Datu aizsardzības būtisko garantiju instrumentu kopums sadarbībai izpildes jautājumos starp EEZ datu aizsardzības iestādēm un trešo valstu kompetentajām datu aizsardzības iestādēm

Pieņemts 2022. gada 14. martā

Pieņemts

Eiropas Datu aizsardzības kolēģija,

ņemot vērā 70. panta 1. punkta u) apakšpunktu un 50. panta a) punktu 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 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. punktu,

IR PIEŅĒMUSI ŠĀDU DOKUMENTU.

Saistībā ar VDAR 50. pantu par starptautisko sadarbību ar trešo valstu kompetentajām datu aizsardzības iestādēm ir izstrādāts turpmāk minētais datu aizsardzības būtisko garantiju instrumentu kopums, kas jānoslēdz papildus izpildes sadarbības nolīgumam vai jāiekļauj tajā.

Šīs garantijas var paredzēt vai nu administratīvā vienošanās, vai starptautiskā nolīgumā. To formulējums būs attiecīgi jāpielāgo atkarībā no tā, vai izstrādātais instruments būs administratīva vienošanās vai starptautisks nolīgums, un no veicamās nosūtīšanas konkrētajiem apstākļiem. Kā atgādināts Eiropas Datu aizsardzības kolēģijas pamatnostādnēs 2/2020 par VDAR 46. panta 2. punkta a) apakšpunktu un 46. panta 3. punkta b) apakšpunktu[2], noslēdzot administratīvu vienošanos, ir jāveic konkrēti pasākumi, lai nodrošinātu efektīvas individuālās tiesības, tiesisko aizsardzību un pārraudzību, vēlams, ar saņēmējas puses apliecinājumu, ka tās valsts tiesību aktos šīs būtiskās garantijas jau ir paredzētas. Ar starptautiskiem nolīgumiem var paredzēt garantijas tieši starptautiskā nolīguma ietvaros vai balstīties uz trešās valsts tiesību aktos jau iekļautiem elementiem.

Konkrēta informācija attiecībā uz administratīvām vienošanās ir izcelta pelēkā krāsā, bet konkrēta informācija attiecībā uz starptautiskiem nolīgumiem ir izcelta zilā krāsā.

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

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

I. DEFINĪCIJAS[3]

Šajā instrumentā:

a) "persondati" ir jebkura informācija par identificētu vai identificējamu fizisku personu ("**datu subjekts**"); identificējama fiziska persona ir persona, kuru tieši vai netieši var identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, minētās personas vārdu, uzvārdu, atrašanās vietas datiem, identifikācijas numuru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem;

b) "persondatu apstrāde" ("**apstrāde**") ir jebkura ar persondatiem vai persondatu kopumiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem, piemēram, vākšana, reģistrācija, organizēšana, strukturēšana, glabāšana, pielāgošana vai pārveidošana, izguve, aplūkošana, izmantošana, izpaušana nosūtot, izplatot vai citādi darot tos pieejamus, saskaņošana vai kombinēšana, apstrādes ierobežošana, dzēšana vai iznīcināšana;

c) "[pušu] kompetentā iestāde"[4] ir iestāde, kuras kompetencē ir datu aizsardzības tiesību aktu izpilde, proti, [X] EEZ un [Y] trešā valstī. Kompetentajām iestādēm saskaņā ar šo instrumentu ir regulatīvās pilnvaras un pienākumi, kas ietver datu aizsardzības noteikumu piemērošanas uzraudzību un izpildi, sūdzību izskatīšanu, datu aizsardzības noteikumu iespējamo pārkāpumu izmeklēšanu un, ja nepieciešams, sankciju piemērošanu;

d) "saņēmēja kompetentā iestāde" ir kompetentā iestāde, kas saņem persondatus, kuri nosūtīti no otras kompetentās iestādes;

e) "persondatu kopīgošana" ir persondatu tālāka kopīgošana (kuru veic kompetentā iestāde, kas saņem datus no EEZ kompetentās datu aizsardzības iestādes) ar trešo personu savā valstī saskaņā ar [izpildes sadarbības nolīgumu];

f) "tālāka nosūtīšana" ir persondatu nosūtīšana, kuru veic saņēmēja kompetentā iestāde, trešai personai citā valstī;

g) "īpašas persondatu / sensitīvu datu kategorijas" ir dati, kas atklāj rasi vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās, un ģenētiskie dati, biometriskie dati, ko apstrādā, lai veiktu fiziskas personas unikālu identifikāciju, kā arī veselības dati vai dati par fiziskas personas dzimumdzīvi vai seksuālo orientāciju un dati par sodāmību un pārkāpumiem;

h) [**"valsts piemērojamie datu aizsardzības tiesību akti"** ir [piemērojamie tiesību akti];]

[i) ["izpildes sadarbības nolīgums" jeb "ISN"[5] ir sadarbības nolīgums izpildes jomā starp [trešās valsts kompetento iestādi] un [Eiropas Ekonomikas zonas iestādi], kas paredzēts, lai veicinātu sadarbību un informācijas apmaiņu;]][6]

[3] Šīs definīcijas izriet no VDAR.
[4] To varētu ievietot starptautiskā nolīgumā.
[5] Šeit jāiekļauj nolīguma nosaukums, kā arī abu attiecīgo (EEZ un trešās valsts) iestāžu nosaukumi.
[6] Šī definīcija jāsniedz administratīvā vienošanās, jo starptautiskā nolīgumā jāiekļauj gan datu aizsardzības garantijas, gan attiecīgās sadarbības klauzulas.

