EIROPAS
KOMISIJA

Briselē, 24.6.2020.
COM(2020) 264 final

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI

Datu aizsardzība kā iedzīvotāju tiesību nodrošināšanas un ES digitālās pārkārtošanās pīlārs – Vispārīgās datu aizsardzības regulas piemērošanas divi gadi

{SWD(2020) 115 final}

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI

Datu aizsardzība kā iedzīvotāju tiesību nodrošināšanas un ES digitālās pārkārtošanās pīlārs – Vispārīgās datu aizsardzības regulas piemērošanas divi gadi

1 DATU AIZSARDZĪBAS NOTEIKUMI KĀ IEDZĪVOTĀJU TIESĪBU NODROŠINĀŠANAS UN ES DIGITĀLĀS PĀRKĀRTOŠANĀS PĪLĀRS

Šis ir pirmais Vispārējās datu aizsardzības regulas[1] (turpmāk – "VDAR") novērtējuma un pārskata ziņojums, kas izstrādāts saskaņā ar VDAR 97. pantu jo īpaši attiecībā uz noteikumu par personas datu nosūtīšanu trešām valstīm un starptautiskām organizācijām un noteikumu par sadarbību un konsekvenci piemērošanu un darbību.

VDAR, kas tiek piemērota kopš 2018. gada 25. maija, ir ES regulējuma centrā,[2] garantē pamattiesības uz datu aizsardzību, kā noteikts Eiropas Savienības Pamattiesību hartā (8. pants) un Līgumos (Līguma par Eiropas Savienības darbību ("LESD") 16. pants). VDAR stiprina datu aizsardzības pasākumus, nodrošina personām papildu un stingrākas tiesības, lielāku pārredzamību un nodrošina, ka visi, kas apstrādā personas datus tās piemērošanas ietvaros, ir atbildīgāki. Tā piešķir spēcīgākas un saskaņotākas izpildes pilnvaras neatkarīgajām datu aizsardzības iestādēm un izveido jaunu pārvaldības sistēmu. Tā arī rada līdzvērtīgus konkurences apstākļus visām uzņēmējsabiedrībām, kas darbojas ES tirgū, neatkarīgi no tā, kur tās ir reģistrētas, un nodrošina brīvu datu plūsmu ES, tādējādi stiprinot iekšējo tirgu.

VDAR ir svarīga uz cilvēku orientētas pieejas tehnoloģijām sastāvdaļa, kā arī kompass tehnoloģiju izmantošanai, īstenojot gan zaļo, gan digitālo pārkārtošanos, un raksturo ES politikas veidošanu. Tas nesen tika uzsvērts Baltajā grāmatā par mākslīgo intelektu[3] un 2020. gada februāra paziņojumā par Eiropas Datu stratēģiju[4] (turpmāk – "Datu stratēģija").

Ekonomikā, kas arvien vairāk balstās uz datu, tostarp personas datu, apstrādi, VDAR ir būtisks līdzeklis, lai nodrošinātu, ka personām ir labāka kontrole pār viņu personas datiem un ka šie dati tiek apstrādi leģitīmā nolūkā, likumīgā, godīgā un pārredzamā veidā. Vienlaikus VDAR palīdz veicināt uzticamas inovācijas, īpaši izmantojot tajā minēto uz risku balstīto pieeju un tādus principus kā integrēta privātuma aizsardzība un privātuma aizsardzība pēc noklusējuma. Komisija ir ierosinājusi papildināt datu

[1] 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 (OV L 119, 4.5.2016., 1.–88. lpp.).

[2] Pēc tās iekļaušanas Līgumā par Eiropas Ekonomikas zonu (EEZ) regulu piemēro arī Norvēģijai, Islandei un Lihtenšteinai.

[3] https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

[4] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy

aizsardzības un privātuma tiesisko regulējumu[5] ar E-privātuma regulu[6], ar kuru paredzēts aizstāt pašreizējo E-privātuma direktīvu[7]. Šo priekšlikumu pašlaik izskata likumdevēji, un ir ļoti svarīgi nodrošināt tā ātru pieņemšanu.

Jaunas iniciatīvas var tikt attīstītas kā Komisijas galveno prioritāšu "Eiropa, kas sagatavota digitālajam laikmetam"[8] un "Eiropas zaļais kurss"[9] daļa, lai iedzīvotājiem dotu iespēju aktīvāk iesaistīties digitālās pārkārtošanās īstenošanā un digitālo rīku izmantošanā ar mērķi panākt klimatneitrālu sabiedrību un ilgtspējīgāku attīstību. VDAR nosaka regulējumu šīm iniciatīvām un nodrošina, ka tās tiek izstrādātas, lai efektīvi palielinātu personu tiesības.

