EIROPAS
KOMISIJA

Briselē, 10.1.2017.
COM(2017) 7 final

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI

Apmaiņa ar personas datiem un šo datu aizsardzība globalizētā pasaulē

1. IEVADS

Personas datu aizsardzība ir daļa no Eiropas kopējās konstitucionālās sistēmas un ir nostiprināta ES Pamattiesību hartas 8. pantā. Tā ir bijusi ES tiesību aktu centrā jau vairāk nekā 20 gadus, sākot ar 1995. gada Datu aizsardzības direktīvu[1] ("1995. gada direktīva"), līdz pat Vispārīgās datu aizsardzības regulas (VDAR)[2] un Policijas direktīvas[3] pieņemšanai 2016. gadā.

Eiropas Komisijas priekšsēdētājs Žans Klods Junkers savā 2016. gada 14. septembra runā par stāvokli Eiropas Savienībā uzsvēra: *"[b]ūt Eiropietim nozīmē tiesības uz to, ka jūsu personas datus aizsargā spēcīgi Eiropas tiesību akti. [...] Jo Eiropā privātumam ir nozīme. Tas ir cilvēka cieņas jautājums.*"

Tomēr personas datu aizsardzības pieprasījums neaprobežojas tikai ar Eiropu. Patērētāji visā pasaulē arvien vairāk novērtē savu privātumu. Savukārt uzņēmumi atzīst, ka spēcīga privātuma aizsardzība tiem nodrošina konkurētspējas priekšrocības, jo pieaug uzticēšanās to pakalpojumiem. Daudzi uzņēmumi, it īpaši globāla mēroga uzņēmumi, saskaņo savu privātuma politiku ar VDAR, gan tāpēc, ka vēlas veikt uzņēmējdarbību Eiropas Savienībā, gan tāpēc, ka to uzskata par paraugu, kuru ievērot.

Tāpat vairākas valstis un reģionālās organizācijas ārpus ES, sākot no mūsu tuvākajām kaimiņvalstīm līdz pat Āzijai, Latīņamerikai un Āfrikai, pieņem jaunus vai atjaunina spēkā esošos datu aizsardzības tiesību aktus, lai izmantotu iespējas, ko sniedz globālā digitālā ekonomika, un lai reaģētu uz augošo pieprasījumu pēc spēcīgākas datu drošības un privātuma aizsardzības. Lai gan dažādām valstīm ir atšķirīga pieeja un likumdošanas attīstības līmenis, ir augšupejošas konverģences pazīmes attiecībā uz svarīgu datu aizsardzības principiem, it īpaši konkrētos pasaules reģionos[4]. Lielāka saderība starp dažādām datu aizsardzības sistēmām atvieglotu starptautisko personas datu plūsmu gan komerciāliem mērķiem, gan sadarbībai starp valstu iestādēm (piemēram, tiesībaizsardzības nolūkos). ES būtu jāizmanto šī iespēja, lai veicinātu tās datu aizsardzības vērtības un atvieglotu datu plūsmu, veicinot tiesību sistēmu konverģenci. Kā paziņots Komisijas darba programmā[5], šajā paziņojumā tāpēc ir izklāstīts Komisijas stratēģiskais satvars lēmumiem par aizsardzības līmeņa pietiekamību, kā arī citiem datu nosūtīšanas instrumentiem un starptautiskās datu aizsardzības instrumentiem.

---

1 Eiropas Parlamenta un Padomes Direktīva 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti, OV L 281, 23.11.1995.

2 Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula), OV L 119, 4.5.2016., 1.–88. lpp. Tā stājās spēkā 2016. gada 24. maijā, un to piemēro no 2018. gada 25. maija.

3 Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināLsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI (OV L 119, 4.5.2016., 89.–131. lpp.). Tā stājās spēkā 2016. gada 5. maijā. ES dalībvalstīm tā ir jātransponē savos tiesību aktos līdz 2018. gada 6. maijam.

4 Skatīt "Data protection regulations and international data flows: Implications for trade and development", *UNCTAD*, (2016): http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

5 Komisijas 2017. gada darba programma "Panākot tādu Eiropu, kas aizsargā, dod iespējas un aizstāv", COM(2016) 710 *final*, 25.10.2016, 12. lpp., un 1. pielikums.

2. ES DATU AIZSARDZĪBAS REFORMAS PAKETE — MŪSDIENĪGS TIESISKAIS REGULĒJUMS, KAS VEICINA LABI AIZSARGĀTAS STARPTAUTISKĀS DATU PLŪSMAS

2016. gada aprīlī pieņemtā ES datu aizsardzības tiesību aktu reforma izveido sistēmu, kas nodrošina gan spēcīgu aizsardzības līmeni, gan ir atvērta globālās informācijas sabiedrības iespējām. Nodrošinot privātpersonām lielāku kontroli pār saviem personas datiem, reforma stiprina patērētāju uzticēšanos digitālajai ekonomikai. Saskaņojot un vienkāršojot tiesisko vidi, tā atvieglo un mazāk apgrūtina uzņēmējdarbības veikšanu ES gan pašmāju, gan ārvalstu uzņēmumiem, arī starptautiski apmainoties ar datiem. Šobrīd ES apvieno starptautisku datu plūsmu atvērtību ar visaugstāko aizsardzības līmeni privātpersonām. Tai ir potenciāls kļūt par datu pakalpojumu centru, un priekšnoteikums tam ir gan brīvas datu plūsmas, gan uzticēšanās.

2.1. Visaptverošs, vienots un vienkāršots ES datu aizsardzības regulējums

Ar ES reformu tiek izveidots visaptverošs regulējums, kas regulē personas datu apstrādi gan privātajā un valsts sektorā, gan tirdzniecības un tiesībaizsardzības jomā (attiecīgi VDAR un Policijas direktīva).

Saskaņā ar VDAR no 2018. gada maija līdzšinējo 28 valstu likumu vietā būs viens vienots Eiropas mēroga noteikumu kopums. Jaunizveidotais vienas pieturas aģentūras mehānisms nodrošinās, ka viena datu aizsardzības iestāde būs atbildīga par ES uzņēmumu veikto pārrobežu datu apstrādes darbību uzraudzību. Tiks garantēta jauno noteikumu interpretācijas konsekvence. It īpaši pārrobežu gadījumos, kuros ir iesaistītas vairāku valstu datu aizsardzības iestādes, tiks pieņemts vienots lēmums, lai kopīgām problēmām nodrošinātu kopīgu risinājumu. Turklāt VDAR nodrošina vienlīdzīgus konkurences apstākļus ES un ārvalstu uzņēmumiem, kuros uzņēmumiem, kas atrodas ārpus ES, būs jāpiemēro tādi paši noteikumi kā Eiropas uzņēmumiem, ja tie piedāvā preces un pakalpojumus vai novēro indivīdu uzvedību ES. Lielāka patērētāju uzticēšanās sniegs labumu gan ES, gan ārējiem tirdzniecības aģentiem.

Policijas direktīvā ir paredzēti kopīgi noteikumi par kriminālprocesos iesaistītu indivīdu personas datu apstrādi, neatkarīgi no tā, vai tas ir aizdomās turamais, cietušais vai liecinieks, vienlaikus ņemot vērā policijas un krimināltiesību jomas īpašo raksturu. Saskaņojot datu aizsardzības noteikumus tiesībaizsardzības jomā, arī noteikumus par starptautisku nosūtīšanu, tiks veicināta pārrobežu sadarbība starp policiju un tiesu iestādēm gan ES iekšienē, gan ar starptautiskajiem partneriem, un tādējādi tiks izveidoti nosacījumi efektīvākai cīņai pret noziedzību. Tas ir nozīmīgs ieguldījums Eiropas Drošības programmā[6].