j) "persondatu aizsardzības pārkāpums" ir drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto persondatu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem;

k) "profilēšana" ir jebkura veida automatizēta persondatu apstrāde, kas izpaužas kā persondatu izmantošana nolūkā izvērtēt konkrētus ar fizisku personu saistītus personiskus aspektus, jo īpaši analizēt vai prognozēt aspektus saistībā ar minētās fiziskās personas sniegumu darbā, ekonomisko situāciju, veselību, personīgām vēlmēm, interesēm, uzticamību, uzvedību, atrašanās vietu vai pārvietošanos;

l) "datu subjekta tiesības" šajā nolīgumā attiecas uz šādām tiesībām:

— "tiesības uz informāciju" ir datu subjekta tiesības kodolīgā, pārskatāmā, saprotamā un viegli pieejamā veidā saņemt informāciju par savu persondatu apstrādi,

— "piekļuves tiesības" ir datu subjekta tiesības saņemt no kompetentās iestādes, kas nosūta vai saņem datus, apstiprinājumu par to, vai tā persondati tiek vai netiek apstrādāti, kā arī konkrētu informāciju par apstrādi, tostarp par apstrādes nolūku, attiecīgo persondatu kategorijām, saņēmējiem, kuriem persondati tiek izpausti, paredzēto glabāšanas laikposmu un tiesiskās aizsardzības iespējām, un datu apstrādes gadījumā piekļūt tiem persondatiem, kas par šo subjektu savākti, kā arī viegli un saprātīgos intervālos īstenot minētās tiesības, lai zinātu par apstrādi un pārliecinātos par tās likumīgumu,

— "tiesības uz labošanu" ir datu subjekta tiesības uz to, lai puse bez liekas kavēšanās izlabotu vai papildinātu datu subjekta neprecīzos persondatus,

— "tiesības uz dzēšanu" ir datu subjekta tiesības uz to, lai puse izdzēstu tā persondatus, ja persondati vairs nav nepieciešami saistībā ar nolūkiem, kādiem tie tika vākti vai apstrādāti, vai ja dati ir savākti vai apstrādāti nelikumīgi,

— "tiesības iebilst" ir datu subjekta tiesības jebkurā laikā, pamatojoties uz tā konkrēto situāciju, iebilst pret puses veikto tā persondatu apstrādi, kā rezultātā puse vairs neapstrādā datus, ja vien puse neuzrāda pārliecinošus leģitīmus iemeslus apstrādei, kas ir svarīgāki par datu subjekta interesēm, tiesībām un brīvībām, vai likumīgu prasību celšanai, īstenošanai vai aizstāvībai,

— "apstrādes ierobežošanas tiesības" ir datu subjekta tiesības ierobežot savu persondatu apstrādi, ja datu subjekts apstrīd persondatu precizitāti, uz laiku, kurā pārzinis var pārbaudīt šo persondatu precizitāti, ja apstrāde ir nelikumīga un datu subjekts iebilst pret persondatu dzēšanu un tā vietā pieprasa to izmantošanas ierobežošanu, ja pusei persondati vairs nav vajadzīgi tiem nolūkiem, kādiem tie tika vākti, un datu subjekts iebilst pret to dzēšanu, taču tie ir nepieciešami datu subjektam, lai celtu, īstenotu vai aizstāvētu likumīgas prasības,

— "tiesības nebūt automatizētu lēmumu, tostarp profilēšanas, subjektam" ir datu subjekta tiesības nebūt tādu lēmumu subjektam, kuru pamatā ir tikai automatizēta apstrāde, tostarp profilēšana, kas attiecībā uz datu subjektu rada tiesiskās sekas vai līdzīgā veidā ievērojami ietekmē datu subjektu.

II. INSTRUMENTA NOLŪKS UN DARBĪBAS JOMA

Šā instrumenta nolūks ir paredzēt atbilstošas garantijas [un atbilstošu konfidencialitātes ievērošanu[7]] attiecībā uz persondatiem, ko [X] nosūtījusi [Y] saskaņā ar VDAR 46. panta 3. punktu un, sadarbības gaitā, saskaņā ar [ISN / šo instrumentu]. Skartās persondatu kategorijas, ko nosūta un apstrādā saskaņā ar [ISN / šo instrumentu], puses uzskaita īpašā pielikumā.

Puses vienojas, ka persondatu nosūtīšanu, kā noteikts [ISN / šajā instrumentā], starp [X] un [Y] reglamentē šā persondatu apstrādes instrumenta noteikumi [īstenojot to attiecīgās izpildes darbības][8] / [saistībā ar to, kā kompetentās iestādes īsteno attiecīgās izpildes darbības.][9]. [Šis instruments ir paredzēts, lai papildinātu ISN starp [X] un [Y].][10]

[[X] un [Y] apstiprina, ka tām ir tiesības rīkoties saskaņā ar šā instrumenta noteikumiem un ka tām nav iemesla uzskatīt, ka spēkā esošās piemērojamās juridiskās prasības tām liedz to darīt.

[X] un [Y] apstiprina, ka tās var pilnībā ievērot šajā nolīgumā paredzētās garantijas, pamatojoties uz piemērojamajām juridiskajām prasībām. [X] un [Y] paredz garantijas, lai aizsargātu persondatus, izmantojot likumu, noteikumu un savu iekšējo vadlīniju un procedūru kombināciju.][11]

[Katra puse nodrošina, lai kompetentā iestāde rīkotos saskaņā ar šā instrumenta noteikumiem un nekādas piemērojamās juridiskās prasības neliegtu kompetentajai iestādei to darīt][12].

