistībā ar nolūkiem, kuriem tie tiek apstrādāti.

12. Šīs darbības jāveic pirms jebkādas nosūtīšanas veikšanas un jāaktualizē pirms nosūtīšanas atsākšanas pēc datu nosūtīšanas darbību apturēšanas: jums jāzina, kur var atrasties eksportētie personas dati 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 un ko piedāvā pakalpojumu sniedzējs, arī tiek uzskatīta par nosūtīšanu[27]. Paskaidrojot sīkāk, ja jūs izmantojat starptautisku mākoņu infrastruktūru, jums jāizvērtē, vai jūsu dati tiks nosūtīti uz trešajām valstīm un kur, ja vien mākoņa pakalpojuma sniedzējs ir reģistrēts EEZ un tas 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.

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).

[24] Saskaņā ar VDAR pārredzamības noteikumiem jums ir pienākums informēt datu subjektus par personas datu 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.

Lēmumi par aizsardzības līmeņa pietiekamību

15. Eiropas Komisija, pieņemot lēmumus par aizsardzības līmeņa pietiekamību attiecībā uz noteiktām vai visām trešajām valstīm, uz kurām jūs nosūtat personas datus, var atzīt, ka tās nodrošina atbilstošu personas datu aizsardzības līmeni[28].

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

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 nosūtat personas datus uz trešajām 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].

---

[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.

[29] VDAR 45. panta 1. punkts.

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

[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 personatu nosūtīšanu uz šādām valstīm, atsaucoties tikai uz aizsardzības līmeņa nepietiekamību. Tās var izmantot savas pilnvaras apturēt vai aizliegt personatu 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.

Piemērs:

ES pilsonis Schrema kungs 2013. gada jūnijā iesniedza sūdzību Īrijas Datu aizsardzības komisijā (DPC) un lūdza šo uzraudzības iestādi aizliegt vai apturēt viņa personas datu nosūtīšanu no Facebook Ireland uz Amerikas Savienotajām Valstīm, jo viņš uzskatīja, ka Amerikas Savienoto Valstu tiesību akti un prakse nenodrošina pietiekamu tās teritorijā esošo personas datu 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 personas datu aizsardzības līmeni ("Drošības zonas" lēmums). Schrema kungs apstrīdēja DPC lēmumu, un Īrijas Augstā tiesa vērsās Eiropas Savienības Tiesā (EST) ar jautājumu par Lēmuma 2000/520 spēkā esamību. Pēc tam, EST nolēma atzīt par spēku zaudējušu Komisijas Lēmumu 2000/520 par "drošības zonas" privātuma principu sniegtās aizsardzības atbilstību[34].

VDAR 46. pants — nosūtīšanas rīki

21. VDAR 46. pantā uzskaitīti vairāki nosūtīšanas rīki ar "atbilstošām garantijām", kurus eksportētāji var izmantot personas datu nosūtīšanai uz trešajām 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 personas dati kopumā saņemtu būtībā līdzvērtīgu aizsardzības līmeni.

23. VDAR 46. pantā pārsvarā sniegtas līgumiska rakstura atbilstošas garantijas, kuras var izmantot nosūtīšanai uz visām trešajām valstīm. Ņemot vērā situāciju trešajā valstī, uz kuru jūs nosūtat datus, joprojām var būt nepieciešams papildināt šos nosūtīšanas rīkus un garantijas ar papildus 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 personas datus noteiktās situācijās. Ievērojot konkrētus nosacījumus, jūs joprojām varat nosūtīt personas datus, pamatojoties uz VDAR 49. pantā minēto atkāpi.

25. VDAR 49. pantam ir izņēmuma raksturs. Tajā ietvertās atkāpes ir jāinterpretē tādā veidā, kas nav pretrunā atkāpju būtībai, jo tās ir atkāpes no noteikuma, saskaņā ar kuru personas datus nedrīkst nosūtīt uz trešo valsti, ja vien šī valsts nenodrošina pietiekamu datu aizsardzības līmeni vai, alternatīvi, ir ieviesti atbilstoši aizsardzības pasākumi. Atkāpes nedrīkst kļūt par prakses "normu",

[34] Lieta C-362/14 (Schrems I).
[35] Lieta C-311/18 (Schrems II), 130. un 133. punkts. Skatīt arī 2.3. punktu turpmāk.

tās jāierobežo līdz konkrētām situācijām. 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. Izvēlētajam VDAR 46. panta nosūtīšanas rīkam ir jābūt efektīvam, lai nodrošinātu, ka praktiskā nosūtīšana neietekmē VDAR garantēto aizsardzības līmeni[37].

29. Jo īpaši aizsardzībai, kas piešķirta nosūtītajiem personas datiem trešajā valstī, ir jābūt nodrošināts līdzvērtīgs aizsardzības līmenis tam, kuru šī regula garantē Eiropas Savienībā, skatot kopā ar Eiropas Savienības Pamattiesību hartu[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, tostarp laikā, kad dati tiek nosūtīti no eksportētāja valsts uz importētāja valsti[39].

30. Tādēļ attiecīgā gadījumā sadarbībā ar importētāju vispirms ir jānovērtē, vai trešās valsts spēkā esošajos tiesību aktos un/vai praksē[40] ir kas tāds, kas jūsu konkrētās nosūtīšanas kontekstā var ietekmēt 46. pantā minētā nosūtīšanas rīka, uz kuru jūs atsaucaties, atbilstošo garantiju efektivitāti. Tas nozīmē, ka ir jānosaka, vai uz jūsu nosūtīšanu attiecas tiesību akti un/vai prakse, kas var apdraudēt jūsu VDAR 46. panta nosūtīšanas rīka efektivitāti. Nepieciešamajam novērtējumam vispirms ir jābalstās uz publiski pieejamiem tiesību aktiem.

31. Šajā novērtējumā jāiekļauj šādi elementi attiecībā uz jūsu importētāja trešās valsts publisko (valsts) iestāžu piekļuvi datiem:

- elementi par to, vai jūsu importētāja trešās valsts publiskās iestādes var mēģināt piekļūt datiem, datu importētājam par to zinot vai ne, ņemot vērā tiesību aktus, praksi un paziņotos precedentus;
- elementi par to, vai jūsu importētāja trešās valsts publiskās iestādes var piekļūt datiem ar datu importētāja starpniecību vai ar telekomunikāciju pakalpojumu sniedzēju vai sakaru kanālu starpniecību, ņemot vērā to rīcībā esošos tiesību aktus, juridiskās pilnvaras, tehniskos, finanšu un cilvēkresursus un ziņotos precedentus.

---

[36] Vairāk informācijas skatīt https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en.

[37] VDAR 44. pants un lietas C-311/18 (Schrems II) 126., 137. un 148. punkts.

[38] Lieta C-311/18 (Schrems II), 105. punkts un otrais secinājums.

[39] Skatīt lietas C-311/18 (Schrems II) 183. punktu saistībā ar 184. punktu.

[40] Skatīt 126. punktu spriedumā lietā C-311/18 (Schrems II), kurā Tiesa skaidri atsaucas uz "attiecīgajā trešā valstī spēkā esošajiem tiesību aktiem un praksi" un pieprasa "(..) praksē nodrošināt uz attiecīgo trešo valsti nosūtīto persondatu efektīvu aizsardzību" (izcēlums pievienots), un 158. punktu.

Atbilstīgo tiesību aktu un prakses apzināšana, ņemot vērā visus nodošanas apstākļus

32. Jums būs jāizvērtē katras datu nosūtīšanas iezīmes un jānosaka, vai jūsu nosūtīšanu ietekmē tās valsts spēkā esošais iekšējais tiesiskais regulējums un/vai prakse, uz kuru dati tiek nosūtīti (vai nosūtīti tālāk). Tādējādi jūsu novērtējums attiecas tikai uz tiesību aktiem un praksi, kas attiecas uz jūsu nosūtīto konkrēto datu aizsardzību, pretstatā vispārējiem un plaši aptverošiem pietiekamības novērtējumiem, ko Eiropas Komisija veic saskaņā ar VDAR 45. pantu.

33. Piemērojamais tiesiskais konteksts un/vai prakse būs atkarīga no jūsu 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 personas datu kategorijām (piemēram, personas dati, kas attiecas uz bērniem, var ietilpt noteiktu trešo valstu tiesību aktu darbības jomā);
- vai dati tiks glabāti trešajā valstī, vai ir tikai nodrošināta attālināta piekļuve datiem, kas glabājas ES/EEZ;
- nosūtāmo datu formāta (t. i., parastā tekstā / pseidonimizēti vai šifrēti[41]);
- iespējas, ka datus var tālāk nosūtīt no trešās valsts uz citu trešo valsti[42].

34. Novērtējumā būtu jāņem vērā visi nosūtīšanā iesaistītie dalībnieki (piemēram, pārziņi, apstrādātāji un apakšapstrādātāji, kas apstrādā datus trešajā valstī), kas identificēti, veicot nosūtīšanas apzināšanas uzdevumu. Jo vairāk iesaistīto pārziņu, apstrādātāju vai importētāju, jo sarežģītāks būs jūsu novērtējums. Šajā novērtējumā jums būs jāņem vērā arī jebkāda paredzētā tālākā nosūtīšana.