2.2. Atjaunots un dažādots instrumentu kopums starptautiskai nosūtīšanai

Kopš pašiem pirmsākumiem ES datu aizsardzības tiesību aktos ir paredzēti vairāki mehānismi starptautiskai datu nosūtīšanai. Šo noteikumu galvenais mērķis ir nodrošināt eiropiešu personas datu aizsardzību, kad tie tiek nosūtīti uz ārvalstīm. Gadu gaitā šie noteikumi ir noteikuši jaunus starptautisko datu plūsmu standartus daudzās jurisdikcijās. Lai gan struktūra būtībā paliek tāda pati kā saskaņā ar 1995. gada direktīvu, reformas noteikumi par

[6] Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu Komitejai, Eiropas Drošības programma, COM(2015) 185 *final,* 9.12.2015.

starptautisku nosūtīšanu precizē un vienkāršo to izmantošanu un ievieš jaunus nosūtīšanas instrumentus.

Saskaņā ar ES tiesību aktiem viens veids, kā nosūtīt personas datus uz ārzemēm, ir pamatojoties uz Komisijas "lēmumiem par aizsardzības līmeņa pietiekamību", kas paredz, ka valstis ārpus ES nodrošina "būtībā ekvivalentu"[7] datu aizsardzības līmeni tam, kāds ir Eiropas Savienībā. Šāda lēmuma mērķis ir nodrošināt brīvu personas datu plūsmu uz attiecīgo trešo valsti bez nepieciešamības datu eksportētājam veikt papildu aizsardzības pasākumus vai saņemt jebkādu atļauju. Precīzs un detalizēts elementu kopums, kas Komisijai ir jāņem vērā, novērtējot ārvalstu aizsardzības sistēmas atbilstību, ir pieejams ieinteresētajām valstīm vai starptautiskajām organizācijām[8]. Komisija tagad var pieņemt lēmumus par aizsardzības līmeņa pietiekamību arī attiecībā uz tiesībaizsardzības nozari[9]. Turklāt, pamatojoties uz praksi saskaņā ar 1995. gada direktīvu, reforma skaidri ļauj noteikt aizsardzības līmeņa pietiekamību attiecībā uz konkrētu trešās valsts teritoriju vai uz konkrētu sektoru vai nozari trešā valstī (tā dēvētā "daļējā" aizsardzības līmeņa pietiekamība)[10].

Ja nav lēmuma par aizsardzības līmeņa pietiekamību, starptautisku nosūtīšanu var veikt, pamatojoties uz vairākiem alternatīviem nosūtīšanas instrumentiem, kas nodrošina atbilstošas datu aizsardzības garantijas[11]. Reforma formalizē un paplašina iespējas izmantot spēkā esošos instrumentus, piemēram, līguma standartklauzulas[12] un saistošus uzņēmuma noteikumus[13]. Piemēram, līguma standartklauzulas tagad var iekļaut līgumā starp ES esošiem apstrādātājiem un apstrādātājiem ārpus ES (tā dēvētās "apstrādātājs apstrādātājam" modeļa klauzulas)[14]. Saistošos uzņēmuma noteikumus, kas līdz šim tika attiecināti tikai uz vienošanos starp vienas korporatīvās grupas struktūrām, tagad var izmantot uzņēmumu grupas, kas nodarbojas ar kopīgu saimniecisko darbību, bet ne vienmēr ir daļa no vienas un tās pašas korporatīvās

---

7 ES Tiesas 2015. gada 6. oktobra spriedums lietā C-362/14 *Maximillian Schrems pret datu aizsardzības komisāru,* 73., 74. un 96. punkts. Skatīt arī VDAR 104. apsvērumu un Policijas direktīvas 67. apsvērumu, kurā ir minēts līdzvērtīguma pēc būtības standarts.

8 Skatīt VDAR 45. pantu. Kā izklāstīts 45. panta 2. punktā, Komisijai savā novērtējumā ir jāņem vērā, *inter alia*, tiesiskums, cilvēktiesību un pamatbrīvību ievērošana, attiecīgie tiesību akti, gan vispārējie, gan nozaru, arī attiecībā uz sabiedrisko drošību, aizsardzību, valsts drošību un krimināltiesībām un publisko iestāžu piekļuvi personas datiem. To pamatā jābūt efektīvām un tiesiski īstenojamām tiesībām, ieskaitot personu aizsardzību administratīvā kārtā vai tiesām, un neatkarīgai uzraudzības iestādei, kas efektīvi darbojas, lai nodrošinātu un īstenotu datu aizsardzības noteikumu ievērošanu. Tiks ņemta vērā arī juridiski saistošu konvenciju, it īpaši Eiropas Padomes Konvencijas Nr. 108, ievērošana un dalība daudzpusējās vai reģionālās sistēmās, kas nodarbojas ar datu aizsardzību.

9 Skatīt Policijas direktīvas 36. panta 2. punktu par konkrētiem aizsardzības līmeņa pietiekamības izvērtēšanas faktoriem.

10 Skatīt VDAR 45. panta 1. punktu un Policijas direktīvas 36. panta 1. punktu,

11 Skatīt, piemēram, Komisijas paziņojumu Eiropas Parlamentam un Padomei par personas datu pārsūtīšanu no ES uz Amerikas Savienotajām Valstīm saskaņā ar Direktīvu 95/46/EK, izpildot Tiesas spriedumu lietā C-362/14 (*Schrems*), COM(2015) 566 *final*, 6.11.2015.

12 Līguma standartklauzulās ir noteikti attiecīgie datu aizsardzības pienākumi starp ES eksportētāju un trešās valsts importētāju.

13 Saistošie uzņēmuma noteikumi ir iekšējie noteikumi, kurus pieņēmušas daudznacionālu uzņēmumu grupas, lai veiktu datu nosūtīšanu uzņēmumu grupas iekšienē struktūrām, kas atrodas valstīs, kas nenodrošina pietiekamu aizsardzības līmeni. Kaut gan saistošie uzņēmuma noteikumi jau tiek izmantoti saskaņā ar 1995. gada direktīvu, VDAR kodificē un formalizē tos kā nosūtīšanas instrumentu.

14 Skatīt VDAR 46. panta 2. punkta c) un d) apakšpunktus un 168. apsvērumu.

grupas[15]. Reforma arī samazina birokrātiju, atceļot vispārējās prasības par iepriekšēju paziņošanu un atļaujas saņemšanu no datu aizsardzības iestādes datu nosūtīšanai uz trešo valsti, pamatojoties uz līguma standartklauzulām vai saistošajiem uzņēmuma noteikumiem[16]. Tas ir svarīgs ES starptautiskās datu nosūtīšanas sistēmas vienkāršojums, jo tādu prasību pastāvēšana, kas šobrīd atšķiras starp dalībvalstīm, bieži tiek uztverta kā nozīmīgs datu plūsmu šķērslis, it īpaši attiecībā uz mazajiem uzņēmumiem[17].

Turklāt reforma ievieš jaunus starptautiskas nosūtīšanas instrumentus[18]. Pārziņi un apstrādātāji saskaņā ar zināmiem nosacījumiem[19] varēs izmantot apstiprinātus rīcības kodeksus vai sertifikācijas mehānismus (piemēram, privātuma zīmogus vai zīmes), lai izveidotu "atbilstošasgarantijas". Tas ļautu izstrādāt vairāk starptautiskai nosūtīšanai pielāgotus risinājumus, atspoguļojot, piemēram, attiecīgā sektora vai nozares, vai konkrētas datu plūsmas īpašās iezīmes un vajadzības. Tas dotu arī iespēju nodrošināt atbilstošas garantijas attiecībā uz datu nosūtīšanu starp valsts iestādēm vai struktūrām, pamatojoties uz starptautiskiem nolīgumiem vai administratīvo kārtību[20]. Visbeidzot, VDAR precizē tā dēvēto "atkāpju"[21] izmantošanu (piemēram, piekrišana, līguma izpilde vai svarīgi iemesli sabiedrības interesēs), uz kurām īpašās situācijās struktūras var balstīt datu nosūtīšanu, ja nav lēmuma par aizsardzības līmeņa pietiekamību un neatkarīgi no kāda no iepriekš minēto instrumentu izmantošanas. It īpaši, VDAR ietver jaunu, kaut arī ierobežotu, atkāpi, kas attiecas uz nosūtīšanu, kas var notikt, lai ievērotu uzņēmuma leģitīmās intereses[22].