III. DATU APSTRĀDES PRINCIPI

1. Nolūka ierobežojums. Persondatus, kas nosūtīti starp [X] un [Y], pati saņēmēja kompetentā iestāde var apstrādāt tikai tādēļ, lai pildītu izpildes funkcijas atbilstīgi VDAR [X] gadījumā un atbilstīgi [piemērojamajiem trešās valsts tiesību aktiem] [Y] gadījumā un lai izpildītu datu aizsardzības noteikumus, kas ir [Y] un [X] jurisdikcijā. Šādu datu tālāku kopīgošanu (tostarp šādas kopīgošanas nolūku), kas nepieciešama tieši saistītām izmeklēšanām/tiesvedībām un kas [Y] gadījumā ir saskaņā ar [attiecīgajiem piemērojamajiem trešās valsts tiesību aktiem] un [X] gadījumā ir saskaņā ar VDAR un piemērojamajiem valsts tiesību aktiem, regulē 7. punkts. [Y] neapstrādā no [X] saņemtos persondatus citā nolūkā, kā vien šajā instrumentā paredzētajā nolūkā, un otrādi, [X] neapstrādā no [Y] saņemtos persondatus citā nolūkā, kā vien šajā instrumentā paredzētajā nolūkā.

2. Datu kvalitāte un proporcionalitāte. [X] un [Y] nosūtītajiem persondatiem jābūt precīziem, adekvātiem un attiecīgiem, un to apjoms nedrīkst būt pārmērīgi liels iepretim nolūkiem, kādiem tie nosūtīti un pēc tam apstrādāti. Kompetentā iestāde informē otru kompetento iestādi, ja tai kļūst zināms, ka iepriekš nosūtītā vai saņemtā informācija ir neprecīza (nepareiza vai novecojusi) un/vai tā ir jāatjaunina. Šādā gadījumā kompetentās iestādes, ņemot vērā persondatu nosūtīšanas nolūkus, veic visus atbilstošos labojumus, kas attiecīgi var ietvert persondatu papildināšanu, dzēšanu, apstrādes ierobežošanu, labošanu vai citādu koriģēšanu.

[7] Dokumenta beigās sk. III.a punktu par konfidencialitātes ievērošanu un dienesta noslēpuma aizsardzību, kurš vajadzības gadījumā jāievieto atkarībā arī no trešās valsts tiesību aktiem.
[8] Administratīvā vienošanās.
[9] Starptautiskā nolīgumā.
[10] Tas būtu jāparedz administratīvā vienošanās.
[11] Tas būtu jāievieto administratīvā vienošanās.
[12] To varētu ievietot starptautiskā nolīgumā.

Persondati jāuzglabā veidā, kas ļauj identificēt datu subjektus, ne ilgāk, kā tas nepieciešams nolūkiem, kādiem dati vākti vai kādiem tos tālāk apstrādā, vai tik ilgi, cik paredzēts piemērojamajos normatīvajos aktos, ja [X] ir informējusi [Y] par šiem EEZ piemērojamajiem noteikumiem un tajos paredzēto persondatu glabāšanas maksimālo laikposmu un [Y] ir informējusi [X] par piemērojamajiem normatīvajiem aktiem un tajos paredzēto persondatu glabāšanas maksimālo laikposmu, un maksimālo laikposmu uzskata par samērīgu un nepieciešamu demokrātiskā sabiedrībā saskaņā ar ES standartiem. Minēto informāciju reģistrē šā instrumenta pielikumā. Puses ievieš atbilstīgas procedūras saskaņā ar šo instrumentu saņemtās informācijas galīgai iznīcināšanai.

3. Pārredzamība. [X] un [Y] sniedz vispārīgu paziņojumu, publicējot šo instrumentu savās tīmekļa vietnēs. Gan [X], gan [Y] sniedz datu subjektiem informāciju par persondatu nosūtīšanu un tālāku apstrādi. Gan [X], gan [Y] principā sniedz datu subjektiem vispārīgu paziņojumu par: a) to, kā un kāpēc tā var apstrādāt un nosūtīt persondatus, b) to vienību veidu, kurām šādus datus var nosūtīt, c) tiesībām, kas datu subjektiem ir pieejamas saskaņā ar piemērojamajām juridiskajām prasībām, tostarp to, kā šīs tiesības īstenot, d) informāciju, kas attiecas uz jebkuru piemērojamo kavēšanos vai ierobežojumiem šādu tiesību īstenošanai, tostarp ierobežojumiem, kurus piemēro persondatu nosūtīšanas gadījumā, un e) kontaktinformāciju strīda atrisināšanas lūguma vai prasības iesniegšanai. Šis paziņojums stājas spēkā, kad gan [X], gan [Y] publicē minēto informāciju savā tīmekļa vietnē kopā ar šo instrumentu.

[X] sniedz datu subjektiem individuālu paziņojumu saskaņā ar paziņošanas prasībām un piemērojamajiem VDAR izņēmumiem un ierobežojumiem (kā noteikts VDAR 14. un 23. pantā). Tālākas kopīgošanas un tālākas nosūtīšanas gadījumā [Y] arī sniedz individuālu paziņojumu, un otrādi — [X] to dara attiecībā uz [Y].

Ja pēc jebkādu piemērojamo individuālā paziņojuma izņēmumu izskatīšanas un pēc apspriedēm ar [Y] [X] secina, ka saskaņā ar VDAR ir jāinformē datu subjekts par tā persondatu kopīgošanu vai nosūtīšanu [Y], [X] par to paziņo [Y] pirms šāda individuāla paziņojuma sniegšanas.