Datu stratēģija[10] aicina izveidot "vienotu Eiropas datu telpu", patiesu vienoto datu tirgu, kā arī desmit nozaru kopējās Eiropas datu telpas, kuras ir būtiskas gan zaļajai, gan digitālajai pārkārtošanai[11]. Attiecībā uz visām šīm prioritātēm svarīgs ir skaidrs un praktiski īstenojams satvars drošai datu apmaiņai un labākai datu pieejamībai. Datu stratēģijā arī paziņots par Komisijas nodomu turpmākajos tiesību aktos izpētīt, kā nodrošināt publiskajās datu bāzēs glabāto datu izmantošanu zinātniskās pētniecības vajadzībām atbilstoši VDAR. Eiropas mākoņa federācijai ir jāatbalsta datu telpas, nodrošinot datu apstrādes un mākoņa infrastruktūras pakalpojumus, kas atbilst VDAR. VDAR nodrošina augstu personas datu aizsardzības līmeni un personu centrālo lomu visās minētajās datu telpās, vienlaikus nodrošinot nepieciešamo elastību, lai pielāgotos dažādām pieejām.

Nepieciešamība nodrošināt uzticēšanos un pieprasījums pēc personas datu aizsardzības sniedzas ārpus ES robežām. Cilvēki visā pasaulē arvien lielāku vērtību piešķir savu datu privātumam un drošībai. Kā tas tika parādīts nesen veiktā pasaules mēroga pētījumā[12], cilvēki to uzskata par svarīgu faktoru, kas ietekmē viņu pirkšanas lēmumus un viņu uzvedību tiešsaistē. Arvien vairāk uzņēmējsabiedrību ir atbildējušas uz šo privātuma prasību, it īpaši brīvprātīgi piemērojot dažas no VDAR paredzētajām tiesībām un aizsardzības pasākumiem arī saviem klientiem ārpus ES. Daudzi uzņēmumi veicina arī personas datu aizsardzību kā konkurētspējas un pārdošanas

---

[5] Šajā tiesiskajā regulējumā ietilpst arī Direktīva par datu aizsardzību tiesībaizsardzības jomā (Direktīva 2016/680) un Regula par datu aizsardzību ES iestādēs un struktūrās (Regula 2018/1725).

[6] Priekšlikums Eiropas Parlamenta un Padomes regulai par privātās dzīves neaizskaramību un personas datu aizsardzību elektronisko sakaru jomā un ar ko atceļ Direktīvu 2002/58/EK (Privātuma un elektronisko sakaru regula), COM/2017/010 final, 2017/03 (COD).

[7] Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (Direktīva par privāto dzīvi un elektronisko komunikāciju) (OV L 201, 31.07.2002., 0037. - 0047. lpp.).

[8] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_lv

[9] Komisijas paziņojums Eiropas Parlamentam, Eiropadomei, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai "Eiropas zaļais kurss", COM/2019/640 final.

[10] Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai "Eiropas Datu stratēģija", COM/2020/66 final.

[11] Šīs desmit nozaru kopējās Eiropas datu telpas ietver šādas jomas: veselību, rūpniecisko ražošanu, enerģētiku, mobilitāti, lauksaimniecību, finanšu datus, valsts pārvaldi, vienoto Eiropas datu prasmju datu telpu, Eiropas zaļā kursa datu telpu un Eiropas atvērtās zinātnes mākoni.

[12] Skatīt, piemēram, 2019. gadā *Cisco* veikto pētījumu par patērētāju privātumu (https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf). Saskaņā ar šo pētījumu, kurā tika aptaujāti 2600 patērētāji visā pasaulē, ievērojams skaits patērētāju jau ir veikuši pasākumus, lai aizsargātu savu privātumu, piemēram, mainot uzņēmējsabiedrības vai pakalpojumu sniedzējus to datu politikas vai datu apmaiņas prakses dēļ.

argumentu pasaules tirgū, piedāvājot inovatīvas preces un pakalpojumus ar jauniem privātuma vai datu drošības risinājumiem. Turklāt privātā un publiskā sektora dalībnieku paplašinātās iespējas vākt un apstrādāt datus lielā mērogā rada būtiskus un sarežģītus jautājumus, kas arvien vairāk izvirza privātumu publisko debašu centrā dažādās pasaules vietās.