35. Jebkurā gadījumā jums būtu jāpievērš īpaša uzmanība visiem attiecīgajiem tiesību aktiem, jo īpaši tiesību aktiem, ar ko nosaka prasības personas datu izpaušanai valsts iestādēm vai piešķir šādām valsts iestādēm pilnvaras piekļūt personas datiem (piemēram, krimināltiesību, regulatīvās uzraudzības un valsts drošības nolūkiem). Ja šīs prasības vai pilnvaras ierobežo datu subjektu pamattiesības, vienlaikus respektējot to būtību un veicot nepieciešamus un samērīgus pasākumus demokrātiskā sabiedrībā, lai aizsargātu svarīgus mērķus, kas atzīti arī Savienības vai ES dalībvalstu tiesību aktos[43], tās nedrīkst apdraudēt saistības, kas ietvertas VDAR 46. pantā paredzētajā nosūtīšanas rīkā, uz kuru jūs paļaujaties.

36. Jums būs jānovērtē attiecīgie vispārīgie noteikumi un prakse, ciktāl tie ietekmē VDAR 46. panta nosūtīšanas rīkā ietverto aizsardzības pasākumu efektīvu piemērošanu.

37. Veicot šo novērtējumu, jāņem vērā dažādi šīs trešās valsts tiesību sistēmas aspekti, piemēram, būtiski ir arī VDAR 45. panta 2. punktā uzskaitītie elementi. Piemēram, tiesiskuma situācija trešajā

[41] Dažas trešās valstis neļauj importēt šifrētus datus.
[42] Ja pārzinis ir sniedzis iepriekšēju konkrētu vai vispārēju rakstisku atļauju atbilstīgi VDAR 28. panta 2. punktam.
[43] 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_en.

valstī var būt būtiska, novērtējot pieejamo mehānismu efektivitāti, lai personas varētu saņemt tiesisko aizsardzību (tiesā) pret nelikumīgu valdības piekļuvi personas datiem. Visaptveroša datu aizsardzības likuma vai neatkarīgas datu aizsardzības iestādes esamība, kā arī to starptautisko dokumentu ievērošana, ar ko paredz datu aizsardzības garantijas, var palīdzēt nodrošināt valdības iejaukšanās samērīgumu.

38. Tiks uzskatīts, ka pienākumi vai pilnvaras, kas izriet no šādiem tiesību aktiem un prakses, apdraud/nav saderīgi ar VDAR 46. panta nosūtīšanas rīka saistībām, ja tie[44]:

- neievēro ES Pamattiesību hartā noteikto pamattiesību un brīvību būtību vai
- pārsniedz to, kas demokrātiskā sabiedrībā ir nepieciešams un samērīgs, lai aizsargātu vienu no svarīgajiem mērķiem, kas atzīti arī Savienības vai dalībvalsts tiesību aktos, piemēram, tie, kas uzskaitīti VDAR 23. panta 1. punktā.

39. Jums būtu jāpārbauda, vai datu importētāja saistības, kas ļauj datu subjektiem īstenot savas tiesības, kā paredzēts VDAR 46. pantā paredzētajā nosūtīšanas rīkā (piemēram, piekļuves, labošanas un dzēšanas pieprasījumi nosūtītajiem datiem, kā arī (tiesu) tiesiskās aizsardzības pieprasījumi), var efektīvi piemērot praksē un vai tās neskar galamērķa trešās valsts tiesību akti un/vai prakse.

40. ES standarti, piemēram, ES Pamattiesību hartas 47. un 52. pants, jāizmanto kā atsauce, jo īpaši, 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.

41. EDAK Eiropas būtisko garantiju (EBG) ieteikumos[45] ir iekļauti paskaidrojumi elementiem, kas jāizvērtē, nosakot, vai tiesisko regulējumu, ar ko reglamentē trešo valstu valsts iestāžu, kas ir valsts drošības aģentūras vai tiesībaizsardzības iestādes, piekļuvi personas datiem, var uzskatīt par attaisnojamu iejaukšanos[46] vai nē. Tas, jo īpaši, būtu rūpīgi jāapsver, ja tiesību akti, kas reglamentē valsts iestāžu piekļuvi datiem, ir neskaidri vai nav publiski pieejami. Pirmā Eiropas būtisko garantiju prasība ir tāda, ka ir jābūt tiesiskajam regulējumam, kas paredz šādu piekļuvi, ja tas ir paredzēts, un ka tā ir publiski pieejama un pietiekami skaidra.

42. Piemērojot datu nosūtīšanas situācijai, pamatojoties uz 46. panta nosūtīšanas rīkiem, EDAK Eiropas būtisko garantiju ieteikumi var palīdzēt datu eksportētājam novērtēt, vai šādas pilnvaras nepamatoti iejaucas datu eksportētāja un importētāja pienākumos nodrošināt būtisku līdzvērtību saskaņā ar VDAR vai nosūtīšanas rīkā ietvertajām saistībām. 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. EDAK atkārtoti uzsver, ka Eiropas būtiskās garantijas ir atsauces standarts, novērtējot trešo valstu uzraudzības pasākumu radīto

---

[44] Skatīt ES Pamattiesību hartas 47. un 52. pantu, VDAR 23. panta 1. punktu, lietas C-311/18 (Schrems II) 174. un 187. punktu un EDAK Ieteikumus 02/2020 par Eiropas būtiskām garantijām uzraudzības pasākumiem, 2020. gada 10. novembris.

[45] EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020.

[46] Un tādējādi neskar saistības, kas noteiktas VDAR 46. pantā paredzētajā nosūtīšanas rīkā.

iejaukšanos starptautiskās datu nosūtīšanas kontekstā. Šie standarti izriet no ES tiesību aktiem un EST un ECT judikatūras, kas ES dalībvalstīm ir saistoša.

43. Jūsu novērtējumam vispirms ir jābalstās uz publiski pieejamiem tiesību aktiem. Pārbaudot arī trešās valsts publisko iestāžu praksi, jūs varēsiet pārbaudīt, vai VDAR 46. panta nosūtīšanas rīkā ietvertie aizsardzības pasākumi var būt pietiekams līdzeklis, lai praksē nodrošinātu nosūtīto personas datu efektīvu aizsardzību[47]. Trešajā valstī spēkā esošās prakses izpēte ir īpaši svarīga jūsu novērtējumam turpmāk aprakstītajās situācijās.

43.1 **Attiecīgie tiesību akti trešajā valstī var oficiāli atbilst ES standartiem attiecībā uz pamattiesībām un brīvībām un to ierobežojumu nepieciešamību un samērīgumu.** Tomēr valsts iestāžu prakse (piemēram, piekļuve privātā sektora rīcībā esošajiem personas datiem vai, īstenojot vai nepiemērojot tiesību aktus kā uzraudzības vai tiesu iestādes), var skaidri norādīt, ka tās parasti nepiemēro/nenodrošina atbilstību tiesību aktiem, kas principā reglamentē to darbību. Šajā gadījumā jums savā novērtējumā ir jāņem vērā šī prakse un jāņem vērā, ka VDAR 46. panta rīks pats par sevi (t. i., bez papildu pasākumiem) nespētu efektīvi nodrošināt līdzvērtīgu aizsardzības līmeni. Šādā gadījumā, ja vēlaties turpināt nosūtīšanu, jums būs jāīsteno atbilstoši papildu pasākumi.

43.2 **Var trūkt attiecīgu trešās valsts tiesību aktu (piemēram, par piekļuvi privātā sektora rīcībā esošajiem personas datiem).** Šajā gadījumā, attiecīgu tiesību aktu trūkuma dēļ, jūs nevarat viennozīmīgi secināt, ka jūsu VDAR 46. panta nosūtīšanas rīku var efektīvi piemērot. Jums būs jāpārbauda, vai ir norādes uz valstī spēkā esošu praksi, kas nav saderīga ar ES tiesību aktiem un VDAR 46. panta nosūtīšanas rīka saistībām. Ja pastāv nesaderīga prakse, VDAR 46. panta nosūtīšanas rīks pats par sevi (t. i., bez atbilstošiem papildu pasākumiem) nespēs efektīvi nodrošināt būtībā līdzvērtīgu aizsardzības līmeni. Šādā gadījumā, ja vēlaties turpināt nosūtīšanu, jums būs jāīsteno atbilstoši papildu pasākumi.

43.3 **Novērtējumā var atklāt, ka attiecīgie tiesību akti trešajā valstī var būt problemātiski[48] un ka nosūtītie dati un/vai attiecīgais importētājs ietilpst vai varētu ietilpt šo problemātisko tiesību aktu darbības jomā[49].**

Ņemot vērā neskaidrības par problemātisko tiesību aktu iespējamo piemērošanu jūsu nosūtīšanai, jūs varat nolemt:

- apturēt nosūtīšanu;

[47] Lieta C-311/18 (Schrems II), 126. punkts.

[48] "Problemātiski tiesību akti" ir tiesību akti, kas 1) persondatu no Eiropas Savienības saņēmējam uzliek pienākumus un/vai ietekmē nosūtītos datus tādā veidā, kas var apdraudēt nosūtīšanas rīku līgumisko garantiju attiecībā uz būtībā līdzvērtīgu aizsardzības līmeni, un 2) neievēro ES Pamattiesību hartā atzīto pamattiesību un brīvību būtību vai pārsniedz to, kas demokrātiskā sabiedrībā ir nepieciešams un samērīgs, lai aizsargātu vienu no svarīgajiem mērķiem, kas atzīti arī Savienības vai ES dalībvalstu tiesību aktos, piemēram, tie, kas uzskaitīti VDAR 23. panta 1. punktā.