4. Drošība un konfidencialitāte. [X] un [Y] atzīst, ka **I pielikumā** [X] ir sniegusi informāciju, aprakstot savus tehniskos un organizatoriskos pasākumus saskaņā ar VDAR, un ka [Y] ir sniegusi informāciju, aprakstot savus tehniskos un organizatoriskos drošības pasākumus, ko [X] uzskata par atbilstošiem, lai aizsargātos pret persondatu nejaušu vai nelikumīgu iznīcināšanu, nozaudēšanu, pārveidošanu, izpaušanu vai piekļuvi tiem. [Y] piekrīt paziņot [X] par visām tehnisko un organizatorisko drošības pasākumu izmaiņām, kas varētu negatīvi ietekmēt aizsardzības līmeni, kuru persondatiem nodrošina šis nolīgums, un atjaunināt informāciju **I pielikumā**, ja šādas izmaiņas tiek veiktas. Šādā gadījumā [Y] sniedz [X] attiecīgu paziņojumu vismaz divus mēnešus pirms to stāšanās spēkā. Un otrādi — [X] informē [Y] saskaņā ar tādiem pašiem nosacījumiem un attiecīgi atjaunina I pielikumu.

[Y] iesniedz [X] savu piemērojamo tiesību aktu un/vai noteikumu aprakstu, kas attiecas uz konfidencialitāti un sekām sakarā ar jebkādu nepubliskojamas vai konfidenciālas informācijas

nelikumīgu izpaušanu vai iespējamiem šo tiesību aktu un/vai noteikumu pārkāpumiem, un otrādi — [X] sniedz tādu pašu informāciju [Y][13][14].

Gadījumā, ja saņēmēja kompetentā iestāde uzzina par persondatu aizsardzības pārkāpumu, kas ietekmē persondatus, kuri nosūtīti saskaņā ar šo instrumentu, tā bez liekas kavēšanās un, ja iespējams, ne vēlāk kā 24 stundu laikā no brīža, kad tai kļuvis zināms par šādu persondatu ietekmējumu, informē otru kompetento iestādi. Paziņotāja kompetentā iestāde arī pēc iespējas ātrāk izmanto saprātīgus un piemērotus līdzekļus, lai novērstu persondatu aizsardzības pārkāpumu un samazinātu iespējamās nelabvēlīgās sekas.

Ja ir iespējams, ka persondatu aizsardzības pārkāpums rada augstu risku fiziskās personas tiesībām un brīvībām, [X] un [Y] bez liekas kavēšanās ziņo datu subjektam par persondatu aizsardzības pārkāpumu, lai tas varētu veikt nepieciešamos piesardzības pasākumus. Paziņojumā apraksta persondatu aizsardzības pārkāpuma raksturu, kā arī sniedz ieteikumus par to, kā attiecīgā fiziskā persona var mīkstināt iespējamās nelabvēlīgās sekas. Šādu paziņošanu datu subjektam veic cik vien iespējams ātri, ja vien kompetentā iestāde nav īstenojusi atbilstīgus tehniskos un organizatoriskos aizsardzības pasākumus un šie pasākumi nav piemēroti persondatiem, ko skāris persondatu aizsardzības pārkāpums, vai tā nav veikusi turpmākus pasākumus, ar ko nodrošina, lai vairs nevarētu materializēties augstais risks attiecībā uz datu subjektu tiesībām un brīvībām, vai tas neprasītu nesamērīgi lielas pūles.

5. Datu subjekta tiesības. Datu subjekts, kura persondati ir nosūtīti [Y], var īstenot savas datu subjekta tiesības, kas definētas I punkta j) apakšpunktā, attiecībā uz datiem, kas saņemti un apstrādāti saskaņā ar instrumentu.

Datu subjekts var tieši iesniegt pieprasījumu [X] vai [Y].

[X] kontaktinformācija:

— pa e-pastu uz šādu adresi: Xxx,

— pa pastu uz šādu adresi:

XXXxxx,

[Y] kontaktinformācija:

— pa e-pastu uz šādu adresi: Xxx,

— pa pastu uz šādu adresi:

XXXxxx.

Datu subjekts var arī pieprasīt, lai [X] identificē visus persondatus, kas nosūtīti [Y], un pieprasīt, lai [X] pārliecinās [Y], ka persondati ir pilnīgi, precīzi un, ja piemērojams, atjaunināti un ka apstrāde notiek saskaņā ar šajā nolīgumā noteiktajiem persondatu apstrādes principiem. [Y] saprātīgi un laikus izskata

[13] Sk. I pielikumu.

[14] Starptautiskā nolīgumā: starptautiskais nolīgums arī var papildināt [Y] piemērojamos tiesību aktus un/vai noteikumus, ja [Y] tiesiskajā regulējumā to trūkst vai tie nav pietiekami, lai sniegtu vajadzīgās garantijas un nodrošinātu atbilstīgu aizsardzības līmeni.

jebkuru šādu pieprasījumu no [X] attiecībā uz visiem persondatiem, ko [X] nosūtījusi [Y]. Saņemot pieprasījumu no datu subjekta, [X] var arī pieprasīt no [Y] informāciju par [Y] veiktu šādu persondatu tālāku kopīgošanu un tālāku nosūtīšanu, lai [X] izpildītu savus pienākumus izpaust informāciju datu subjektam saskaņā ar [VDAR un [valsts tiesību aktiem, kas piemērojami [Y]]][15] / [šo instrumentu][16]. Saņemot šādu pieprasījumu no [X], [Y] sniedz [X] visu informāciju, kura ir bijusi pieejama [Y], par šādu persondatu apstrādi, ko veic trešā persona, ar kuru [Y] ir kopīgojusi vai kurai nosūtījusi šādus persondatus. [Y] arī saprātīgi un laikus izskata jebkuru šādu pieprasījumu no [X] attiecībā uz visiem persondatiem, ko [X] nosūtījusi [Y].