VDAR pieņemšana ir mudinājusi citas pasaules valstis daudzos pasaules reģionos apsvērt iespēju sekot šim piemēram. Šī tendence ir vērojama visā pasaulē: no Čīles līdz Dienvidkorejai, no Brazīlijas līdz Japānai, no Kenijas līdz Indijai un no Kalifornijas līdz Indonēzijai. ES vadība datu aizsardzības jomā parāda, ka tā var darboties kā pasaules mēroga standartu noteicēja digitālās ekonomikas regulēšanai, un to ir atzinīgi novērtējušas ietekmīgas starptautiskās sabiedrības personas, piemēram, ANO ģenerālsekretārs Antoniu Gutērrešs, kurš ir minējis, ka VDAR ir "*rādījusi piemēru* […]*, kas iedvesmo līdzīgus pasākumus citur*" un "*mudina[-āja] ES un tās dalībvalstis turpināt vadīt digitālā laikmeta pilnveidošu un būt tehnoloģisko inovāciju un noteikumu priekšgalā*".[13]

Pašreizējā Covid-19 pandēmijas krīze spilgti parāda šo privātuma debašu globalizāciju gan krīzes laikā, gan tad, kad pasaule tiecas no tās izkļūt. Savienībā vairākas dalībvalstis veica ārkārtas pasākumus, cenšoties aizsargāt sabiedrības veselību. VDAR skaidri nosaka, ka visiem ierobežojumiem ir jārespektē pamattiesību un brīvību būtība un demokrātiskā sabiedrībā tiem ir jābūt nepieciešamiem un samērīgiem pasākumiem, lai aizsargātu sabiedrības intereses, kā, piemēram, sabiedrības veselība. Tā kā ierobežojošie pasākumi tiek pakāpeniski pārtraukti, lēmumu pieņēmējiem ir jāpievēršas tam, lai iedzīvotājiem tiktu piedāvāti uzticami digitāli risinājumi, kas ievēro tiesības uz privātumu un personas datu aizsardzību.

Daudzās valstīs iebūvēti privātuma aizsardzības mehānismi, piemēram, lietotāju brīvprātīga reģistrēšanās, datu minimizēšana un drošība, kā arī ģeogrāfiskās atrašanās vietas izslēgšana, tiek uzskatīti par būtiskiem, lai nodrošinātu uzticamību un sabiedrisko atzīšanu uz datiem orientētiem risinājumiem, kuru mērķis ir uzraudzīt un ierobežot vīrusa izplatību, kalibrēt sabiedriskās kārtības pretpasākumus, sniegt palīdzību pacientiem vai īstenot izejas stratēģijas. Datu aizsardzības un privātuma tiesiskais regulējums ES[14] ir izrādījies pietiekami elastīgs rīks, kas ļauj izstrādāt praktiskus risinājumus (piemēram, izsekošanas lietotnes), vienlaikus nodrošinot augstu personas datu aizsardzības līmeni. Šajā sakarā 2020. gada 16. aprīlī Komisija publicēja norādījumus lietotnēm, kas sniedz atbalstu cīņā pret pandēmiju saistībā ar datu aizsardzību.[15]

Personas datu aizsardzība ir arī būtisks līdzeklis, ar ko novērst manipulēšanu ar iedzīvotāju izvēlēm, jo īpaši ar tādu mērķauditorijas atlasi, kas vērsta uz vēlētājiem,

---

[13] ANO ģenerālsekretāra uzruna Itālijas Senātā 2019. gada 18. decembrī (pieejama: https://www.un.org/press/en/2019/sgsm19916.doc.htm).

[14] Papildus VDAR šajā tiesiskajā regulējumā ietilpst arī E-privātuma direktīva (Direktīva 2002/58/EK), kas cita starpā paredz noteikumus par piekļuvi informācijai un tās glabāšanu lietotāja gala iekārtās.

[15] Komisijas paziņojums "Norādījumi par lietotnēm, kas sniedz atbalstu cīņā pret Covid-19 pandēmiju saistībā ar datu aizsardzību" (2020/C 124 I/01, C/2020/2523, OV C 124I, 17.4.2020, 1.–9. lpp.). 2020. gada 16. aprīlī, reaģējot uz koronavīrusa pandēmiju, ES dalībvalstis ar Komisijas atbalstu ir izstrādājušas ES instrumentu kopumu mobilo lietotņu izmantošanai kontaktu izsekošanai un brīdināšanai. Šī ir daļa no kopīgas koordinētas pieejas, lai atbalstītu pakāpenisku brīvas pārvietošanās aizlieguma atcelšanu. https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

pamatojoties uz nelikumīgu personas datu apstrādi, izvairoties no iejaukšanās demokrātiskos procesos un saglabājot atklātās debates, taisnīgumu un caurskatāmību, kas ir būtiski demokrātijas kritēriji. Šī iemesla dēļ 2018. gada septembrī Komisija publicēja norādījumus par Savienības datu aizsardzības regulējuma piemērošanu vēlēšanu kontekstā[16].