[49] Var būt neskaidrs, vai importētājs un/vai nosūtītie dati ietilpst to vispārīgo terminu darbības jomā, kurus bieži izmanto valsts drošības tiesību aktos, lai ierobežotu to piemērošanas jomu, piemēram, "elektronisko sakaru pakalpojumu sniedzējs" un "ārvalstu izlūkošanas informācija".

- īstenot papildu pasākumus[50], lai novērstu risku, ka jūsu importētājam un/vai jūsu nosūtītajiem datiem varētu tikt piemēroti datu importētāja trešās valsts tiesību akti un/vai prakse, kas var apdraudēt nosūtīšanas rīka līgumiskās garantijas attiecībā uz līdzvērtīgu aizsardzības līmeni tam, ko garantē EEZ; vai

- Ja uzskatāt, ka jums nav pamata uzskatīt, ka jūsu nosūtītajiem datiem un/vai importētājam praksē tiks piemēroti būtiski un problemātiski tiesību akti, jūs varat arī nolemt veikt nosūtīšanu bez nepieciešamības īstenot papildu pasākumus. Veicot novērtējumu, attiecīgā gadījumā sadarbībā ar importētāju jums būs jāpierāda un jādokumentē, ka tiesību akti netiek interpretēti un/vai piemēroti praksē, lai aptvertu jūsu nosūtītos datus un importētāju, ņemot vērā arī citu dalībnieku pieredzi, kas darbojas tajā pašā nozarē un/vai saistīti ar līdzīgiem nosūtītiem personas datiem, un papildu informācijas avotus, kas aprakstīti turpmāk[51].

  Tāpēc jums būs jāpierāda un jādokumentē ar detalizētu ziņojumu[52], ka jūsu nosūtītajiem datiem un/vai importētājam praksē netiks piemēroti problemātiski tiesību akti un ka līdz ar to tie neliegs importētājam izpildīt savus pienākumus saskaņā ar VDAR 46. panta nosūtīšanas rīku[53].

Iespējamie informācijas avoti

44. Attiecīgā gadījumā jūsu datu importētājam būtu jāsniedz attiecīgie avoti un informācija par trešo valsti, kurā tas ir reģistrēts, un tiesību aktiem, kas piemērojami nosūtīšanai.

45. Jūs un jūsu importētājs varat papildināt savu novērtējumu ar informāciju, kas iegūta no avotiem , piemēram, tiem, kas uzskaitīti 3. pielikumā.

46. Papildus trešās valsts tiesiskajam regulējumam, ko piemēro nosūtīšanai, avotiem un informācijai vajadzētu būt būtiskai, objektīvai, uzticamai, pārbaudāmai un publiski pieejamai vai citādi pieejamai, lai noteiktu, vai jūsu 46. panta nosūtīšanas rīku var efektīvi piemērot[54], un jums būs jānovērtē un jādokumentē, ka tie tādi ir.

Atbilstība: informācijai ir jābūt saistītai ar konkrēto nosūtīšanu un/vai importētāju un to atbilstību ES tiesību aktos un VDAR 46. panta nosūtīšanas instrumentā noteiktajām prasībām, nevis pārāk vispārīgai vai abstraktai.

[50] Skatīt VDAR 109. apsvērumu un lietas C-311/18 (Schrems II) 132. punktu.
[51] Skatīt 45. līdz 47. punktu.
[52] Jūsu sagatavotajos ziņojumos būs jāiekļauj visaptveroša informācija par tiesību aktu un prakses juridisko novērtējumu un par to piemērošanu konkrētai nodošanai, novērtējuma sagatavošanas iekšējo procedūru (tostarp informāciju par novērtēšanas dalībniekiem, piemēram, juridiskajiem birojiem, konsultantiem vai iekšējām nodaļām) un pārbaužu datumiem. Ziņojumi jāapstiprina eksportētāja likumīgajam pārstāvim.
[53] Pierādīšana, ka jūsu nosūtītajiem datiem un importētājam praksē netiek piemēroti problemātiski tiesību akti, ņemot vērā arī citu dalībnieku, kas darbojas tajā pašā nozarē un/vai ir saistīti ar līdzīgiem nosūtītiem persondatiem, pieredzi, neatbrīvo jūs no pienākuma paredzēt nepieciešamos papildu pasākumus, lai aizsargātu persondatus to nosūtīšanas un apstrādes laikā galamērķa trešā valstī (piemēram, datu pilnīga šifrēšana — skatīt tehnisko papildu pasākumu piemērus 2. pielikumā), ja jūsu analīze par piemērojamiem galamērķa trešās valsts tiesību aktiem liecina, ka piekļuve datiem var notikt arī šajā nosūtīšanas brīdī, pat ja importētājs neiejaucas. Iespējams, ka jūs jau esat paredzējis šādus pasākumus kopā ar importētāju, kas darbojas kā pārzinis vai apstrādātājs saskaņā ar VDAR 32. pantu.
[54] Neizsmeļošu sarakstu ar informācijas avotiem, ko jūs un importētājs varat izmantot, skatīt 3. pielikumā.

Objektīva informācija: ir informācija, ko pamato empīriski pierādījumi, kuru pamatā ir pagātnē gūtās zināšanas, nevis pieņēmumi par iespējamiem notikumiem un riskiem.

Ticamība: eksportētājam un importētājam objektīvi jānovērtē informācijas avota un pašas informācijas uzticamība un tie jāizvērtē atsevišķi.

Pārbaudāmība: informācijai un secinājumiem vajadzētu būt pārbaudāmiem vai pretstatāmiem ar cita veida informāciju vai avotiem kā daļai no vispārējā novērtējuma, arī lai kompetentā uzraudzības vai tiesu iestāde vajadzības gadījumā varētu pārbaudīt šīs informācijas objektivitāti un ticamību.

Publiski pieejama vai citādi pieejama informācija: informācijai vēlams būt publiskai vai vismaz pieejamai, lai atvieglotu iepriekš minēto kritēriju pārbaudi un nodrošinātu tās iespējamu apmaiņu ar uzraudzības iestādēm, tiesu iestādēm un galu galā datu subjektiem.

47. Jūs varat ņemt vērā arī dokumentētu importētāja praktisko pieredzi ar attiecīgiem iepriekšējiem piekļuves pieprasījumiem, kas saņemti no valsts iestādēm trešajā valstī. Jūs kā papildu informācijas avotu varēsiet izmantot importētāja pieredzi tikai tad, ja trešās valsts tiesiskais regulējums neaizliedz importētājam sniegt informāciju par informācijas izpaušanas pieprasījumiem no publiskām iestādēm vai par šādu pieprasījumu neesamību (un šāds novērtējums būtu jādokumentē). Tomēr jāņem vērā, ka tas, ka importētājs iepriekš nav saņēmis pieprasījumus, pats par sevi nekad nevar tikt uzskatīts par izšķirošu faktoru VDAR 46. panta nosūtīšanas rīka efektivitātei, kas ļauj veikt nosūtīšanu bez papildu pasākumiem. Jūs varēsiet ņemt vērā šo informāciju kopā ar cita veida informāciju, kas iegūta no citiem avotiem, kā daļu no vispārējā novērtējuma par trešās valsts tiesību aktiem un praksi saistībā ar jūsu nosūtīšanu. Importētāja attiecīgā un dokumentētā pieredze būtu jāapstiprina un tai nevajadzētu būt pretrunā ar attiecīgu, objektīvu, uzticamu, pārbaudāmu un publiski pieejamu vai citādi pieejamu informāciju par attiecīgo tiesību aktu praktisko piemērošanu (piemēram, par tādu piekļuves pieprasījumu esamību vai neesamību, ko saņēmuši citi dalībnieki, kuri darbojas tajā pašā nozarē un/vai saistīti ar līdzīgiem nosūtītiem personas datiem[55], un/vai tiesību aktu piemērošanu praksē, piemēram, judikatūra un neatkarīgu pārraudzības struktūru ziņojumi).

Jūsu novērtējuma rezultāti

48. Šis vispārējais novērtējums par jūsu importētāja trešās valsts tiesību aktiem un praksi, kas attiecas uz jūsu nosūtīšanu, būtu jāveic ar pienācīgu rūpību un rūpīgi jādokumentē. Jūsu kompetentās uzraudzības un/vai tiesu iestādes to var pieprasīt un saukt jūs pie atbildības par jebkuru lēmumu, ko pieņemat, pamatojoties uz to[56].

49. Jūs novērtējumā varat secināt, ka VDAR 46. panta nosūtīšanas rīks, uz kuru jūs atsaucaties un tajā ietvertās garantijas:

    - faktiski nodrošina nosūtītajiem personas datiem trešajā 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); vai

[55] Pieredze varētu būt citu tādu struktūru pieredze, kuras jūs tieši zināt tāda paša veida iepriekšējas nosūtīšanas dēļ, ko esat veicis vai par ko ziņots attiecīgajā judikatūrā, NVO ziņojumos u. c. (skatīt 3. pielikumu).
[56] VDAR 5. panta 2. punkts.

- faktiski nenodrošina līdzvērtīgu aizsardzības līmeni. Datu importētājs nevar izpildīt savus pienākumus, jo trešās valsts tiesību akti un/vai prakse, ko piemēro nosūtīšanai, neatbilst ES standartiem pamattiesību un pamatbrīvību jomā, un to liedz arī ierobežojumu nepieciešamība un samērīgums, lai aizsargātu leģitīmus sabiedrības interešu mērķus. EST uzsvēra, ka gadījumos, kad VDAR 46. panta nosūtīšanas rīki ir nepietiekami, datu eksportētāja pienākums ir vai nu ieviest efektīvus papildinošos pasākumus, vai neveikt personas datu nosūtīšanu[57].