Visbeidzot, reforma pilnvaro Komisiju izstrādāt starptautiskās sadarbības mehānismus, lai veicinātu datu aizsardzības noteikumu izpildi, arī izmantojot savstarpējas palīdzības pasākumus[23]. Tādējādi tiek atzīts, ka ciešāka sadarbība starp uzraudzības iestādēm starptautiskā līmenī varētu nodrošināt gan individuālo tiesību efektīvāku aizsardzību, gan lielāku tiesisko noteiktību uzņēmumiem.

3. STARPTAUTISKA DATU NOSŪTĪŠANA TIRDZNIECĪBAS NOZARĒ — DARĪJUMU VEICINĀŠANA, AIZSARGĀJOT PRIVĀTUMU

Privātuma neaizskaramība ir priekšnoteikums stabilām, drošām un konkurētspējīgām tirdzniecības plūsmām visā pasaulē. Pivātums nav tirgojama prece[24]. Internets un preču un pakalpojumu digitalizācija ir pārveidojusi pasaules ekonomiku, un datu, arī personas datu, nosūtīšana pāri robežām ir dažādu lielumu un nozaru Eiropas uzņēmumu ikdienas darba daļa.

---

15 Skatīt VDAR 46. panta 2. punkta b) apakšpunktu un 110. apsvērumu.

16 Skatīt VDAR 46. panta 2. punktu.

17 Tas, ka reģistrācijas prasības rada tirdzniecības ierobežojumus daudziem uzņēmumiem, itīpaši MVU, tika uzsvērts, piemēram, *UNCTAD* ziņojuma 34. lpp.

18 Skatīt VDAR 46. panta 2. punkta e) un f) apakšpunktus.

19 Pārziņi ārpus ES varēs ievērot ES rīcības kodeksu vai sertifikācijas mehānismu, uzņemoties saistošasun īstenojamas saistības, izmantojot līgumiskas vai citas juridiskas saistības, lai piemērotu minētajos instrumentos ietvertos datu aizsardzības pasākumus. Skatīt VDAR 42. panta 2. punktu.

20 Skatīt VDAR 46. panta 2. punkta a) apakšpunktu un 46. panta 3. punkta b) apakšpunktu.

21 Skatīt VDAR 49. pantu.

22 Skatīt 49. panta 1. punkta otro daļu.

23 Skatīt VDAR 50. pantu.

24 Skatīt, piemēram, Komisijas paziņojumu Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai "Tirdzniecība visiem. Ceļā uz atbildīgāku tirdzniecības un ieguldījumu politiku", COM(2015) 497 *final*, 14.10.2015, 7. lpp.

Tā kā tirdzniecības apmaiņā arvien vairāk tiek izmantotas personas datu plūsmas, šādu datu privātums un drošība ir kļuvusi par patērētāju uzticēšanās galveno faktoru. Piemēram, divas trešdaļas eiropiešu apgalvo, ka ir satraukti par to, ka nespēj kontrolēt tiešsaistē sniegto informāciju, bet puse respondentu pauž bažas, ka varētu kļūt par krāpšanas upuriem[25]. Tajā pašā laikā Eiropas uzņēmumi, kas darbojas dažās trešās valstīs, arvien vairāk saskaras ar protekcionisma ierobežojumiem, kurus nevar pamatot ar leģitīmiem konfidencialitātes apsvērumiem.

Tādējādi digitālajā laikmetā augstu datu aizsardzības standartu veicināšanai un starptautiskās tirdzniecības veicināšanai jāiet roku rokā. Lai gan personas datu aizsardzība nav apspriežama[26] sarunās par tirdzniecības nolīgumiem, ES starptautisku datu nosūtīšanas režīms, kā minēts iepriekš, paredz plašu un daudzveidīgu instrumentu kopumu, lai nodrošinātu datu plūsmas dažādās situācijās, vienlaikus nodrošinot augstu aizsardzības līmeni.

3.1. Lēmumi par aizsardzības līmeņa pietiekamību

Pietiekamas aizsardzības atzinums nodrošina brīvu personas datu plūsmu no ES, neliekot ES datu nosūtītājam veikt papildu aizsardzības pasākumus vai ieviešot papildu nosacījumus. Konstatējot, ka tās tiesību sistēma nodrošina pietiekama līmeņa aizsardzību, ar šādu lēmumu atzīst, ka konkrētās valsts sistēma ir pielīdzināma ES dalībvalstu sistēmai. Tādējādi datu nosūtīšana uz attiecīgo valsti tiks pielīdzināta ES iekšējai datu nosūtīšanai, nodrošinot priviliģētu piekļuvi ES vienotajam tirgum un vienlaikus atverot tirdzniecības kanālus ES uzņēmējiem. Kā paskaidrots iepriekš, šis atzinums nosaka, ka ir nepieciešams aizsardzības līmenis, kas ir pielīdzināms (vai "būtībā ekvivalents")[27] ES garantētajam aizsardzības līmenim. Tas ietver visaptverošu trešās valsts sistēmas novērtējumu, ieskaitot tās noteikumu par piekļuvi personas datiem novērtējumu, ko veic valsts iestādes tiesībaizsardzības, valsts drošības un citu sabiedrības interešu nolūkos.

Tajā pašā laikā, kā Tiesa 2015. gadā apstiprinājusi *Schrems* nolēmumā, pietiekamas aizsardzības standarts neparedz ES noteikumu precīzu replicēšanu[28]. Drīzāk pārbaude atklāj, vai attiecīgās valsts tiesību sistēma spēj nodrošināt nepieciešamo augsta līmeņa aizsardzību, ņemot vērā tiesību uz privātumu būtību un to efektīvu īstenošanu, izpildāmību un uzraudzību. Līdz šim pieņemtie lēmumi par aizsardzības līmeņa pietiekamību liecina, ka Komisija var atzīt daudzveidīgas privātuma sistēmas, kas pārstāv dažādas juridiskās tradīcijas, par pietiekamām. Šie lēmumi attiecas uz valstīm, kas ir cieši saistītas ar Eiropas Savienību un tās dalībvalstīm (Šveice, Andora, Fēru salas, Gērnsija, Džērsija un Menas sala), nozīmīgiem tirdzniecības partneriem (Argentīna, Kanāda, Izraēla un ASV), un valstīm, kuras savā reģionā pirmās izstrādā datu aizsardzības likumus (Jaunzēlande, Urugvaja).

Lēmumi par Kanādu un ASV ir "daļēji" pietiekamas aizsardzības atzinumi. Lēmums par Kanādu attiecas tikai uz privātajām struktūrām, uz kurām attiecas Kanādas likums par

---

25 Eirobarometra īpašā aptauja Nr. 431, Datu aizsardzība, 2015. jūnijs.

26 Priekšsēdētāja Ž. K. Junkera politikas pamatnostādnes *"Jauns sākums Eiropai — mana programma nodarbinātībai, izaugsmei, taisnīgumam un demokrātiskām pārmaiņām"*.

27 Skatīt 7. zemsvītras piezīmi.

28 Sal. ar 74. punktu *Schrems* nolēmumā.

personas datu un elektronisko dokumentu aizsardzību. Nesen pieņemtais lēmums par ES un ASV privātuma vairogu[29] ir īpašs gadījums, jo, tā kā ASV nav vispārēju datu aizsardzības tiesību aktu,[30] tas balstās uz iesaistīto uzņēmumu saistībām piemērot augstas aizsardzības standartus, kas izklāstīti minētajā lēmumā, kas savukārt ir izpildāms saskaņā ar ASV tiesību aktiem. Turklāt privātuma vairogs pamatojas uz īpašām pārstāvniecībām un garantijām, ko sniegusi ASV valdība attiecībā uz piekļuvi valsts drošības nolūkos[31], kuras pamatā ir pietiekamas aizsardzības atzinums. Komisija rūpīgi uzraudzīs atbilstību šīm saistībām, un tā būs daļa no gada pārskata par regulējuma darbību.