Pēc tā persondatu nosūtīšanas [X] viena mēneša laikā sniedz arī informāciju datu subjektam par darbību, kas veikta pēc tā pieprasījuma. [X] viena mēneša laikā pēc pieprasījuma saņemšanas informē datu subjektu arī par darbības neveikšanas iemesliem un par iespēju iesniegt sūdzību un vērsties tiesā. [X] un [Y] var veikt atbilstošus pasākumus, piemēram, pieprasīt saprātīgu maksu administratīvo izmaksu segšanai vai atteikties rīkoties pēc datu subjekta pieprasījuma, kas ir acīmredzami nepamatots vai pārmērīgs.

Datu subjekta tiesības var tikt ierobežotas, lai novērstu to kompetento iestāžu uzraudzības vai izpildes funkciju aizskārumu vai kaitējumu, kuras rīkojas, īstenojot tām piešķirtās oficiālās pilnvaras, attiecībā uz svarīgiem plašas sabiedrības interešu mērķiem, kas atzīti [Y trešā valstī] un [kompetentajā dalībvalstī] vai Eiropas Savienībā, tostarp pamatojoties uz starptautiskās sadarbības savstarpības principu. Ierobežojumam jābūt nepieciešamam, samērīgam un likumā noteiktam, un to piemēro tikai tik ilgi, kamēr pastāv ierobežojuma iemesls.

Ar jebkuru strīdu vai prasību, ko datu subjekts ceļ par tā persondatu apstrādi saskaņā ar šo instrumentu, var vērsties attiecīgi pie [X], [Y] vai abām iestādēm, kā noteikts 8. punktā.

[X] un [Y] vienojas, ka tās nepieņems juridisku lēmumu attiecībā uz datu subjektu, pamatojoties tikai uz persondatu automatizētu apstrādi, tostarp profilēšanu, bez cilvēka līdzdalības.

6. Īpašas persondatu / sensitīvu datu kategorijas. Īpašas persondatu / sensitīvu datu kategorijas, kas definētas I punkta e) apakšpunktā, [X] nenosūta [Y], ja vien tās nav nepieciešamas, lai izskatītu sūdzības, izmeklētu iespējamus datu aizsardzības noteikumu pārkāpumus un, ja nepieciešams, piemērotu korektīvus pasākumus. Ja tās tiek nosūtītas, [Y] ievieš papildu garantijas, kas jānosaka katrā gadījumā atsevišķi, piemēram, piekļuves ierobežojumus, ierobežojumus attiecībā uz nolūkiem, kādiem informāciju var apstrādāt, ierobežojumus attiecībā uz tālāku nosūtīšanu, vai īpašas garantijas, piemēram, papildu drošības pasākumus, saistībā ar kuriem īpaši jāapmāca darbinieki, kam atļauts piekļūt informācijai.

7. Persondatu tālāka kopīgošana. [Y] kopīgo no [X] saņemtos datus tikai ar tām vienībām, kas norādītas[17] [ISN][18] / [šajā instrumentā][19], un tikai tad, ja tas nepieciešams konkrētās izpildes darbības veikšanai.

[15] Administratīvā vienošanās.
[16] Starptautiskā nolīgumā.
[17] Sk. arī II pielikumu.
[18] Administratīvā vienošanās.
[19] Starptautiskā nolīgumā.

Gadījumā, ja [Y] plāno kopīgot jebkādus persondatus ar jebkuru trešo personu, kura norādīta [ISN][20] / [šajā instrumentā][21], [Y] pieprasa iepriekšēju rakstisku [X] atļauju un kopīgo šos persondatus tikai tad, ja trešā persona apņemas ievērot tos pašus datu aizsardzības principus un garantijas, kas paredzēti šajā instrumentā. Pieprasot šādu iepriekšēju rakstisku atļauju, [Y] norāda to persondatu veidu, ko tā plāno kopīgot, kā arī iemeslus un nolūkus, kādiem [Y] plāno kopīgot persondatus. Ja [X] nesniedz rakstisku atļauju šādai kopīgošanai samērīgā termiņā, kas nepārsniedz desmit dienas, [Y] apspriežas ar [X] un izskata visus iebildumus, kas tai varētu būt. Ja [Y] nolemj kopīgot persondatus bez [X] rakstiskas atļaujas, [Y] paziņo [X] par savu nodomu kopīgot šos datus. Tad [X] var izlemt, vai apturēt persondatu nosūtīšanu.

Izņēmuma gadījumos [Y] var kopīgot persondatus ar trešo personu bez iepriekšējas rakstiskas atļaujas un atbilstošiem apliecinājumiem, ja tas nepieciešams uz [Y] attiecināmo juridisko pienākumu izpildei vai saistībā ar tiesvedību, ciktāl šī kopīgošana tiek veikta arī to svarīgo sabiedrības interešu apsvērumu dēļ, kas atzīti [Y trešā valstī] un [X dalībvalstī] vai Eiropas Savienībā, vai ja kopīgošana ir nepieciešama likumīgu prasību celšanai, īstenošanai vai aizstāvībai. Šādos gadījumos, ja [Y] ir kopīgojusi ar [trešām personām] jebkādus persondatus, uz kuriem attiecas šis instruments, [Y] periodiski informē [X] par kopīgoto persondatu raksturu un kopīgošanas iemeslu, ja šādas informācijas sniegšana neapdraud notiekošu izmeklēšanu. Šāds ierobežojums attiecībā uz informāciju, kas saistīta ar notiekošu izmeklēšanu, tiek piemērots tikai tik ilgi, kamēr pastāv ierobežojuma iemesls.