Piemērs:

Situācija:
EST 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.

Novērtējums:
Ja, izvērtējot attiecīgos ASV tiesību aktus, jūs uzskatāt, ka uz jūsu nosūtīšanu, iespējams, attiecas *FISA* 702. panta darbības joma, bet jūs neesat pārliecināts, ka tas ietilpst tā praktiskajā piemērošanas jomā, jūs varat nolemt:

1. apturēt nosūtīšanu;
2. pieņemt atbilstīgus papildu pasākumus, kas efektīvi nodrošina nosūtīto datu aizsardzības līmeni, kas ir līdzvērtīgs EEZ garantētajam līmenim; vai
3. aplūkot citu objektīvu, ticamu, būtisku, pārbaudāmu un, vēlams, publiski pieejamu informāciju (kas var ietvert jūsu datu importētāja sniegto informāciju), lai precizētu *FISA* 702. panta piemērošanas jomu praksē attiecībā uz jūsu konkrēto nosūtīšanu. Šai informācijai būtu jāsniedz atbildes uz dažiem būtiskiem jautājumiem, piemēram, turpmāk minētajiem.

- Vai publiski pieejamā informācija liecina, ka pastāv juridisks aizliegums informēt par konkrētu pieprasījumu piekļūt saņemtajiem datiem un plaši ierobežojumi sniegt vispārīgu informāciju par pieprasījumiem piekļūt saņemtajiem datiem vai par saņemto pieprasījumu neesamību?

- Vai jūsu datu importētājs ir apstiprinājis, ka tas iepriekš ir saņēmis ASV publisko iestāžu pieprasījumus par piekļuvi datiem? Vai arī jūsu datu importētājs ir apstiprinājis, ka tas iepriekš nav saņēmis ASV publisko iestāžu pieprasījumus par piekļuvi datiem un ka tam nav aizliegts sniegt informāciju par šādiem pieprasījumiem vai to neesamību?

- Vai jūsu iegūtā informācija par ASV tiesu praksi un pārraudzības struktūru, pilsoniskās sabiedrības organizāciju un akadēmisko iestāžu[58] ziņojumi atklāj datu importētājus tajā pašā nozarē, kurā jūsu importētājs iepriekš ir saņēmis pieprasījumus par piekļuvi datiem par līdzīgiem nosūtītiem datiem?

[57] EST spriedums lietā C-311/18 (Schrems II), 134. un 135. punkts.
[58] piemēram, *FISA* 702. panta noteikumi; Ārvalstu izlūkošanas uzraudzības tiesas (*FISC*) reglaments, deklasificēti *FISC* atzinumi un lēmumi, ASV tiesu judikatūra; Privātuma un pilsonisko brīvību pārraudzības padomes (*PCLOB*) ziņojumi un uzklausīšanas protokoli; ASV Tieslietu departamenta ģenerālinspektora biroja ziņojumi; Valsts drošības aģentūras Pilsoņu brīvību un privātuma biroja direktora ziņojumi; Kongresa Izpētes dienesta sagatavotie ziņojumi; Amerikas Pilsoņu brīvību savienības fonda (*ACLU*) ziņojumi.

Atbildes uz šiem jautājumiem, ko jūs iegūstat vispārējā novērtējumā, ļauj secināt, ka:

- *FISA* 702. pants praksē attiecas uz jūsu konkrēto nosūtīšanu, tādējādi apdraudot jūsu VDAR 46. panta nosūtīšanas rīka efektivitāti. Līdz ar to, ja vēlaties veikt nosūtīšanu, jums attiecīgā gadījumā, sadarbībā ar importētāju, jāapsver, vai varat pieņemt papildu pasākumus, kas efektīvi nodrošinātu nosūtīto datu aizsardzības līmeni, kas ir līdzvērtīgs EEZ garantētajam. Ja nevarat atrast efektīvus papildu pasākumus, jūs nedrīkstat nosūtīt personas datus.

vai

- *FISA* 702. pants praksē neattiecas uz jūsu konkrēto nosūtīšanu, un tāpēc tas neskar jūsu VDAR 46. panta nosūtīšanas rīka efektivitāti. Pēc tam jūs varat veikt nosūtīšanu, neveicot nekādus papildu pasākumus.

2.4 4. solis. Pieņemt papildinošus pasākumus

50. 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 trešajā valstī tādu aizsardzības līmeni, kas ir līdzvērtīgs ES garantētajam[59]. "Papildu pasākumi" pēc definīcijas papildina aizsardzības pasākumus, ko jau nodrošina VDAR 46. pantā paredzētais nosūtīšanas rīks, un visas citas piemērojamās drošības prasības (piemēram, tehniskās drošības pasākumus), kas noteiktas VDAR[60].

51. Izmantojot konkrētu VDAR 46. panta nosūtīšanas rīku, jums katrā gadījumā atsevišķi jānosaka, kuri papildinošie pasākumi varētu būt efektīvi vairākkārtējai nosūtīšanai uz konkrētu trešo valsti. Jums novērtējums nav jāveic ikreiz, kad veicat to pašu konkrēta veida datu nosūtīšanu uz vienu un to pašu trešo valsti. Dažiem datiem, ko plānots nosūtīt, var būt vajadzīgi papildu pasākumi, bet citiem datiem tas var nebūt nepieciešams (ņemot vērā formālu un/vai praktisku trešās valsts tiesību aktu piemērošanu). Šādā gadījumā Jūs varēsiet balstīties uz iepriekšējiem izvērtējumiem (1., 2., un 3. iepriekš) soļa ietvaros, un pārbaudīt, ņemot vērā tur izdarītos secinājumus, papildinošo pasākumu iespējamo efektivitāti, garantējot nepieciešamo aizsardzības līmeni.

52. 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.

53. Līgumiskie un organizatoriskie pasākumi vien parasti neaizkavēs trešās valsts publisko iestāžu piekļuvi personas datiem, pamatojoties uz problemātiskiem tiesību aktiem un/vai praksi[61]. Patiešām būs situācijas, kad tikai ar tehniskiem pasākumiem iespējams aizkavēt vai padarīt

[59] Lieta C-311/18 (Schrems II), 96. punkts.

[60] VDAR 109. apsvērums un lieta C-311/18 (Schrems II), 133. punkts.

[61] "Problemātiski tiesību akti" ir tiesību akti, kas 1) persondatu no Eiropas Savienības saņēmējam uzliek pienākumus un/vai ietekmē nosūtītos datus tādā veidā, kas var apdraudēt nosūtīšanas rīku līgumisko garantiju attiecībā uz būtībā līdzvērtīgu aizsardzības līmeni, un 2) neievēro ES Pamattiesību hartā atzīto pamattiesību un brīvību būtību vai pārsniedz to, kas demokrātiskā sabiedrībā ir nepieciešams un samērīgs, lai aizsargātu vienu no svarīgajiem mērķiem, kas atzīti arī Savienības vai ES dalībvalstu tiesību aktos, piemēram, tie, kas uzskaitīti VDAR 23. panta 1. punktā.

neiespējamu trešo valstu valsts iestāžu piekļuvi personas datiem, jo īpaši uzraudzības nolūkos[62]. Šādās situācijās līgumiski vai organizatoriski pasākumi var papildināt tehniskos pasākumus un stiprināt vispārējo datu aizsardzības līmeni (piemēram, ieviešot pārbaudes un likvidējot automātiskos pasākumus valsts iestāžu mēģinājumiem piekļūt datiem veidā, kas neatbilst ES standartiem).

54. Attiecīgā gadījumā sadarbībā ar datu importētāju, Jūs varat iepazīties ar šādiem (neizsmeļošiem) faktoriem, lai noteiktu, kuri papildu pasākumi būtu visefektīvākie, lai aizsargātu nosūtītos datus no publisko iestāžu pieprasījumiem piekļūt datiem, pamatojoties uz praksē piemērotiem problemātiskiem tiesību aktiem:

    - nosūtāmo datu formāts (t. i., parastā tekstā / pseidonimizēti vai šifrēti);
    - datu veids (piemēram, EEZ tiek nodrošināts augstāks aizsardzības līmenis datu kategorijām, uz kurām attiecas VDAR 9. un 10. pants)[63];
    - 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[64]));
    - Trešās valsts tiesību aktu praktiskās piemērošanas metode vai parametri, kas noslēgti 3. posmā;
    - iespēja, ka dati var tikt nosūtīti tālāk tajā pašā trešā valstī vai pat uz citām trešajām valstīm (piemēram, iesaistot datu importētāja apakšapstrādātājus[65]).

<u>Papildinošo pasākumu piemēri</u>

55. Daži tehnisko, līgumisko un organizatorisko pasākumu piemēri, kurus varētu apsvērt, ja tie jau nav iekļauti izmantotajā VDAR 46. pantā paredzētajā nosūtīšanas rīkā, ir atrodami 2. pielikumā aprakstītajos neizsmeļošajos sarakstos.

***

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

---

[62] 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. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[63] Skatīt 42. zemsvītras piezīmi.

[64] 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.

[65] Skatīt 26. zemsvītras piezīmi.