Pēdējos gados arvien vairāk valstu visā pasaulē ir pieņēmušas jaunus tiesību aktus datu un privātuma aizsardzības jomā vai ir vēl to pieņemšanas procesā. 2015. gadā to valstu skaits, kas bija pieņēmušas datu konfidencialitātes likumus, bija 109, kas ir ievērojams pieaugums no 76, kā tas bija 2011. gada vidū[32]. Turklāt aptuveni 35 valstis šobrīd izstrādā datu aizsardzības likumus[33]. Šie jaunie vai modernizētie likumi parasti balstās uz galveno kopīgo principu kopumu, arī, *inter alia*, datu aizsardzības atzīšanu par vienu no pamattiesībām, visaptverošu tiesību aktu pieņemšanu šajā jomā, īstenojamu individuālo privātuma tiesību esamību un neatkarīgas uzraudzības iestādes izveidošanu. Tādējādi paveras jaunas iespējas, it īpaši izmantojot pietiekamas aizsardzības atzinumus, vēl vairāk atvieglot datu plūsmas, vienlaikus garantējot nepārtrauktu augsta līmeņa personas datu aizsardzību.

Saskaņā ar ES tiesību aktiem pietiekamas aizsardzības atzinuma priekšnoteikums ir, lai būtu datu aizsardzības noteikumi, kas ir salīdzināmi ar ES noteikumiem[34]. Tas attiecas gan uz būtisko aizsardzību, kas piemērojama personas datiem, gan uz attiecīgo uzraudzību un kompensācijas mehānismiem, kas pieejami trešā valstī.

Saskaņā ar regulējumu par pietiekamas aizsardzības atzinumiem Komisija uzskata, ka, novērtējot, ar kurām trešām valstīm būtu jāturpina dialogs par aizsardzības pietiekamību, ir jāņem vērā šādi kritēriji[35]:

i) ES (faktisko vai potenciālo) tirdzniecības attiecību apmērs ar konkrēto trešo valsti, arī tas, vai ir brīvās tirdzniecības nolīgums vai notiek sarunas;

---

29 Īstenošanas lēmums (ES) 2016/1260, 2016. gada 12. jūlijs.

30 Komisija mudina ASV turpināt centienus, lai panāktu visaptverošu privātuma un datu aizsardzības sistēmu, pieļaujot konverģenci starp abām sistēmām ilgtermiņā. Skatīt Komisijas paziņojumu Eiropas Parlamentam un Padomei "Transatlantiskās datu plūsmas — uzticēšanās atjaunošana, paredzot spēcīgākas drošības garantijas", COM(2016) 117 *final*, 29.2.2016.

31 Tās ietver Prezidenta politikas direktīvas Nr. 28 (*PPD-28*) piemērošanu, kas nosaka vairākus ierobežojumus un drošības garantijas "sakaru izlūkošanas" darbībām, un īpaša Ombuda biroja izveidi ES privātpersonu sūdzībām šajā sakarā.

32 *G. GREENLEAF*, "Global data privacy laws 2015: 109 countries, with European laws now in a minority", (2015) 133 *Privacy Laws & Business International Report*, 14.–17. lpp.

33 *UNCTAD* pētījums, 8. un 42. lpp. (skatīt 4. zemsvītras piezīmi).

34 Šajā sakarā, veicot aizsardzības pietiekamības novērtējumu, Komisija ņem vērā arī trešās valsts saistības, kas izriet no juridiski saistošām konvencijām, it īpaši tās pievienošanos Konvencijai Nr. 108 un tās papildu protokolam. Skatīt VDAR 45. panta 2. punkta c) apakšpunktu un 105. apsvērumu.

35 Attiecībā uz valstīm, ar kurām ir attiecīgas intereses sadarboties iekšējās drošības un tiesībaizsardzības jomā, Komisija pētīs konkrētu pietiekamas aizsardzības atzinumu iespēju saskaņā ar Policijas direktīvu, skatīt 4. sadaļu.

ii) personas datu plūsmu apmērs no ES, atspoguļojot ģeogrāfiskās un/vai kultūras saites;

iii) tas, ka trešā valsts ir pirmā valsts savā reģionā privātuma un datu aizsardzības tiesību aktu pieņemšanas jomā un varētu būt paraugs citām valstīm[36]; un

iv) vispārējās politiskās attiecības ar attiecīgo trešo valsti, it īpaši attiecībā uz kopīgu vērtību veicināšanu un kopīgiem mērķiem starptautiskā līmenī.

Pamatojoties uz šiem apsvērumiem, Komisija aktīvi sadarbosies ar galvenajiem tirdzniecības partneriem Austrumāzijā un Dienvidaustrumāzijā, sākot ar Japānu un Koreju 2017. gadā[37], un atkarībā no progresa datu aizsardzības likumu modernizēšanā — ar Indiju, bet arī ar valstīm Latīņamerikā, it īpaši *Mercosur*, un Eiropas kaimiņvalstīm, kuras arī ir izteikušas vēlmi iegūt "pietiekamas aizsardzības atzinumu". Turklāt Komisija atzinīgi vērtē citu trešo valstu pausto interesi, kas vēlas iesaistīties šajos jautājumos. Diskusijas par iespējamu pietiekamas aizsardzības atzinumu ir divpusējs dialogs, kas ietver visu nepieciešamos paskaidrojumu sniegšanu par ES datu aizsardzības noteikumiem un izpētot veidus, kā palielināt konverģenci ar trešo valstu tiesību aktiem un praksi.

Noteiktās situācijās, tā vietā, lai izmantotu valsts mēroga pieeju, lietderīgāk varētu būt izmantot citas iespējas, piemēram, daļēja vai nozarei specifiska pietiekamība (piemēram, finanšu pakalpojumiem vai IT nozarēs), kas skar ģeogrāfiskos apgabalus vai nozares, kas veido svarīgu konkrētās trešās valsts ekonomikas daļu. Tas jāapsver, ņemot vērā elementus, kā, piemēram, privātuma režīma attīstības raksturus un stāvoklis (autonoms likums, vairāki vai nozaru likumi u. c.), trešās valsts konstitucionālā struktūra vai, vai konkrētas ekonomikas nozares ir īpaši pakļautas datu plūsmām no ES.

Lēmuma par aizsardzības līmeņa pietiekamību pieņemšana ietver īpaša dialoga un ciešu sadarbības formu izveidošanu ar attiecīgo trešo valsti. Lēmumi par aizsardzības līmeņa pietiekamību ir "dzīvi" dokumenti, kurus Komisijai ir nepieciešams rūpīgi uzraudzīt un kuri jāpielāgo, ja parādās tendences, kas ietekmē aizsardzības līmeni, ko nodrošina attiecīgā trešā valsts[38]. Tāpēc tiks veiktas periodiskas pārbaudes vismaz reizi četros gados, lai risinātu aktuālus jautājumus un apmainītos ar labāko praksi starp tuviem partneriem[39]. Šī dinamiskā pieeja attiecas arī uz jau esošajiem lēmumiem par aizsardzības līmeņa pietiekamību, kuri pieņemti saskaņā ar 1995. gada direktīvu un kuri būs jāpārskata, ja tie vairs nebūs saskaņā ar piemērojamo standartu[40]. Tāpēc attiecīgās trešās valstis ir aicinātas informēt Komisiju par jebkurām būtiskām tiesību aktu un prakses izmaiņām, kas notikušas kopš attiecīgā lēmuma

---

36 Tas var būt īpaši nozīmīgi jaunattīstības un pārejas valstīm, jo personas datu aizsardzība ir gan būtisks tiesiskuma elements, gan svarīgs ekonomikas konkurētspējas faktors.