Un otrādi — [Y] var pieprasīt, lai [X] piemēro tos pašus noteikumus un garantijas attiecībā uz to datu tālāku kopīgošanu, kas saistībā ar šo instrumentu saņemti no [Y].

8. Persondatu tālāka nosūtīšana. [Y] nosūta no [X] saņemtos persondatus trešo valstu kompetentajām iestādēm tikai tiem pašiem nolūkiem, kādiem dati tai nosūtīti.

Gadījumā, ja [Y] plāno nosūtīt jebkādus persondatus trešai personai trešā valstī, [Y] pieprasa iepriekšēju rakstisku [X] atļauju un nosūta šādus persondatus tikai tad, ja persondatu aizsardzības līmenis netiek samazināts, piemēram, trešā persona apņemas ievērot tos pašus datu aizsardzības principus un garantijas, kas paredzēti šajā nolīgumā, vai tiek pieņemts attiecīgs lēmums par aizsardzības līmeņa pietiekamību[22]. Pieprasot šādu iepriekšēju rakstisku atļauju, [Y] norāda to persondatu veidu, ko tā plāno nosūtīt, kā arī iemeslus un nolūkus, kādiem [Y] plāno nosūtīt šos persondatus. Ja [X] nesniedz rakstisku atļauju šādai nosūtīšanai samērīgā termiņā, kas nepārsniedz desmit dienas, [Y] apspriežas ar [X] un izskata visus iebildumus, kas tai varētu būt. Un otrādi — [Y] var piemērot [X] to pašu procedūru attiecībā uz to datu tālāku nosūtīšanu, ko [X] saņēmusi no [Y] saistībā ar šo instrumentu.

9. Reāla tiesiskā aizsardzība. [Y] sniedz informāciju [X] par tās piemērojamajiem tiesību aktiem, kas nodrošina datu subjektiem tiesisko aizsardzību, un otrādi — [X] sniedz informāciju [Y] par tās piemērojamajiem tiesību aktiem, kas nodrošina datu subjektiem tiesisko aizsardzību. Minēto informāciju norāda šā instrumenta pielikumā. Ar jebkuru strīdu vai prasību, ko datu subjekts ceļ par tā persondatu apstrādi saskaņā ar šo instrumentu, var vērsties attiecīgi pie [X], [Y] vai abām iestādēm.

[20] Administratīvā vienošanās.
[21] Starptautiskā nolīgumā.
[22] "Attiecīgs lēmums par aizsardzības līmeņa pietiekamību" ir ES aizsardzības līmeņa pietiekamība, ar ko atzīst, ka tālāk nosūtāmajiem datiem ir aizsardzības līmenis, kurš ir praktiski līdzvērtīgs ES nodrošinātajam aizsardzības līmenim, ja tos apstrādā saņēmēji trešā valstī.

Katra kompetentā iestāde informē otru kompetento iestādi par jebkuru šādu strīdu vai prasību un dara visu iespējamo, lai strīdu vai prasību atrisinātu laikus un izlīguma veidā[23].

[Jebkuras sūdzības [X] izskata saskaņā ar VDAR un valsts tiesību aktiem. [Y] un [X] var iesniegt viens otrai sūdzību izskatīšanas mehānisma un tam piemērojamās procedūras detalizētu aprakstu.

Piemēram,

par jebkādām bažām vai sūdzībām par persondatu apstrādi, ko veic [Y], var ziņot tieši [Y iekšējai(-am) izpildes/atzinumu/sūdzību struktūrai/dienestam], jo īpaši izmantojot [speciālu kanālu sūdzībām], kur informāciju var sniegt, aizpildot tiešsaistes veidlapu tīmekļa vietnē, vai izmantojot elektronisko pastu, vēstuli, tālruni, vai arī var ziņot [X], nosūtot šādu informāciju tās sūdzību nodaļai, kā arī tās datu aizsardzības inspektoram. [Y] informē [X] par ziņojumiem, ko tā saņem no datu subjektiem par to persondatu apstrādi, kurus [Y] ir saņēmusi no [X], un apspriežas ar [X] par atbildi uz šo jautājumu. Un otrādi — [X] informē [Y] par sūdzībām, ko tā saņem no datu subjektiem par to persondatu apstrādi, kurus [X] ir saņēmusi no [Y], un apspriežas ar [Y] par atbildi uz šo jautājumu. [X] un [Y] samērīgi un laikus atbild uz datu subjektu pieprasījumiem.][24]

Datu subjektam ir tiesības saņemt tiesisko aizsardzību (tostarp iegūt piekļuvi persondatiem un veikt to labošanu vai dzēšanu, kā arī saņemt kompensāciju par zaudējumiem) saskaņā ar [šo instrumentu][25] / [VDAR un [X] valsts tiesību aktiem] un [valsts piemērojamajiem tiesību aktiem] attiecībā uz pieprasījumiem, kas vērsti pret [Y]][26], ja netiek ievērotas šajā instrumentā paredzētās garantijas. Situācijās, kad [X] uzskata, ka [Y] nav rīkojusies saskaņā ar šajā instrumentā paredzētajām garantijām, [X] atbilstīgi šim instrumentam var apturēt persondatu nosūtīšanu, līdz šis jautājums ir pienācīgi atrisināts, un informēt datu subjektu par to. Pirms nosūtīšanas apturēšanas [X] apspriež šo jautājumu ar [Y], un [Y] atbild bez liekas kavēšanās. Un otrādi — saskaņā ar šo instrumentu [Y] var apturēt datu nosūtīšanu, pamatojoties uz tiem pašiem iemesliem un tādā pašā veidā.