57. Ja jūs nevarat atrast vai ieviest efektīvus papildinošos pasākumus, kas nodrošina nosūtītajiem personas datiem līdzvērtīgu aizsardzības līmeni[66], jūs nedrīkstat uzsākt personas datu nosūtīšanu uz attiecīgo trešo valsti, pamatojoties uz jūsu norādīto VDAR 46. panta nosūtīšanas rīku. Ja jūs jau veicat nosūtīšanu, jums ir jāaptur vai jāpārtrauc personas datu nosūtīšana[67] . 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[68].

Piemērs:

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

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

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

59. 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.

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

60. 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[69]. Datu eksportētājam un importētājam jānodrošina, ka papildu klauzulas nav iespējams interpretēt veidā, kas ierobežotu LSK paredzētās

---

[66] 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. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

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

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

[69] 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.

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).

61. 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[70], 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)

62. 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[71].

63. Spriedums lietā Schrems II skar personas datu nosūtīšanu, pamatojoties uz SUN, jo trešo valstu tiesību akti var ietekmēt šādu instrumentu sniegto aizsardzību.

64. Visas saistības, kas jāiekļauj, tiks minētas atjauninātajos WP256/257 atsauces dokumentos[72], uz kuriem visām grupām, kas paļaujas uz SUN kā nosūtīšanas rīkiem, būs jāsaskaņo savi pašreizējie un turpmākie SUN.

65. Tiesa ir uzsvērusi, ka datu nosūtītāja un datu saņēmēja uzdevums ir novērtēt, vai attiecīgajā trešajā 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.

---

[70] 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.

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

[72] 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.

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

66. 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[73]. Tādēļ spriedums lietā Schrems II skar personas datu nosūtīšanu, pamatojoties uz ad hoc līgumu klauzulām, jo trešo valstu tiesību akti var ietekmēt šādu instrumentu sniegto aizsardzību.

2.6 6. solis. Atkārtoti izvērtēt atbilstošos intervālos

67. Jums pastāvīgi un attiecīgā gadījumā sadarbībā ar datu importētājiem jāseko līdzi notikumiem trešajā valstī, uz kuru esat nosūtījis personas datus, 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).

68. 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

69. VDAR ir paredzēti noteikumi par personas datu apstrādi EEZ, tādējādi nodrošinot brīvu personas datu plūsmu EEZ ietvaros. VDAR V nodaļā ir reglamentēta personas datu nosūtīšana uz trešajām valstīm un noteiktas augstas prasības — nosūtīšana nedrīkst samazināt fizisko personu datu aizsardzības līmeni, ko garantē VDAR (VDAR 44. pants). EST spriedumā lietā C-311/18 (Schrems II) uzsvērta nepieciešamība nodrošināt uz trešo valsti nosūtītiem personas datiem VDAR garantētā aizsardzības līmeņa nepārtrauktību[74].

70. 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 apstrādāti.

71. 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 personas datiem nav iespējams nodrošināt būtībā līdzvērtīgu aizsardzības līmeni, nepilnības var novērst ar papildinošiem pasākumiem.

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

---

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

73. Kompetentajai uzraudzības iestādei ir pilnvaras apturēt vai pārtraukt personas datu 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 personas datus nosūta pārzinim vai apstrādātājam trešajā valstī.
- “Datu importētājs” ir pārzinis vai apstrādātājs trešajā valstī, kurš saņem vai piekļūst personas datiem, kas nosūtīti no EEZ.
- “VDAR 46. panta nosūtīšanas rīks” ir VDAR 46. pantā ietvertās garantijas, kuras datu eksportētāji ievieš, nosūtot personas datus 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 personas datu 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

74. Turpmāk uzskaitīti to papildinošo pasākumu piemēri, kurus jūs varētu apsvērt 4. solī "Pieņemt papildinošus pasākumus". Šis uzskaitījums nav izsmeļošs. Varat izpētīt citus papildu pasākumus. Jāņem vērā, ka turpmākā tehnoloģiskā, juridiskā vai organizatoriskā attīstība var novest pie jaunu papildu pasākumu rašanās. Viena vai vairāku šo pasākumu izvēle un ieviešana ne vienmēr un sistemātiski nenodrošina, ka jūsu veiktā nosūtīšana atbilst būtiskiem līdzvērtības standartiem, ko pieprasa ES tiesību akti. Jums būtu jāizvēlas tādi papildinoši pasākumi, kas var efektīvi garantēt šādu aizsardzības līmeni jūsu nosūtīšanai.

75. Jebkādus papildu pasākumus var uzskatīt par efektīviem EST sprieduma "Schrems II" nozīmē tikai tad, ja un ciktāl ar tiem — atsevišķi vai kopā ar citiem — tiek novērsti konkrēti trūkumi, kas konstatēti, novērtējot situāciju trešajā valstī attiecībā uz tās tiesību aktiem un praksi, kas piemērojama jūsu nosūtīšanai. Ja tomēr jūs nevarat nodrošināt līdzvērtīgu aizsardzības līmeni, jūs nedrīkstat nosūtīt personas datus.

76. Iespējams, ka jums kā pārzinim vai apstrādātājam jau būs jāīsteno daži no šajā pielikumā aprakstītajiem pasākumiem, lai nodrošinātu atbilstību VDAR. Tas nozīmē, ka, iespējams, nepieciešams ieviest līdzīgus pasākumus attiecībā uz personas datiem, ko apstrādā EEZ un nosūta datu importētājam, uz kuru attiecas lēmums par aizsardzības līmeņa pietiekamību, vai citām trešajām valstīm[75].

2.1 Tehniskie pasākumi

77. 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 personas datu 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 līdzvērtīga aizsardzības līmeņa pret šīs trešās valsts publisko iestāžu piekļuvi šiem datiem līgumiskās garantijas[76].

78. Skaidrības labad, šajā sadaļā ir aprakstīti daži piemēri scenārijiem, kuros daži tehniskie pasākumi varētu būt efektīvi, lai nodrošinātu līdzvērtīgu aizsardzības līmeni. Šajā iedaļā ir daži scenāriji, kuros nav noteikti tehniskie pasākumi, lai nodrošinātu šo aizsardzības līmeni.

Piemēri scenārijiem, kas attiecas uz gadījumiem, kad tiek noteikti *efektīvi* pasākumi

79. Turpmāk uzskaitīto pasākumu mērķis ir nodrošināt, ka trešo valstu publisko iestāžu piekļuve nosūtītajiem datiem neietekmē VDAR 46. panta nosūtīšanas rīkos ietverto atbilstošo garantiju efektivitāti. Pat ja valsts iestāžu piekļuve atbilst importētāja valsts tiesību aktiem, šie pasākumi

[75] VDAR 5. panta 2. punkts un 32. pants.
[76] Lieta C-311/18 (Schrems II), 135. punkts.

būtu nepieciešami, lai garantētu līdzvērtīgu aizsardzības līmeni tam, ko garantē EEZ, ja praksē šāda piekļuve pārsniedz to, kas ir nepieciešams un samērīgs demokrātiskā sabiedrībā[77]. Šo pasākumu mērķis ir novērst iespējamu 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.

80. Trešo valstu valsts iestādes var censties piekļūt nosūtītajiem datiem:

    a) tranzītā, piekļūstot sakaru līnijām, kuras izmanto datu nosūtīšanai saņēmējvalstij. 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.

81. 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 personas datiem. Tas var ietvert jebkādas šifrēšanas atslēgas, kas nepieciešamas, lai dati būtu nolasāmi.

82. Scenārijos aprakstīti īpaši apstākļi un pasākumi, kas veikti, lai kalpotu par piemēru. Jebkuras izmaiņas scenārijos var novest pie atšķirīgiem secinājumiem. Scenāriji attiecas uz situācijām, kad ir secināts, ka vispirms ir vajadzīgi papildu pasākumi, t. i., kad praksē attiecīgajai nosūtīšanai piemēro trešās valsts problemātiskus tiesību aktus.

83. Pārziņiem, iespējams, būs obligāti jāizmanto 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

84. Datu eksportētājs izmanto mitināšanas pakalpojumu sniedzēju trešajā valstī personas datu glabāšanai, piemēram, dublēšanas nolūkos.

[77] 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.

Ja

1. Personas datus pirms nosūtīšanas apstrādā, izmantojot spēcīgu šifrēšanu, un tiek pārbaudīta importētāja identitāte,
2. šifrēšanas algoritmam un tā parametru noteikšanai (piemēram, atslēgas garums, darbības režīms, ja atbilstoši) jāatbilst jaunākajiem tehnoloģijas sasniegumiem, un tos var uzskatīt par noturīgiem pret saņēmējvalsts iestāžu veiktu kriptoanalīzi, ņemot vērā tām pieejamos resursus un tehniskās iespējas (piemēram, skaitļošanas jauda pārlases uzbrukumiem),
3. šifrēšanas noturīgumā un atslēgas garumā ņemts vērā konkrētais laika periods, kurā jāsaglabā šifrēto personas datu konfidencialitāte[78],
4. šifrēšanas algoritms ir ieviests pareizi un izmantojot pienācīgi uzturētu programmatūru bez zināmām vājajām vietām, 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 tiek saglabātas vienīgi datu eksportētāja kontrolē vai struktūrā, kurai uzticas eksportētājs, EEZ vai jurisdikcijā, kas piedāvā būtībā līdzvērtīgu aizsardzības līmeni tam, ko garantē EEZ,

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

2. lietošanas gadījums. Pseidonimizētu datu nosūtīšana

85. 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 personas datus tādā veidā, ka personas datus vairs nevar sasaistīt ar konkrētu datu subjektu, kā arī tos nevar izmantot, lai izdalītu datu subjektu lielākā grupā, bez papildu informācijas izmantošanas[79],

[78] Kriptogrāfisko algoritmu aizsardzības spēja laika gaitā samazinās, jo tiek atklāti jauni kriptoanalīzes paņēmieni, rodas jaunas datošanas paradigmas, piemēram, kvantu datošana, un vispārēji palielinās pieejamā datošanas jauda, ja vien netiek pierādīts, ka izmantotie algoritmi ir informācijai teorētiski droši. Šīs bažas jo īpaši attiecas uz publiskās atslēgas algoritmiem, kas rakstīšanas laikā ir koplietošanā. Tādējādi datu eksportētājam ir jāņem vērā, ka publiskās iestādes var apņemties piekļūt šifrētiem datiem 80. punktā aprakstītajos apstākļos un uzglabāt tos, līdz to resursi ir pietiekami atšifrēšanai. Papildu pasākumu var uzskatīt par efektīvu tikai tad, ja šāda atšifrēšana un turpmāka apstrāde tajā laikā vairs nebūtu datu subjektu tiesību pārkāpums, piemēram, tāpēc, ka datus vairs nevar izmantot to tiešai vai netiešai identificēšanai.