37 Japāna un Koreja nesen ir pieņēmušas vai modernizējušas savus tiesību aktus, lai ieviestu visaptverošu datu aizsardzības režīmu.

38 VDAR 45. panta 4. un 5. punkts nosaka, ka Komisija trešās valstīs un starptautiskajās organizācijās pastāvīgi uzrauga norises un piešķir tai tiesības atcelt, grozīt vai apturēt lēmumu par aizsardzības līmeņa pietiekamību, ja tā konstatē, ka attiecīgā valsts vairs nenodrošina pietiekamu aizsardzības līmeni.

39 VDAR 45. panta 3. punkts.

40 VDAR 97. panta 2. punkta a) apakšpunkts arī nosaka, ka Komisija līdz 2020. gadam iesniedz novērtējuma ziņojumu Eiropas Parlamentam un Padomei.

par aizsardzības līmeņa pietiekamību pieņemšanas. Ir būtiski nodrošināt nepārtrauktu šo lēmumu atbilstību jaunajiem reformas noteikumiem[41].

ES datu aizsardzības noteikumi nevar būt brīvas tirdzniecības nolīguma sarunu priekšmets[42]. Lai gan dialogos par datu aizsardzību un tirdzniecības sarunās ar trešām valstīm ir jāievēro atsevišķi virzieni, lēmums par aizsardzības līmeņa pietiekamību, arī daļēju vai nozarei specifisku aizsardzību, ir vislabākā iespēja veidot savstarpēju uzticēšanos, garantējot netraucētu personas datu plūsmu un tādējādi veicinot tirdzniecisko apmaiņu, kas ietver personas datu nosūtīšanu uz attiecīgo trešo valsti. Tādējādi šie lēmumi var atvieglot tirdzniecības sarunas vai var papildināt esošos tirdzniecības nolīgumus, ļaujot tiem paplašināt to priekšrocības. Tajā pašā laikā, veicinot aizsardzības līmeņa konverģenci ES un trešā valstī, pietiekamas aizsardzības atzinums samazina risku, ka šī valsts personas datu aizsardzības iemeslu dēļ piemēros nepamatotas datu lokalizācijas vai uzglabāšanas prasības. Turklāt, kā norādīts paziņojumā "Tirdzniecība visiem", Komisija centīsies izmantot ES tirdzniecības nolīgumus, lai izstrādātu noteikumus, kas attiektos uz e-komerciju un pārrobežu datu plūsmu un apkarotu jaunas digitālā protekcionisma formas, pilnībā ņemot vērā un neskarot ES datu aizsardzības noteikumus[43].

Komisija veiks šādus pasākumus:

- Noteiks par prioritāti diskusijas par iespējamiem lēmumiem par aizsardzības līmeņa pietiekamību ar galvenajiem tirdzniecības partneriem Austrumāzijā un Dienvidaustrumāzijā, sākot ar Japānu un Koreju 2017. gadā, bet apsverot arī citus stratēģiskos partnerus, piemēram, Indiju, un ar Latīņamerikas valstīm, itīpaši *Mercosur*, un Eiropas kaimiņvalstīm.

- Cieši uzraudzīs spēkā esošo lēmumu par aizsardzības līmeņa pietiekamību darbību. Tas it īpaši ietver ES un ASV privātuma vairoga regulējuma īstenošanu, it īpaši izmantojot ikgadēju kopīgā pārbaudes mehānismu.

- Palīdzēs un sadarbosies ar valstīm, kas ir ieinteresētas pieņemt stingrus datu aizsardzības likumus, un atbalstīs to konverģenci ar ES datu aizsardzības principiem.

3.2. Alternatīvi datu nosūtīšanas mehānismi

ES datu aizsardzības noteikumos vienmēr ir bijis atzīts, ka nav vienas pieejas, kas derētu visiem, attiecībā uz starptautisku datu nosūtīšanu. To vēl skaidrāk apliecina noteikumi, kas izriet no reformas. Lai gan pietiekamas aizsardzības atzinumi būs pieejami tikai tām trešām

[41] Ņemot vērā sekas no nolēmuma *Schrems* lietā, kurā konstatēts, ka Komisija ir pārsniegusi savas pilnvaras, "drošības zonas" (*"Safe Harbour"*) lēmumā ierobežojot datu aizsardzības iestāžu pilnvaras apturēt vai aizliegt datu plūsmas, 2016. gada 16. decembrī Komisija pieņēma "Omnibus" lēmumu, ar kuru groza lēmumu, kas svītro līdzīgus noteikumus pastāvošajos lēmumos par aizsardzības līmeņa pietiekamību un aizstāj tos ar noteikumiem, kas tikai paredz prasību sniegt informāciju starp dalībvalstīm un Komisiju gadījumā, ja datu aizsardzības iestādes aptur vai aizliedz nosūtīšanu uz kādu trešo valsti. "Omnibus" lēmums ievieš arī prasību Komisijai pārraudzīt attiecīgās norises trešā valstī. Skatīt OV L355, 17.12.2016, 83. lpp.

[42] Pietiekamas aizsardzības atzinums ir vienpusējs īstenošanas lēmums, ko pieņem Komisija saskaņā ar ES datu aizsardzības tiesību aktiem, pamatojoties uz tajos noteiktajiem kritērijiem.

[43] Skatīt paziņojumu par tirdzniecību visiem, 12. lpp., (24. zemsvītras piezīme).

valstīm, kas atbilst attiecīgajiem kritērijiem, VDAR nodrošina daudzveidīgu mehānismu kopumu, kas ir pietiekami elastīgi, lai pielāgotos dažādām nosūtīšanas situācijām. Instrumentus var izveidot tā, lai tiktu ņemtas vērā konkrēto nozaru, uzņēmējdarbības modeļu un/vai dalībnieku īpašās vajadzības vai nosacījumi. Piemēram, tās varētu būt līguma standartklauzulas, kas vērstas uz konkrētas nozares prasībām, piemēram, īpašas garantijas, apstrādājot konfidenciālus datus veselības nozarē, vai konkrēta veida apstrādes darbības, kas ir izplatītas dažās trešās valstīs, piemēram, ārpakalpojumu sniegšana Eiropas uzņēmumiem. To varētu izdarīt vai nu pieņemot jaunas standarta klauzulas, vai papildinot jau esošās ar papildu garantijām, kas varētu ietvert risinājumus gan ar tehniskajām un organizatoriskajām, gan ar uzņēmējdarbības modeli saistītajām situācijām[44]. Dažas specifiskas nozaru vajadzības var īstenot, izmantojot saistošus uzņēmuma noteikumus, kas attiecas uz uzņēmumu grupām, kas veic kopīgas saimnieciskās darbības, piemēram, tūrisma nozarē. Starptautiska nosūtīšana starp apstrādātājiem varētu tikt pilnveidota, izveidojot apstrādātājs apstrādātājam līguma standartklauzulas vai/un saistošus uzņēmuma noteikumus apstrādātājiem. Visbeidzot, jauni nosūtīšanas mehānismi, piemēram, apstiprināti rīcības kodeksi un akreditētas trešo personu sertifikācijas, nodrošinās nozari ar iespēju ieviest pielāgotus risinājumus starptautiskai nosūtīšanai, vienlaikus gūstot labumu no konkurences priekšrocībām, kas saistītas, piemēram, ar konfidencialitātes zīmogu vai preču zīmi. Dažus no šiem instrumentiem var attīstīt kā nosūtīšanai specifiskus mehānismus vai kā daļu no vispārējiem instrumentiem, lai pierādītu atbilstību visiem VDAR noteikumiem, piemēram, apstiprināta rīcības kodeksa gadījumā.