10. Pārraudzība. [X] un [Y] periodiski pārskata savas vadlīnijas un procedūras, ar ko īsteno instrumentā aprakstītās persondatu garantijas. Pēc otras kompetentās iestādes pamatota pieprasījuma kompetentā iestāde pārskata savas vadlīnijas un procedūras, lai pārliecinātos un apstiprinātu, ka šajā instrumentā paredzētās garantijas tiek reāli īstenotas, un nosūta pārskata kopsavilkumu otrai kompetentajai iestādei[27].

[23] Starptautiskā nolīgumā: starptautiskais nolīgums arī var papildināt [Y] piemērojamos tiesību aktus un/vai noteikumus, ja [Y] tiesiskajā regulējumā to trūkst vai tie nav pietiekami, lai sniegtu vajadzīgās garantijas un nodrošinātu atbilstīgu aizsardzības līmeni.

[24] Tas būs jāparedz administratīvā vienošanās. Starptautiskā nolīgumā paredz precīzākus noteikumus, lai nodrošinātu to, ka sūdzības par nolīguma pārkāpumiem izskata kompetentās iestādes, un to, kādā veidā tas notiek.

[25] Starptautiska nolīguma gadījumā.

[26] Administratīvas vienošanās gadījumā.

[27] Ņemot vērā prasību par kompetento iestāžu neatkarību, ja šī prasība tiktu izpildīta saskaņā ar Eiropas Savienības Tiesas un Eiropas Cilvēktiesību tiesas atgādinātajiem kritērijiem, ārēja pārraudzība varētu nebūt vajadzīga. Tomēr, ja trešās valsts kompetentajai iestādei nav ES prasīto neatkarības garantiju, iekļauj norādi, ka ir vajadzīga (ārēja) neatkarīga pārraudzība.

IV. SPĒKĀ STĀŠANĀS UN IZBEIGŠANA

Šis instruments stājas spēkā no parakstīšanas dienas [un paliek spēkā tikai tik ilgi, kamēr ir spēkā arī ISN][28]. Puses var apspriesties un pārskatīt šā instrumenta noteikumus [saskaņā ar tādiem pašiem nosacījumiem, kādi noteikti ISN][29].

Jebkura puse jebkurā laikā var izbeigt šā instrumenta darbību. Jo īpaši šā instrumenta darbību izbeidz, tiklīdz kāda no kompetentajām iestādēm vairs nevar nodrošināt šajā instrumentā paredzētās garantijas. Šī kompetentā iestāde par izbeigšanu informē arī otru kompetento iestādi. Tāpat šā instrumenta darbību izbeidz, tiklīdz kāda no kompetentajām iestādēm uzzina, ka otra kompetentā iestāde vairs nespēj nodrošināt šajā instrumentā paredzēto garantiju ievērošanu. Šī kompetentā iestāde par izbeigšanu informē arī otru kompetento iestādi. Pēc šā instrumenta darbības izbeigšanas kompetentās iestādes turpina ievērot konfidencialitāti [atbilstīgi ISN][30] attiecībā uz visu informāciju, kas sniegta saskaņā ar [šo instrumentu][31] [ISN][32]. Pēc šā instrumenta darbības izbeigšanas visus persondatus, kas iepriekš nosūtīti saskaņā ar šo instrumentu, [Y] turpina apstrādāt, ievērojot šajā instrumentā paredzētās garantijas.

V. CITI JAUTĀJUMI

Šo instrumentu, tostarp tā pielikumus, sagatavo […] un […], un abi/visi teksti ir vienlīdz autentiski.

*

* *

[28] Administratīvas vienošanās gadījumā.
[29] Administratīvas vienošanās gadījumā iekļauj šo norādi, savukārt starptautiskā nolīgumā tas ir jāprecizē šeit.
[30] Administratīvas vienošanās gadījumā. Starptautiska nolīguma gadījumā norādi uz pašu starptautisko nolīgumu sniedz šeit.
[31] Starptautiska nolīguma gadījumā.
[32] Administratīvas vienošanās gadījumā.

Ja nepieciešams paredzēt īpašu klauzulu par konfidencialitāti un dienesta noslēpumu atkarībā no saņēmējas iestādes valsts tiesiskā regulējuma analīzes:

III.a (jāiekļauj pirms IV. punkta). [Y] saņemtās informācijas konfidencialitāte un dienesta noslēpums

1) [Y] ievēro visas saskaņā ar šo instrumentu saņemtās informācijas konfidencialitāti:

(i) atbilstīgi šai vienošanās uzskatot visu saņemto informāciju vai palīdzības pieprasījumus — tostarp to, ka cita iestāde apsver izmeklēšanu izpildes nolūkos, ir sākusi to vai ir iesaistīta tajā — par konfidenciāliem un, ja nepieciešams, veicot papildu pasākumus, lai ievērotu nosūtītājas puses iekšējās juridiskās prasības;

(ii) nodrošinot, ka gadījumos, kad [Y] saņem pieteikumu no trešās personas (piemēram, fiziskas personas, tiesu iestādes vai citas tiesībaizsardzības iestādes) par tādas konfidenciālas informācijas izpaušanu, kas saskaņā ar šo vienošanos saņemta no [X], [Y] rīkojas šādi:
   a. saglabā visas šādas informācijas konfidencialitāti;
   b. nekavējoties paziņo [X], kas sniegusi konkrēto informāciju;
   c. iegūst [X] piekrišanu attiecīgās informācijas izpaušanai;
   d. informē [X], ja pastāv valsts tiesību akti, kas tomēr uzliek pienākumu izpaust informāciju;

(iii) pēc izstāšanās no šīs vienošanās, saglabājot visas tās konfidenciālās informācijas konfidencialitāti, ko atbilstīgi šai vienošanās ar to kopīgojusi [X], nosūtot atpakaļ un dzēšot šo informāciju;

(iv) nodrošinot, ka tiek veikti visi atbilstošie tehniskie un organizatoriskie pasākumi, lai visa informācija, kas tai sniegta saskaņā ar šo vienošanos, tiktu glabāta drošībā. Tas ietver informācijas nosūtīšanu atpakaļ vai apstrādi saskaņā ar [X] piekrišanu.