[79] 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;" Papilddati var būt tabulas, kurās pseidonīmi sakrīt ar identifikācijas atribūtiem, ko tie aizstāj, kriptogrāfiskās atslēgas vai citi parametri atribūtu pārveidošanai, vai citi dati, kas ļauj attiecināt pseidonimizētus datus uz identificētām vai identificējamām fiziskām personām.

2. minētā papildu informācija ir vienīgi datu eksportētāja rīcībā, un to glabā atsevišķi dalībvalstī vai trešajā valstī, vienībā, kurai eksportētājs uzticas, EEZ vai jurisdikcijā, kas piedāvā būtībā līdzvērtīgu aizsardzības līmeni tam, ko garantē EEZ,
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, par kuru būtu sagaidāms, ka tā varētu būt saņēmējvalsts iestāžu rīcībā un ka tās to varētu izmantot un, ka pseidonimizētus personas datus 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.

86. 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[80], var ļaut identificēt šo personu, pat ja nav norādīts tās vārds, adrese vai citi skaidri identificējami dati.

87. 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 personas datu 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.

88. 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.

89. Ja pseidonimizācijas laikā personas datos ietvertie atribūti tiek pārveidoti, izmantojot kriptogrāfisku algoritmu, piemēro norādījumus 80. un 81. zemsvītras piezīmē. Turpmāk ir ieteicams atteikties no kriptogrāfijas ekskluzīvas izmantošanas un piemērot izmaiņas, pamatojoties uz tabulas meklēšanas mehānismiem.

3. lietošanas gadījums. Datu šifrēšana, lai aizsargātu tos no importētāja trešās valsts publisko iestāžu piekļuves, kad tie tranzītā šķērso eksportētāju un tā importētāju

90. Datu eksportētājs vēlas nosūtīt datus uz galamērķi, kurā tiesību akti un/vai prakse ļauj valsts iestādēm piekļūt datiem, kamēr tie tiek virzīti tranzītā no eksportētāja valsts uz galamērķa valsti.

Ja

1. datu eksportētājs nosūta personas datus datu importētājam jurisdikcijā, kurā tiesību akti un/vai prakse ļauj publiskajām iestādēm piekļūt datiem, kamēr tie tiek transportēti internetā uz šo trešo valsti bez Eiropas būtiskām garantijām attiecībā uz šo piekļuvi, tiek izmantota

[80] VDAR 4. panta 1. punkts: ""persondati" ir jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu ("datu subjekts"); 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;".

transporta šifrēšana, kurā tiek nodrošināts, ka izmantotie šifrēšanas protokoli ir mūsdienīgi un nodrošina efektīvu aizsardzību pret aktīviem un pasīviem uzbrukumiem ar resursiem, par kuriem zināms, ka tie ir pieejami šīs trešās valsts publiskajām iestādēm,

2. saziņā iesaistītās puses vienojas par uzticamu publiskās atslēgas sertifikācijas iestādi vai infrastruktūru,
3. tiek izmantoti īpaši aizsardzības un mūsdienīgi pasākumi pret aktīviem un pasīviem uzbrukumiem nosūtīšanas un saņemšanas sistēmām, kas nodrošina transporta šifrēšanu, tostarp programmatūras ievainojamības un iespējamo lūku testi,
4. ja pārsūtīšanas šifrēšana pati par sevi nenodrošina atbilstošu drošību, ņemot vērā pieredzi ar infrastruktūru vai izmantotās programmatūras ievainojamību, personas datus pilnībā šifrē lietojumslānī, izmantojot vismodernākās šifrēšanas metodes,
5. 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, kad dati tiek nosūtīti uz šo trešo valsti, ņemot vērā tām pieejamos resursus un tehniskās iespējas (piemēram, datošanas jauda pārlases uzbrukumiem) (skatīt 80. zemsvītras piezīmi iepriekš)[81],
6. šifrēšanas iedarbīgumā ņemts vērā konkrētais laika periods, kurā jāsaglabā šifrēto personas datu konfidencialitāte,
7. šifrēšanas algoritms ir ieviests pareizi un izmantojot pienācīgi uzturētu programmatūru bez zināmām vājajām vietām, kuras atbilstība izvēlētā algoritma specifikācijai ir pārbaudīta, piemēram, ar sertifikāciju,
8. 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

91. Datu eksportētājs nosūta personas datus datu importētājam trešajā 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 izvairītos no konfidenciālas informācijas aizsardzības (šifrēšanas atslēgas, paroles, citi akreditācijas dati u. c.),

[81] Dažas atsauces uz tehniskajiem norādījumiem, ko publicējušas ES un tās dalībvalstu oficiālās kiberdrošības iestādes, skatīt 80. zemsvītras piezīmē.

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. personas dati 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 ir tikai aizsargātā datu importētāja pārziņā un, iespējams, pats eksportētājs vai cita vienība, kurai uzticas eksportētājs, kas atrodas EEZ, vai jurisdikcijā, kas piedāvā līdzvērtīgu aizsardzības līmeni tam, ko garantē EEZ, un kas ir pienācīgi aizsargāta pret neatļautu izmantošanu vai izpaušanu ar jaunākajiem sasniegumiem atbilstošiem tehniskiem un organizatoriskiem pasākumiem, 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

92. Datu eksportētājs vēlas, lai personas datus 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 personas datus. Datu eksportētājs saņem apstrādes rezultātus no katra apstrādātāja atsevišķi un apvieno saņemtās daļas, lai iegūtu gala rezultātu, kas var būt personas dati vai apkopoti dati.

Ja

1. datu eksportētājs apstrādā personas datus 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. pārzinis, veicot rūpīgu attiecīgo datu analīzi, ir noteicis, ņemot vērā trūkstošo informāciju, par kuru būtu sagaidāms, ka tā varētu būt saņēmējvalstu iestāžu rīcībā un ka tās to varētu izmantot kā personas datu daļas, kuras tas nosūta apstrādātājiem, nevar sasaistīt ar identificētu vai identificējamu fizisku personu, pat izmantojot savstarpējas atsauces ar šādu informāciju,
6. nav pierādījumu par sadarbību starp valsts iestādēm, kuras atrodas katra apstrādātāja attiecīgajās jurisdikcijās, kas tām ļautu piekļūt visiem apstrādātāju rīcībā esošajiem personas datiem un ļautu atjaunot un izmantot personas datu saturu nekodētā formā apstākļos, kad šāda izmantošana neievērotu datu subjektu pamattiesību un brīvību būtību. Tāpat jebkuras valsts publiskām iestādēm nevajadzētu būt pilnvarām piekļūt personas datiem, kas ir apstrādātāju rīcībā visās skartajās jurisdikcijās.

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

Piemēri scenārijiem, kas attiecas uz gadījumiem, kad netiek noteikti *efektīvi* pasākumi

93. Atsevišķos scenārijos turpmāk aprakstītie pasākumi nav efektīvi, nodrošinot līdzvērtīgu aizsardzības līmeni datu nosūtīšanai uz trešajām valstīm. Tādēļ tie nav kvalificējami kā atbilstoši papildus pasākumi.

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

94. Datu eksportētājs nosūta personas datus vai nu elektroniski, vai darot tos pieejamus mākoņdatošanas pakalpojumu sniedzējam vai citam apstrādātājam, lai trešajā valstī tiktu apstrādāti personas dati saskaņā ar tā norādījumiem (piemēram, tehniskā atbalsta sniegšanai vai jebkāda veida mākoņapstrādei), un šie dati nav pseidonimizēti vai tos nav iespējams pseidonomizēt, kā aprakstīts 2. lietošanas gadījumā, vai šifrēti, kā aprakstīts 1. lietošanas gadījumā, jo apstrāde prasa piekļuvi datiem skaidrā veidā,

Ja

1. pārzinis nosūta personas 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 attiecīgajiem nosūtītajiem datiem pārsniedz to, kas demokrātiskā sabiedrībā ir nepieciešams un samērīgs, ja attiecīgajai nosūtīšanai praksē ir piemērojami problemātiski trešās valsts tiesību akti (skatīt 3. soli)[82].

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

95. Aprakstītajos scenārijos, kad nešifrēti personas dati ir tehniski nepieciešami apstrādātājam pakalpojuma sniegšanai, tādi pasākumi kā pārsūtīšanas šifrēšana un neaktīvo datu miera šifrēšana, nav uzskatāmas par papildus pasākumu, kas nodrošina līdzvērtīgu aizsardzības līmeni, ja datu importētāja rīcībā ir šifrēšanas atslēgas.