Komisija sadarbosies ar nozares, pilsoniskās sabiedrības un datu aizsardzības iestādēm, ar mērķi plašāk izmantot visu VDAR instrumentu kopumu potenciālu starptautiskai nosūtīšanai. Notiekošais dialogs ar ieinteresētajām personām saistībā ar reformas īstenošanu palīdzēs noteikt šajā ziņā prioritārās rīcības jomas. Tas var ietvert jau uzsāktā darba pabeigšanu, piemēram, darbu pie apstrādātājs apstrādātājam līguma standartklauzulu izstrādes, sadarbībā ar 29. panta darba grupu (ko 2018. gadā aizstās Eiropas Datu aizsardzības pārvalde)[45]. Tas var ietvert jaunu ES atbilstības infrastruktūras komponentu izstrādi, piemēram, ka Komisija definētu sertifikācijas mehānismus izveides un darbības prasības un tehniskos standartus, ieskaitot aspektus, kas attiecas uz starptautisku nosūtīšanu[46]. Dažas šīs darbības var papildināt ar darbu starptautiskā līmenī, it īpaši ar organizācijām, kas ir izstrādājušas līdzīgus nosūtīšanas mehānismus. Piemēram, varētu izpētīt veidus, kā veicināt konverģenci starp saistošiem uzņēmuma noteikumiem saskaņā ar ES tiesību aktiem un pārrobežu privātuma noteikumiem, kas izstrādāti Āzijas un Klusā okeāna ekonomiskās sadarbības forumā (*APEC*)[47] gan attiecībā uz piemērojamiem standartiem, gan uz pieteikšanās procesu katrā sistēmā. Tam būtu jāveicina augstas datu aizsardzības standarti visā pasaulē, vienlaikus

---

44 Skatīt VDAR 46. panta 2. punkta c) apakšpunktu un 109. apsvērumu, kas precizē, ka apstiprinātu modeļu klauzulu grozījumi ir iespējami, ja vien tie, tieši vai netieši, nav pretrunā ar šīm modeļa klauzulām vai ja tie nepārkāpj indivīda pamattiesības un pamatbrīvības.

45 Šobrīd spēkā nav neviena līguma standartklauzula par ES apstrādātāju nosūtītiem datiem ārpus ES esošiem apstrādātajiem.

46 VDAR 43. panta 8. un 9. punkts.

47 Skatīt 2014. gada APEC/ES dokumentu "Common Referential for the Structure of the EU Binding Corporate Rules and the APEC Cross Border Privacy Rules System (CBPR)", kurā salīdzinātas abu sistēmu atbilstības un sertifikācijas prasības: http://www.apec.org/~/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf.

mazinot atšķirības starp pieejām privātuma un datu aizsardzībai, palīdzot uzņēmējiem pārvietoties starp dažādām sistēmām un izstrādājot tiem atbilstošu politiku.

Komisija veiks šādus pasākumus:

- Strādās ar ieinteresētajām personām, lai izstrādātu alternatīvus personas datu nosūtīšanas mehānismus, kas pielāgoti konkrēto nozaru, uzņēmējdarbības modeļu un/vai operatoru īpašajām vajadzībām vai apstākļiem.

3.3. Starptautiskā sadarbība personas datu aizsardzības jomā

3.3.1. Datu aizsardzības standartu veicināšana, izmantojot daudzpusējus instrumentus un forumus

ES datu aizsardzības tiesiskais regulējums bieži vien kalpo kā atskaites punkts trešām valstīm, kas izstrādā tiesību aktus šajā jomā. ES turpinās aktīvi iesaistīties dialogā ar starptautiskajiem partneriem gan divpusējā, gan daudzpusējā līmenī, lai veicinātu konverģenci, izstrādājot augstus un sadarbspējīgus personas datu aizsardzības standartus visā pasaulē. Tas veicina efektīvāku personas tiesību aizsardzību un tajā pašā laikā samazina šķēršļus pārrobežu datu plūsmai, kas ir svarīgs brīvas tirdzniecības elements.

Komisija it īpaši aicina trešās valstis pievienoties Eiropas Padomes Konvencijai Nr. 108 un tās papildu protokolam[48]. Konvencija, kas ir atvērta arī tām valstīm, kas nav Eiropas Padomes dalībnieces, un kuru ir ratificējušas jau 50 valstis, arī Āfrikas un Dienvidamerikas valstis[49], ir vienīgais saistošais daudzpusējais instruments datu aizsardzības jomā. Šobrīd tā tiek pārskatīta, un Komisija aktīvi veicinās ātru modernizētā teksta pieņemšanu, lai ES kļūst par tās dalībnieci. Tā atspoguļos tos pašus principus, kādi ir nostiprināti jaunajos ES datu aizsardzības noteikumos, un tādējādi veicinās konverģenci starp augstu datu aizsardzības standartu kopumu.

2017. gada G20 samits nodrošinās papildu iespējas ES strādāt, lai ieviestu konverģenci attiecībā uz principu, ka augsti datu aizsardzības standarti ir būtiska turpmākās globālās informācijas sabiedrības attīstības sastāvdaļa, kas spēj veicināt inovācijas, izaugsmi un sociālo labklājību[50].

Komisija arī cer sadarboties ar svarīgiem jauniem dalībniekiem, piemēram, ANO īpašo referentu par tiesībām uz privātumu,[51] un turpināt attīstīt darba attiecības ar reģionālajām organizācijām, piemēram, *APEC*, lai veicinātu pasaules kultūru attiecībā uz tiesībām uz privātumu un personas datu aizsardzību.

---

[48] Eiropas Padomes 1981. gada 28. janvāra Konvencija par personas aizsardzību attiecībā uz personas datu automatizēto apstrādi (ETS Nr. 180) un 2001. gada Papildprotokols Konvencijai par personas aizsardzību attiecībā uz personas datu automatizēto apstrādi attiecībā uz uzraudzības iestādēm un pārrobežu datu plūsmām (ETS Nr. 181).

[49] Maurīcija, Senegāla un Urugvaja ir ratificējušas konvenciju. Turklāt Kaboverde, Maroka un Tunisija ir uzaicinātas pievienoties.

[50] Skatīt arī ESAO ministru deklarāciju "Digital Economy: Innovation, Growth and Social Prosperity" ("*Cancun* deklarācija"), 2016. gada 23. jūnijs.

[51] Skatīt: http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx.

Plašāku pasākumu ietvaros, lai uzlabotu informētību par privātumu un palielinātu starptautisko datu aizsardzību, Eiropas Komisija 2016. gada 15. novembrī apstiprināja projektu saskaņā ar partnerības instrumentu ar mērķi stiprināt sadarbību ar partnervalstīm šajā jomā[52]. Tas ietvers finansējumu darbībām, piemēram, apmācībām un izpratnes veicināšanai. Savukārt saistībā ar reformas īstenošanu ES var gūt labumu no labākās prakses apmaiņas un citu sistēmu pieredzes ar jauniem izaicinājumiem privātuma aizsardzības jomā un jauniem juridiskiem vai tehniskiem risinājumiem, arī attiecībā uz izpildi, atbilstības instrumentiem (piemēram, sertifikācijas mehānismi, privātuma ietekmes novērtējumi) vai dažu noteiktu datu kopu aizsardzību (piemēram, bērnu dati).

3.3.2. Sadarbība izpildes jomā

Arvien vairāk ir nepieciešams uzlabot sadarbību ar trešo valstu attiecīgajām privātuma izpildes un uzraudzības iestādēm, ņemot vērā starptautisko uzņēmumu globālo mērogu, kas apstrādā lielu daudzumu personas datu daudzās valstīs. Bieži vien datu aizsardzības noteikumu neatbilstības problēmas vai datu pārkāpumi vienlaikus ietekmē cilvēkus vairāk nekā vienā jurisdikcijā. Šādos gadījumos privātpersonu aizsardzību varētu padarīt efektīvāku, izmantojot kopīgu rīcību. Tajā pašā laikā uzņēmēji gūtu labumu no skaidrākas tiesiskās vides, kurā kopīgas interpretācijas instrumenti un īstenošanas prakses tiek attīstītas vispasaules līmenī.