Veicot šo novērtējumu un pārskatu, Komisija ņēma vērā Padomes[17], Eiropas Parlamenta[18], Eiropas Datu aizsardzības kolēģijas (turpmāk - "Kolēģija")[19] un individuālo datu aizsardzības iestāžu[20], daudzpusējās ieinteresēto personu grupas[21] un citu ieinteresēto personu ieguldījumu, tostarp izmantojot ceļvedim sniegtās atsauksmes[22].

Vispārējais viedoklis ir tāds, ka divus gadus pēc tam, kad VDAR sāka piemērot, tā ir veiksmīgi sasniegusi savus mērķus, proti, stiprināt personas tiesības uz personas datu aizsardzību un garantēt personas datu brīvu apriti ES[23]. Tomēr ir noteiktas arī vairākas jomas, kurās nākotnē ir veicami uzlabojumi. Tāpat kā vairums ieinteresēto personu un datu aizsardzības iestāžu, Komisija uzskata, ka šobrīd būtu pāragri izdarīt konkrētus secinājumus par VDAR piemērošanu. Ir iespējams, ka lielākā daļa no jautājumiem, kurus identificējušas dalībvalstis un ieinteresētās personas, nākamajos gados tiks atrisināti, pateicoties lielākai pieredzei VDAR piemērošanā. Neskatoties uz to, šajā ziņojumā ir uzsvērtas problēmas, kas līdz šim radušās, piemērojot VDAR, un izklāstīti iespējamie veidi, kā tās risināt.

Neskatoties uz to, ka uzmanība tiek koncentrēta uz diviem jautājumiem, kas uzsvērti VDAR 97. panta 2. punktā, proti, uz starptautisku nosūtīšanu un sadarbības un konsekvences mehānismiem, šis novērtējums un pārskats ir ar plašāku apjomu, lai pievērstos arī jautājumiem, kurus pēdējo divu gadu laikā ir izvirzījuši dažādi dalībnieki.

2 GALVENIE SECINĀJUMI

VDAR ieviešana un sadarbības un konsekvences mehānismu darbība

---

[16] Komisijas norādījumi par Savienības datu aizsardzības regulējuma piemērošanu vēlēšanu kontekstā – Eiropas Komisijas ieguldījums vadītāju sanāksmē Zalcburgā 2018. gada 19. un 20. septembrī, COM/2018/638 final.

[17] Padomes nostāja un secinājumi par Vispārīgās datu aizsardzības regulas piemērošanu: https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/lv/pdf

[18] Eiropas Parlamenta Pilsoņu brīvību, tieslietu un iekšlietu (*LIBE*) komitejas 2020. gada 21. februāra vēstule komisāram Reindersam, atsauce: IPOL-COM-LIBE D (2020)6525.

[19] Kolēģijas ieguldījums VDAR novērtēšanā saskaņā ar 97. pantu, pieņemts 2020. gada 18. februārī: https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en

[20] https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en

[21] Komisijas izveidotās Regulas daudzpusējās ieinteresēto personu grupas sastāvā ir pilsoniskās sabiedrības un uzņēmēju pārstāvji, akadēmiķi un praktizējoši speciālisti: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537

[22] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12322-Report-on-the-application-of-the-General-Data-Protection-Regulation/feedback?p_id=7669437

[23] Skatīt, piemēram, Padomes nostāju un secinājumus, kā arī Kolēģijas ieguldījumu.

VDAR ieviesa inovatīvu pārvaldības sistēmu, kuras pamatā ir neatkarīgas datu aizsardzības iestādes dalībvalstīs un to sadarbība pārrobežu gadījumos un Eiropas Datu aizsardzības kolēģijas ("Kolēģija") ietvaros. Vispārējais uzskats ir tāds, ka datu aizsardzības iestādes ir līdzsvaroti izmantojušas savas nostiprinātās korektīvās pilnvaras, ieskaitot brīdinājumus un rājienus, naudas sodus un pagaidu vai galīgus apstrādes ierobežojumus[24]. Komisija norāda, ka iestādes izmantoja administratīvos naudas sodus, sākot no dažiem tūkstošiem eiro līdz vairākiem miljoniem atkarībā no pārkāpumu smaguma. Citām sankcijām, piemēram, apstrādes aizliegumiem, var būt vienāda, vai pat lielāka preventīva iedarbība nekā naudas sodiem. VDAR galvenais mērķis ir mainīt visu iesaistīto dalībnieku kultūru un izturēšanos personu labā. Sīkāka informācija par korektīvo pilnvaru izmantošanu datu aizsardzības iestādēs ir sniegta pievienotajā dienestu darba dokumentā.