7. lietošanas gadījums. Personas datu nosūtīšana uzņēmējdarbības nolūkos, tostarp ar attālinātu piekļuvi

96. Datu eksportētājs nosūta personas datus vienībām trešajā valstī, lai tos izmantotu kopīgas uzņēmējdarbības nolūkos, vai nu elektroniski, vai darot tos pieejamus datu importētāja attālinātai piekļuvei, un šie dati netiek vai nevar būt pseidonimizēti, kā aprakstīts 2. lietošanas gadījumā, vai šifrēti, kā aprakstīts 1. lietošanas gadījumā, jo apstrāde prasa piekļuvi datiem

[82] 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.

skaidrā formā. Tipisks piemērs var būt pārzinis vai apstrādātājs, kas reģistrēts dalībvalsts teritorijā, nosūta personas datus pārzinim vai apstrādātājam trešajā 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 personas datus datu importētājam trešajā valstī, padarot tos pieejamus plaši izmantotā informācijas sistēmas veidā, kas ļauj importētājam tieši piekļūt datiem pēc paša izvēles, vai nosūtot tos tieši, atsevišķi vai vairumā, izmantojot sakaru pakalpojumu,
2. importētājs[83] datus skaidrā veidā apstrādā trešajā valstī (tostarp savām vajadzībām, ja importētājs ir pārzinis),
3. saņēmējvalsts iestādēm piešķirtās pilnvaras piekļūt nosūtītajiem datiem pārsniedz to, kas demokrātiskā sabiedrībā ir nepieciešams un samērīgs, ja attiecīgajai nosūtīšanai praksē piemēro problemātiskus trešās valsts tiesību aktus (skatīt 3. soli),

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

97. Aprakstītajos scenārijos, kad nešifrēti personas dati ir tehniski nepieciešami apstrādātājam pakalpojuma sniegšanai, tādu pasākumu veikšana kā pārsūtīšanas šifrēšana un neaktīvo datu nav uzskatāmas par papildinošu pasākumu, kas nodrošina līdzvērtīgu aizsardzības līmeni, ja datu importētāja rīcībā ir šifrēšanas atslēgas.

2.2 Papildu līgumiskie pasākumi

98. Šie pasākumi parasti sastāv no vienpusējām, divpusējām vai daudzpusējām[84] līgumsaistībām[85]. 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 personas datus[86].

99. 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 līdzvērtīgam ES garantētajam aizsardzības līmenim nepieciešamajiem nosacījumiem. Tā kā līgumisko pasākumu raksturs parasti nav saistošs šīs trešās valsts iestādēm,

---

[83] Tas var būt pārzinis vai apstrādātājs trešā valstī, kurš saņem vai piekļūst persondatiem, kas nosūtīti no EEZ.

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

[85] 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.

[86] 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).

ja vien tās nav līgumslēdzējas puses[87], šos pasākumus bieži ir nepieciešams apvienot 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.

100. 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 trešajām valstīm nosūtīto datu aizsardzību.

101. 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[88].

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

Paredzēt līgumsaistības, izmantojot konkrētus tehniskus pasākumus

103. Atkarībā no konkrētajiem nosūtīšanas apstākļiem (tostarp trešās valsts tiesību aktu praktiskās piemērošanas) līgumā, iespējams, jāparedz, ka nosūtīšanas īstenošanai jāievieš konkrēti tehniskie pasākumi (skatīt iepriekš piedāvātos tehniskos pasākumus).

104. 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:

105. Eksportētājs var pievienot līgumam pielikumus ar informāciju, ko importētājs, pieliekot visas pūles, nodrošinātu pirms līguma noslēgšanas 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 trešajā valstī. Tajā var arī uzsvērt importētāja pienākumu palīdzēt eksportētājam veikt novērtējumu un uzņemties atbildību par objektīvas, ticamas, būtiskas, pārbaudāmas un publiski pieejamas vai citādi pieejamas informācijas sniegšanu.

106. 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 personas datiem, jo īpaši izlūkošanas, tiesībaizsardzības, administratīvās un regulatīvās uzraudzības jomās, kas piemērojamas nosūtītajiem datiem;

[87] Lieta C-311/18 (Schrems II), 125. punkts.
[88] EST spriedums lietā C-311/18 (Schrems II), 132. punkts.

(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 personas datu 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 personas datiem, kurus importētājs ir saņēmis noteiktā laika posmā[89], 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[90];

precizēt, vai un cik lielā mērā importētājam ir likumīgi aizliegts sniegt iepriekš 1.–5. punktā minēto informāciju.

107. 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.

108. Efektivitātes nosacījumi:

- Importētājam jāspēj sniegt eksportētājam šāda veida informācija, ciktāl tam tā ir zināma, kad ir pieliktas visas pūles tās iegūšanā.
- 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 personas datu izpaušanu, nedz radīt cerības, ka turpmāk netiks saņemti piekļuves pieprasījumi.

***

109. 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 personas datiem; 2) nav mērķtiecīgi izveidojis vai mainījis savus uzņēmējdarbības procesus veidā, kas atvieglo piekļuvi personas datiem vai sistēmām; un 3) ka valsts tiesību akti vai valdības politika neprasa, lai importētājs izveido vai uztur apiešanas iespējas vai arī atvieglo piekļuvi

[89] 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.
[90] 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.

personas datiem vai sistēmām, vai lai importētāja valdījumā būtu šifrēšanas atslēga, vai arī tam būtu pienākums to nodot[91].

110. 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.
- 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 esamību ir uzzinājis.
- Gadījumos, kad datu importētājs ir atklājis personas datus, kas nosūtīti, pārkāpjot izvēlētā nosūtīšanas rīka saistības, līgumā var iekļaut arī kompensāciju no datu importētāja datu subjektam par jebkādu nodarīto materiālo un nemateriālo kaitējumu.

***

111. Eksportētājs var nostiprināt savas tiesības uz vietas un/vai attālināti veikt importētāja datu apstrādes iekārtu revīziju[92] 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.

112. Efektivitātes nosacījumi:

- Lai revīzija būtu pilnībā efektīva, tās tvērumam juridiski un tehniski būtu jāattiecas uz jebkādu importētāja apstrādātāju vai apakšapstrādātāju veikto personas datu apstrādi trešajā valstī.
- Piekļuvēm reģistriem un citiem līdzīgiem resursiem jābūt viltojumdrošām (piemēram, tām jābūt nemaināmām, izmantojot jaunākos šifrēšanas paņēmienus, piemēram, jaukšanas metodi, un tās arī regulāri jānosūta eksportētājam), lai revidenti varētu atrast pierādījumus par informācijas izpaušanu. Piekļuves reģistros un citos līdzīgos resursos būtu jānošķir no piekļuvēm, kas saistītas ar parasto uzņēmējdarbību, un piekļuvēm, kas saistītas ar pasūtījumiem vai piekļuves pieprasījumiem.

***

113. Ja sākotnēji tikuši novērtēti importētāja trešās valsts tiesību akti un prakse un ticis uzskatīts, ka tie eksportētāja nosūtītajiem datiem nodrošina līdzvērtīgu aizsardzības līmeni ES paredzētajam, eksportētājs joprojām var paredzēt datu importētāja pienākumu nekavējoties, ja situācija mainās,

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

[92] 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.

informēt datu eksportētāju, ja tas nespēj izpildīt līgumā noteiktās saistības un līdz ar to prasīto "līdzvērtīga datu aizsardzības līmeņa" standartu[93].

114. Šī nespēja nodrošināt atbilstību var rasties sakarā ar izmaiņām trešās valsts tiesību aktos vai praksē[94]. 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.

115. 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 personas datu 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 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.

***

116. 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

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

[94] Skatīt sprieduma lietā C-311/18 (Schrems II) 139. punktu, kurā Tiesa apgalvo, ka "lai gan 5. klauzulas d) punkta i) apakšpunkts ļauj personas datu 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 personas datu pārzinim par tiesībaizsardzības iestādes saistošu pieprasījumu izpaust personas datus, viņam tomēr atbilstoši LSK lēmuma pielikuma 5. klauzulas a) punktam ir jāinformē personas datu pārzinis par neiespējamību izpildīt datu aizsardzības standartklauzulu prasības".

rīkojumu izpaust personas datus vai tamlīdzīgi. Ja šis paziņojums netiek atjauninās, tā ir norāde eksportētājam, ka importētājs, iespējams, ir saņēmis rīkojumu.

117. 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

118. 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 personas datus, ja tas nav obligāti saskaņā ar piemērojamiem procesuālajiem noteikumiem. Datu importētājs arī apņemas sniegt minimālo pieļaujamo informācijas daudzumu, atbildot uz rīkojumu, balstoties uz pamatotu rīkojuma interpretāciju.

119. Efektivitātes nosacījumi:

- Trešās valsts tiesiskajā regulējumā jābūt efektīviem tiesiskajiem līdzekļiem, 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 apturošai iedarbībai. Pretējā gadījumā valsts iestādēm joprojām būs piekļuve personu datiem, un jebkurai izrietošai prasībai par labu indivīdam būtu ierobežota ietekme uz viņa/viņas kaitējuma atlīdzības pieprasījumu par datu izpaušanas negatīvajām sekām.
- Importētājam jāspēj dokumentēt un eksportētājam pierādīt darbības, kuras tas ir veicis, pieliekot visas pūles, lai izpildītu šīs saistības.