Tāpēc ir pienācis laiks pastiprināt sadarbību starp īstenotājiem datu plūsmu bezrobežu un saistītajā pasaulē[53]. ES ir gatava dot savu ieguldījumu. Kā norādīts iepriekš, VDAR ļauj Komisijai izstrādāt starptautiskus sadarbības mehānismus, lai veicinātu datu aizsardzības tiesību aktu efektīvu izpildi, arī izmantojot savstarpējas palīdzības pasākumus. Šajā kontekstā, būtu jāizpēta iespēja izstrādāt pamatnolīgumu par sadarbību starp ES datu aizsardzības iestādēm un izpildiestādēm dažās trešās valstīs, ņemot vērā arī pieredzi, ko guvusi Komisija citās izpildes jomās, piemēram, konkurences un patērētāju aizsardzības jomā.

---

[52] Komisijas Īstenošanas lēmums C(2016)7198, ar ko apstiprina partnerības instrumenta 2016. gada ikgadējās rīcības programmas (*AAP 2016*) otro posmu.

[53] Esošie tīkli ietver Globālo privātuma aizsardzības tīklu (*GPEN*), kas ieviests 2010. gadā un uzsākts 2010. gadā ESAO aizbildniecībā. Tas ir neformāls privātuma tiesībaizsardzības iestāžu tīkls, kurā ir iesaistījušās ES datu aizsardzības iestādes, kurām ir pienākums, cita starpā, sadarboties ar tiesībaizsardzības iestādēm, dalīties labākās prakses pieredzē, risinot pārrobežu problēmas un atbalstot kopīgas īstenošanas iniciatīvas un izpratnes veidošanas kampaņas. Tas nerada dalībniekiem nekādus jaunus juridiski saistošus pienākumus un galvenokārt ir paredzēts, lai atvieglotu sadarbību privātuma tiesību aktu izpildē, kas reglamentē privāto sektoru. Skatīt https://privacyenforcement.net/.

Komisija veiks šādus pasākumus:

- Veicinās ātru Eiropas Padomes Konvencijas Nr. 108 modernizētā teksta pieņemšanu ar mērķi, lai ES kļūtu par tās dalībnieci un veicinātu trešo valstu pievienošanos.

- Izmantos daudzpusējus forumus, piemēram, Apvienoto Nāciju Organizāciju, G20 un *APEC*, lai veicinātu globālu datu aizsardzības tiesību ievērošanas kultūru.

- Izstrādās starptautiskās sadarbības mehānismus ar galvenajiem starptautiskajiem partneriem, lai veicinātu efektīvu izpildi.

4. EFEKTĪVĀKA SADARBĪBA TIESĪBAIZSARDZĪBAS JOMĀ AR STINGRIEM DATU AIZSARDZĪBAS PASĀKUMIEM

Personas datu apmaiņa ir neatņemama noziedzīgu nodarījumu novēršanas, izmeklēšanas un saukšanas pie kriminālatbildības daļa. Savstarpēji saistītā pasaulē, kur noziegums reti apstājas pie valstu robežām, ātra personas datu apmaiņa ir būtiska veiksmīgai sadarbībai tiesībaizsardzības jomā un efektīvai rīcībai pret noziedzību. Šādas apmaiņas pamatā ir jābūt stingriem datu aizsardzības pasākumiem. Tas arī veicina uzticības veidošanos starp tiesībaizsardzības iestādēm un stiprina juridisko noteiktību, ja tiek vākta un/vai notiek apmaiņa ar informāciju.

Noteikumi par starptautisku nosūtīšanu Policijas direktīvā reglamentē datu apmaiņu starp tiesībaizsardzības iestādēm ES un ārpus ES, kā arī, īpašās situācijās, nosūtot informāciju no tiesībaizsardzības iestādēm citām struktūrām. Direktīva ievieš iespēju veikt pietiekamas aizsardzības atzinumus krimināllikumu tiesībaizsardzības sektorā. Komisija veicinās šādu pietiekamas aizsardzības atzinumu iespēju ar atbilstošām trešām valstīm, it īpaši ar tām valstīm, ar kurām ir nepieciešama cieša un ātra sadarbība cīņā pret noziedzību un terorismu un ar kurām jau notiek būtiska personas datu apmaiņa. Pamatojoties uz to, Komisija par prioritāti noteiks sarunas par lēmumiem par aizsardzības līmeņa pietiekamību ar trešām valstīm, kuras ir galvenie partneri šajos pasākumos.

2016. gada decembrī noslēgtais ES un ASV datu aizsardzības jumta nolīgums[54] ir veiksmīgs piemērs tam, kā tiesībaizsardzības iestāžu sadarbību ar svarīgu starptautisku partneri var uzlabot, risinot sarunas par spēcīgu datu aizsardzības pasākumu kopumu. Automātiski papildinot esošos juridiskos instrumentus, kas ir datu apmaiņas pamatā (īpaši divpusējos nolīgumus gan ES, gan dalībvalstu līmenī), jumta nolīgums rada tūlītējus un tiešus ieguvumus indivīdiem un stiprina sadarbību tiesībaizsardzības jomā, veicinot informācijas apmaiņu. Arī izveidojot pamatu nākotnes datu nosūtīšanas nolīgumiem ar ASV, jumta nolīgums ļaus novērst nepieciešamību atkārtoti pārrunāt šos pašus aizsardzības pasākumus. Jumta nolīgums

[54] ES un ASV nolīgums par tādu personas datu aizsardzību, kas policijas un tiesu iestāžu sadarbības krimināllietās ietvaros tiek pārsūtīti un apstrādāti nolūkā novērst, izmeklēt un atklāt noziedzīgos nodarījumus, tostarp terorismu, vai saukt pie kriminālatbildības par tiem: http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf ("jumta nolīgums")

ir pirmais divpusējais starptautiskais nolīgums ar visaptverošu datu aizsardzības tiesību un pienākumu kopumu saskaņā ar ES *acquis*. Tāpēc tas var kalpot par pamatu sarunās par līdzīgiem nolīgumiem ar trešām valstīm ne vien attiecībā uz tiesu iestāžu un policijas sadarbību, bet arī citās publiskās izpildes jomās (piemēram, konkurences politika, patērētāju aizsardzība). Tas attieksies gan uz savstarpēju apmaiņu starp valdībām, gan datu nosūtīšanu starp privātiem uzņēmumiem un tiesībaizsardzības iestādēm. Tas varētu arī atvieglot Savienībai tādu nolīgumu noslēgšanu, kuri attiecas uz datu apmaiņu starp attiecīgajām ES aģentūrām (it īpaši Eiropolu un *Eurojust*) un trešām valstīm[55]. Tādējādi Komisija pētīs iespēju noslēgt līdzīgus pamatnolīgumus ar tai svarīgākajiem tiesībaizsardzības partneriem.

Turklāt Policija direktīva paredz iespēju, ievērojot stingrus aizsardzības pasākumus un īpašos apstākļos, ES tiesībaizsardzības iestādēm pieprasīt informāciju tieši no privāta uzņēmuma trešā valstī un nodot pieprasīto informāciju par personu (parasti vārdu vai IP adresi)[56]. Turpretī VDAR ir īpaši risinātas situācijas, kad ES privātie uzņēmumi pēc pieprasījuma nosūta tiesībaizsardzības iestādēm e-pierādījumus, kas satur personas datus. Šāda nosūtīšana ārpus ES ir pieļaujama tikai saskaņā ar konkrētiem nosacījumiem, piemēram, pamatojoties uz starptautisku nolīgumu vai, ja izpaušanai ir svarīgs sabiedrības interešu iemesls, kas ir atzīts Savienības vai dalībvalstu tiesību aktos[57].