2) [X] var lūgt, lai saskaņā ar šo vienošanos sniegtā informācija tiktu izmantota vai izpausta tikai atbilstīgi īpašiem nosacījumiem, kurus precizē [X]. Ja [Y] plāno izmantot šo iespēju, tā informē [X] un, ja [X] piekrīt šiem nosacījumiem, ievēro tos. Pretējā gadījumā [X] var atteikties atbildēt uz pieprasījumu.

3) [Y] loceklis vai locekļi un personāls ievēro pienākumu glabāt dienesta noslēpumu vai pienākumu ievērot konfidencialitāti gan esot amatā, gan arī pēc pilnvaru termiņa beigām, attiecībā uz jebkādu konfidenciālu informāciju, ko tie ieguvuši, pildot savus amata pienākumus vai īstenojot pilnvaras. Viņu pilnvaru laikā minētais pienākums glabāt dienesta noslēpumu jo īpaši attiecas uz fizisku personu ziņojumiem par viņu valsts attiecīgā piemērojamā tiesiskā regulējuma pārkāpumiem.

*

* *

Instrumenta pielikumi

Pielikums. Apstrādes, nolūka, datu kategoriju, saņēmēju apraksts

Piemēram:

X: *[X identitāte un kontaktinformācija]*

1. Nosaukums: …

Adrese: …

Kontaktpersonas vārds, uzvārds, amats un kontaktinformācija: …

Paraksts un datums: …

Y: *[Y identitāte un kontaktinformācija]*

1. Nosaukums: …

Adrese: …

Kontaktpersonas vārds, uzvārds, amats un kontaktinformācija: …

Paraksts un datums: …

Nosūtīšanas apraksts:

To datu subjektu kategorijas, kuru persondati ir nosūtīti

……..

Nosūtīto persondatu kategorijas

……..

Nosūtītie sensitīvie dati (attiecīgā gadījumā) un piemērotie ierobežojumi vai garantijas, ar ko tiek pilnībā ņemts vērā datu raksturs un saistītie riski, piemēram, stingrs nolūka ierobežojums, piekļuves ierobežojumi (tostarp piekļuve tikai darbiniekiem, kuri pabeiguši specializētu apmācību), datu piekļuves uzskaite, ierobežojumi tālākai nosūtīšanai vai papildu drošības pasākumi

……..

Nosūtīšanas biežums (piemēram, vai dati tiek nosūtīti vienreiz vai pastāvīgi)

……..…

Apstrādes raksturs

……..…

Datu nosūtīšanas un tālākas apstrādes nolūks(-i)

……..

Laikposms, cik ilgi persondati tiks glabāti, vai, ja tas nav iespējams, kritēriji, ko izmanto minētā laikposma noteikšanai

……..

I pielikums. Piemērojamo tiesību aktu un attiecīgo tehnisko un organizatorisko drošības pasākumu apraksts

Tehniskie un organizatoriskie pasākumi jāapraksta konkrēti, nevis vispārīgi. Turklāt skaidri jānorāda, kuri pasākumi attiecas uz katru nosūtīšanu / vairākkārtēju nosūtīšanu.

Jāapraksta tehniskie un organizatoriskie pasākumi, ko X un Y īsteno, lai nodrošinātu pienācīgu drošības līmeni, ievērojot apstrādes raksturu, apmēru, kontekstu un nolūku, kā arī riskus fizisku personu tiesībām un brīvībām.

[Iespējamo pasākumu piemēri:

persondatu pseidonimizācijas un šifrēšanas pasākumi,

apstrādes sistēmu un pakalpojumu nepārtrauktas konfidencialitātes, integritātes, pieejamības un noturības nodrošināšanas pasākumi,

pasākumi, ar ko nodrošina spēju laicīgi atjaunot persondatu pieejamību un piekļuvi tiem gadījumā, ja ir noticis fizisks vai tehnisks negadījums,

procesi regulārai tehnisko un organizatorisko pasākumu efektivitātes testēšanai, novērtēšanai un izvērtēšanai nolūkā nodrošināt apstrādes drošību,

lietotāju identifikācijas un autorizācijas pasākumi,

datu aizsardzības pasākumi nosūtīšanas laikā,

datu aizsardzības pasākumi glabāšanas laikā,

pasākumi, ar ko nodrošina persondatu apstrādes vietu fizisko drošību,

pasākumi, ar ko nodrošina notikumu reģistrēšanu,

pasākumi, ar ko nodrošina sistēmu konfigurāciju, tostarp noklusējuma konfigurāciju,

iekšējo IT un IT drošības pārvaldības un vadības pasākumi,

procesu un produktu sertificēšanas/apliecināšanas pasākumi,

datu minimizēšanas nodrošināšanas pasākumi,

datu kvalitātes nodrošināšanas pasākumi,

pasākumi, ar ko nodrošina datu ierobežotu saglabāšanu,

pārskatatbildības nodrošināšanas pasākumi,

pasākumi datu pārnesamības atļaušanai un dzēšanas nodrošināšanai.]

II pielikums. To vienību saraksts, ar kurām [Y] ir atļauts tālāk kopīgot konfidenciālu informāciju

III pielikums. Tiesiskās aizsardzības tiesiskā regulējuma apraksts