***

120. Identiskā situācijā, kā aprakstīts iepriekš, importētājs var apņemties informēt pieprasījuma iesniedzēju valsts iestādi par pasūtījuma neatbilstību VDAR 46. panta nosūtīšanas rīkā[95] 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.

121. 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

122. Līgumā var paredzēt, ka personas datiem, kas parastās uzņēmējdarbības laikā (tostarp atbalsta sniegšanas gadījumos) nosūtīti kā parasts teksts, var piekļūt tikai ar eksportētāja un/vai datu subjekta skaidru vai netiešu vienošanos attiecībā uz īpašu piekļuvi datiem.

123. 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)[96].
- Valsts noteikumi vai politika, kas uzliek importētājam pienākumu neizpaust piekļuves rīkojuma faktu, var padarīt šo klauzulu neefektīvu, ja to nevar papildināt ar tehniskām 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.

***

[95] *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.

[96] VDAR 4. panta 11. punkts.

124. Līgums varētu uzlikt importētājam un/vai eksportētājam pienākumu nekavējoties informēt datu subjektu par pieprasījumu vai rīkojumu, kas saņemts no trešās valsts publiskajām iestādēm, vai par importētāja nespēju izpildīt līgumsaistības, lai datu subjekts varētu pieprasīt informāciju un efektīvi vērsties tiesā (piemēram, iesniedzot prasību savai kompetentajai uzraudzības iestādei un/vai tiesu iestādei un pierādīt savas tiesības celt prasību trešās valsts tiesās), tostarp kompensāciju no datu importētāja par jebkādu materiālu un nemateriālu kaitējumu, kas nodarīts, atklājot viņa/viņas personas datus, kuri nosūtīti saskaņā ar izvēlēto nosūtīšanas rīku, pārkāpjot tajā ietvertās saistības.

125. Efektivitātes nosacījumi:

- Ar šādu paziņojumu varētu brīdināt datu subjektu par iespējamu trešo valstu publisko 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 personas datu nosūtīšanas apturēšanu vai izbeigšanu sakarā ar to, ka importētājs nespēj izpildīt savas līgumsaistības piekļuves pieprasījuma saņemšanas rezultātā.

***

126. 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.

127. Efektivitātes nosacījumi

- Dažu valstu noteikumi var neļaut datu importētājam sniegt šāda veida palīdzību tieši datu subjektiem, lai gan tie var ļaut datu importētājam nodrošināt šo palīdzību datu subjektiem.
- 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 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, tostarp attiecībā uz uzraudzības pasākumiem.

2.3 Organizatoriskie pasākumi

128. Papildu organizatoriski pasākumi var būt iekšējā politika, organizatoriskās metodes un standarti, kurus pārziņi un apstrādātāji var piemērot paši sev, kā arī datu importētājiem trešajās valstīs. Tie var palīdzēt nodrošināt konsekvenci personas datu 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 personas datu aizsardzības līmeni, kas būtībā līdzvērtīgs ES garantētajam.

129. 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

130. 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 komandas iecelšanu, kuru veido IT, datu aizsardzības un privātuma tiesību eksperti, pieprasījumu, kuri skar no ES nosūtīto personas datu, 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.

131. Jāizstrādā īpašas apmācības procedūras personālam, kurš atbild par valsts iestāžu pieprasījumu par piekļuvi personas datiem 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 personas datiem, 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.

132. Efektivitātes nosacījumi:

- Šīs politikas ir izskatāmas tikai tajos gadījumos, kad trešās valsts publisko iestāžu pieprasījums ir saderīgs ar ES tiesību aktiem[97]. Ja pieprasījums nav saderīgs, ar šo politiku nepietiks, lai

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

nodrošinātu līdzvērtīgu personas datu aizsardzības līmeni, un, kā minēts iepriekš, nosūtīšana ir jāpārtrauc vai jāievieš atbilstoši papildinošie pasākumi, lai novērstu no piekļuvi.

Pārredzamības un pārskatatbildības pasākumi

133. 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 jāsniedz attiecīgajiem datu subjektiem.

134. 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 šādas nespējas dēļ netiktu nodrošināts pietiekams aizsardzības līmenis.

***

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

136. 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

137. 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 personas datiem. 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).

138. 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 personas datu 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.

***

139. 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 personas datu starptautisku nosūtīšanu.

140. 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 personas datu nosūtīšanas nepieciešamības novērtējums, pārskats par piemērojamiem trešās valsts tiesību aktiem un garantijām, kuras importētājs apņēmies ieviest.

Standartu un paraugprakses pieņemšana

141. 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.

Citi

142. 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 personas datu aizsardzības līmenis.

***

143. Datu importētāja apņemšanās neveikt personas datu 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 personas datu aizsardzības līmeni[98].

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

3. PIELIKUMS IESPĒJAMIE INFORMĀCIJAS AVOTI TREŠĀS VALSTS NOVĒRTĒJUMAM

144. Jūsu datu importētājam būtu jāspēj norādīt attiecīgos avotus un informāciju par trešo valsti, kurā tas ir reģistrēts, tostarp par importētājam piemērojamiem tiesību aktiem un praksi un nosūtītajiem datiem. Jūs un importētājs varat atsaukties uz vairākiem informācijas avotiem, piemēram, tiem, kas neizsmeļoši uzskaitīti turpmāk un sakārtoti prioritārā secībā:

- Eiropas Savienības Tiesas (EST) un Eiropas Cilvēktiesību tiesas (ECT)[99] judikatūra, kā minēts Eiropas būtisko garantiju ieteikumos[100];
- Lēmumi par aizsardzības līmeņa pietiekamību galamērķa valstī, ja nosūtīšana balstīta uz citu juridisko pamatu[101];
- Starpvaldību organizāciju, piemēram, Eiropas Padomes[102], citu reģionālo struktūru[103] rezolūcijas un ziņojumi; un ANO struktūras un aģentūras (piemēram, ANO Cilvēktiesību padome[104], Cilvēktiesību komiteja[105]);
- Kompetento regulatīvo tīklu, piemēram, Pasaules privātuma asamblejas (*GPA*), ziņojumi un analīze;[106]
- Valsts judikatūra vai lēmumi, ko pieņēmušas neatkarīgas tiesu vai administratīvās iestādes, kas ir kompetentas datu privātuma un trešo valstu datu aizsardzības jomā;
- Neatkarīgu pārraudzības vai parlamentāro struktūru ziņojumi;
- Ziņojumi, kuru pamatā ir praktiskā pieredze saistībā ar iepriekšējiem informācijas izpaušanas pieprasījumiem no publiskām iestādēm vai šādu pieprasījumu neesamība no vienībām, kas darbojas tajā pašā nozarē, kurā darbojas importētājs;
- *Warrant Canary* no citām struktūrām, kas apstrādā datus tajā pašā jomā kā importētājs;
- Ziņojumi, ko sagatavojušas vai pasūtījušas tirdzniecības palātas, uzņēmēju, profesionālās un tirdzniecības asociācijas, valsts diplomātiskās, tirdzniecības un ieguldījumu aģentūras eksportētājam vai citām trešajām valstīm, kas eksportē uz trešo valsti, uz kuru tiek veikta nosūtīšana;
- Akadēmisko institūciju un pilsoniskās sabiedrības organizāciju (piemēram, NVO) ziņojumi;

---

[99] Skatīt ECT judikatūras par masu novērošanu faktu lapu:

[100] Skatīt EDAK Ieteikumus 02/2020 attiecībā uz Eiropas būtiskajām garantijām uzraudzības pasākumiem, 2020. gada 10. novembris, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en

[101] 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

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

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

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

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

[106] Skatīt, piemēram, https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf

- Privātu uzņēmējdarbības izpētes pakalpojumu sniedzēju ziņojumi par uzņēmumu finanšu, regulatīvajiem un reputācijas riskiem;
- Paša importētāja *Warrant Canary*[107];
- Pārskatāmības ziņojumi ar nosacījumu, ka tajos ir skaidri minēts, ka piekļuves pieprasījumi nav saņemti. Pārredzamības ziņojumi, kuros klusēts par šo jautājumu, nebūtu uzskatāmi par pietiekamiem pierādījumiem, jo šie ziņojumi visbiežāk ir vērsti uz piekļuves pieprasījumiem, kas saņemti no tiesībaizsardzības iestādēm, un sniedz skaitļus tikai par šo aspektu, vienlaikus klusējot par saņemtajiem piekļuves pieprasījumiem valsts drošības nolūkos. Tas nenozīmē, ka piekļuves pieprasījumi netika saņemti, bet gan to, ka šo informāciju nevar kopīgot[108];
- Importētāja iekšējie paziņojumi vai ieraksti, kuros skaidri norādīts, ka pietiekami ilgu laikposmu nav saņemti piekļuves pieprasījumi; un priekšroku dodot paziņojumiem un ierakstiem, kas saistīti ar importētāja atbildību un/vai ko sagatavojuši iekšējās amatpersonas ar zināmu autonomiju, piemēram, iekšējie revidenti, datu aizsardzības speciālisti u. c.[109]

[107] Nosacījumi importētāja dokumentētās praktiskās pieredzes apsvēršanai saistībā ar attiecīgiem iepriekšējiem piekļuves pieprasījumiem, kas saņemti no valsts iestādēm trešā valstī, skatīt 47. punktā.
[108] Turpat.
[109] Turpat.