Šī sadarbība, kas ir kļuvusi īpaši svarīga veiksmīgai noziedzības un terorisma izmeklēšanai un saukšanai pie krimināltiesībās, ir uzsvērta Padomes secinājumos par to, kā uzlabot krimināltiesības kibertelpā. Padome aicināja Komisiju veikt konkrētus pasākumus, pamatojoties uz kopīgu ES pieeju, lai uzlabotu sadarbību ar pakalpojumu sniedzējiem, padarītu savstarpējo tiesisko palīdzību vēl efektīvāku un piedāvātu risinājumus problēmām, nosakot un īstenojot jurisdikciju kibertelpā[58]. Šie pasākumi attiecas gan uz savstarpēju apmaiņu starp tiesībaizsardzības iestādēm pakalpojumu sniedzējiem, kas atrodas ES, gan uz apmaiņu ar trešo valstu iestādēm un uzņēmumiem. Komisija 2017. gada jūnijā izklāstīs iespējas attiecībā uz piekļuvi elektroniskiem pierādījumiem, ņemot vērā nepieciešamību nodrošināt ātru un uzticamu sadarbību, kas balstīta uz Policijas direktīvā un VDAR noteiktajiem stingrajiem datu aizsardzības standartiem gan ES iekšējās situācijās, gan starptautiskai nosūtīšanai.

Visbeidzot, saskaņā ar jauno juridisko pamatu Eiropolam Komisija izvērtēs noteikumus, kas ietverti šajos sadarbības nolīgumos starp Eiropolu un trešām personām, kas noslēgti saskaņā ar Padomes Lēmumu 2009/371/TI, arī to datu aizsardzības noteikumus[59]. Turklāt, kā noteikts

---

55 Operatīvās sadarbības nolīgumiem ar Eiropolu un *Eurojust* arī ir bijusi liela nozīme vīzu režīma liberalizācijas dialogos ar dažām trešām valstīm, arī, piemēram, saistībā ar notiekošo dialogu ar Turciju.

56 Skatīt Policijas direktīvas 39. pantu un 73. apsvērumu.

57 Skatīt VDAR 48. pantu un 115. apsvērumu.

58 Eiropas Savienības Padomes secinājumi par krimināltiesību uzlabošanu kibertelpā, 2016. gada 9. jūnijs. www.consilium.europa.eu/en/meetings/jha/2016/06/cyberspace--en_pdf/. Komisijai ir uzdots līdz 2017. gada jūnijam iesniegt Padomei rezultātus par šiem jautājumiem pēc tās progresa ziņojuma Padomei, kas iesniegts 2016. gada decembrī.

59 Skatīt 25. panta 4. punktu Eiropas Parlamenta un Padomes Regulā (ES) 2016/794 (2016. gada 11. maijs) par Eiropas Savienības Aģentūru tiesībaizsardzības sadarbībai (Eiropolu) un ar kuru aizstāj un atceļ Padomes Lēmumus 2009/371/TI, 2009/934/TI, 2009/935/TI, 2009/936/TI un 2009/968/TI, OV L 135, 24.5.2016,

2015. gada Eiropas Drošības programmā, Savienības nākotnes pieejā attiecībā uz PDR datu apmaiņu ar trešām valstīm tiks ņemta vērā vajadzība piemērot vienotus standartus un īpašus pamattiesību aizsardzības pasākumus. Komisija turpinās izstrādāt tiesiski pamatotus un ilgtspējīgus risinājumus pasažieru datu reģistra (PDR) datu apmaiņai ar trešām valstīm, apsverot arī iespēju noslēgt parauglīgumu par PDR, kurā būtu izklāstītas prasības, kas trešām valstīm jāizpilda, lai tās varētu saņemt PDR datus no ES. Tomēr jebkāda turpmākā politika šajā jomā būs atkarīga it īpaši no gaidāmā Eiropas Savienības Tiesas atzinuma par iecerēto ES un Kanādas PDR nolīgumu[60].

EFEKTĪVĀKA SADARBĪBA TIESĪBAIZSARDZĪBAS JOMĀ AR STINGRIEM DATU AIZSARDZĪBAS PASĀKUMIEM

Komisija veiks šādus pasākumus:

- Veicinās lēmumu par aizsardzības līmeņa pietiekamību iespēju saskaņā ar Policijas direktīvu ar attiecīgām trešām valstīm.
- Veicinās sarunas par nolīgumiem tiesībaizsardzības jomā ar svarīgiem starptautiskiem partneriem pēc jumta nolīguma ar ASV parauga.
- Ievēros Padomes secinājumus par krimināltiesību uzlabošanu kibertelpā, lai atvieglotu e-pierādījumu pārrobežu apmaiņu, kas ir saskaņā ar datu aizsardzības noteikumiem.

5. SECINĀJUMI

Aizsardzība un personas datu apmaiņa savstarpēji viena otru neizslēdz. Spēcīga datu aizsardzības sistēma atvieglo datu plūsmas, veidojot patērētāju uzticību tiem uzņēmumiem, kas rūpējas par to, kā viņi rīkojas ar savu klientu personas datiem. Tādējādi augsti datu aizsardzības standarti kļūt par priekšrocību pasaules digitālajā ekonomikā. Tas pats sakāms par tiesībaizsardzības iestāžu sadarbību: privātuma aizsardzības pasākumi ir neatņemama efektīvas un ātras informācijas apmaiņas sastāvdaļa cīņā pret noziedzību, balstoties uz savstarpēju uzticēšanos un juridisko noteiktību.

Pabeidzot tās datu aizsardzības noteikumu reformu, ES aktīvi jāsadarbojas ar trešām valstīm šajā jautājumā. Tai jācenšas panākt lielāku datu aizsardzības principu augšupvērstu konverģenci starptautiski, gan divpusējā, gan daudzpusējā līmenī. Tas nāk par labu gan iedzīvotājiem, gan uzņēmumiem un ir to interesēs. Jaunais datu aizsardzības tiesiskais regulējums nodrošina ES nepieciešamos un piemērotus instrumentus, lai sasniegtu šos mērķus. Pamatojoties uz šajā paziņojumā sniegto stratēģisko pieeju, Komisija aktīvi

(53.-114. lpp.). Komisijai ir pienākums līdz 2021. gada 14. jūnijam iesniegt novērtējuma ziņojumu par Eiropola sadarbības nolīgumiem, kas noslēgti līdz 2017. gada 1. maijam.

[60] Tiesas atzinums par 2014. gada ES un Kanādas PDR nolīguma projektu, kuru izskatīšanai Tiesā iesniedzis Eiropas Parlaments (atzinums 1/15). Tiesai tika lūgts novērtēt nolīguma projekta saderību ar ES Pamattiesību hartu.

sadarbosies ar galvenajām trešām valstīm, lai izpētītu iespēju pieņemt pietiekamas aizsardzības atzinumus, sākot ar Japānu un Koreju 2017. gadā, ar mērķi veicināt regulatīvo konverģenci virzībā uz ES standartiem un veicināt tirdzniecības attiecības. Tajā pašā laikā ES pilnībā izmantos alternatīvo nosūtīšanas instrumentu klāstu, lai aizsargātu datu aizsardzības tiesības un atbalstītu uzņēmējus, kad dati tiek nosūtīti uz valstīm, kuru valsts tiesību akti nenodrošina pietiekamu datu aizsardzības līmeni. Šādi instrumenti būtu arī jāizmanto, lai vēl vairāk veicinātu sadarbību starp ES uzraudzības un tiesībaizsardzības iestādēm un to starptautiskajiem partneriem. Komisija nodrošinās ES datu aizsardzības politikas iekšējās un ārējās dimensijas saskaņotību un veicinās stingru datu aizsardzību starptautiskā līmenī, lai uzlabotu sadarbību tiesībaizsardzības jomā, sekmētu brīvu tirdzniecību un attīstītu augstus personas datu aizsardzības standartus visā pasaulē.