Lai gan vēl ir pāragri pilnībā novērtēt jauno sadarbības un konsekvences mehānismu darbību, datu aizsardzības iestādes ir attīstījušas savstarpējo sadarbību, izmantojot vienas pieturas aģentūras mehānismu[25] un plaši izmantojot savstarpējo palīdzību[26]. Vienas pieturas aģentūras mehānisms, kas ir iekšējā tirgus galvenā priekšrocība, tiek izmantots, lai izlemtu daudzus pārrobežu gadījumus[27]. Pašlaik tiek izskatīti svarīgi lēmumi ar pārrobežu dimensiju, uz kuriem attiecas vienas pieturas aģentūras mehānisms. Šie lēmumi, kuros bieži ir iesaistītas starptautiskas lielo tehnoloģiju uzņēmējsabiedrības, būtiski ietekmēs personu tiesības daudzās dalībvalstīs.

Tomēr patiesi kopīgas Eiropas datu aizsardzības kultūras izveidošana starp datu aizsardzības iestādēm joprojām ir procesā. Datu aizsardzības iestādes vēl nav pilnībā izmantojušas visus instrumentus, ko paredz VDAR, piemēram, kopīgas operācijas, kas varētu novest līdz kopīgai izmeklēšanai. Reizēm kopīgas pieejas atrašana nozīmēja pāriet uz mazāko kopsaucēju, kā rezultātā tika palaistas garām iespējas veicināt lielāku saskaņošanu[28].

Ir nepieciešams turpmāks progress, lai visā ES padarītu efektīvāku un saskaņotāku pārrobežu lietu izskatīšanu, tostarp no procesuālā viedokļa, piemēram, tādos jautājumos kā sūdzību izskatīšanas procedūras, sūdzību pieļaujamības kritēriji, tiesvedības ilgums atšķirīgiem termiņiem vai saistībā ar termiņu neesamību valsts administratīvajā procesuālajā likumā, procedūras laiks, kurā tiek piešķirtas tiesības tikt uzklausītam, kā arī informācija un sūdzības iesniedzēju iesaistīšana procedūras laikā. Atzinīgi vērtējams pārdomu process, ko šajā sakarā uzsāka Kolēģija; un Komisija piedalās šajās diskusijās[29].

Kolēģijas darbībām un vadlīnijām ir būtiska nozīme, lai konsekventi turpinātu attīstīt apmaiņu starp Kolēģiju un ieinteresētajām personām[30]. Līdz 2019. gada beigām

---

[24] Skatīt dienestu darba dokumenta 2.1. punktu.

[25] Ja uzņēmējsabiedrība apstrādā datus pārrobežu mērogā, kompetentā datu aizsardzības iestāde ir tās dalībvalsts iestāde, kurā uzņēmējsabiedrībai ir galvenā uzņēmējdarbības vieta.

[26] Skatīt dienestu darba dokumenta 2.2. punktu.

[27] Laikā no 2018. gada 25. maija līdz 2019. gada 31. decembrim, izmantojot vienas pieturas aģentūras mehānismu, tika iesniegts 141 lēmumu projekts, no kuriem tika pieņemti 79 galīgie lēmumi.

[28] Piemēram, valstu saraksti par apstrādes darbību veidiem, kuriem jāveic datu aizsardzības ietekmes novērtējums saskaņā ar VDAR 35. pantu, varēja būt labāk saskaņoti.

[29] Skatīt dienestu darba dokumenta 2.2. punktu.

[30] Jo īpaši uzņēmējdarbības un pilsoniskās sabiedrības pārstāvji. Skatīt dienestu darba dokumenta 2.3. punktu.

Kolēģija bija pieņēmusi 67 dokumentus, tostarp 10 jaunas pamatnostādnes[31] un 43 atzinumus[32]. Ieinteresētās personas parasti atzinīgi vērtē Kolēģijas pamatnostādnes un pieprasa papildu pamatnostādnes par galvenajiem VDAR terminiem, kā arī norāda uz neatbilstībām starp valstu norādēm un Kolēģijas pamatnostādnēm. Viņas uzsver vajadzību pēc praktiskākiem padomiem, jo īpaši konkrētākiem piemēriem, un vajadzību datu aizsardzības iestādēm būt aprīkotām ar nepieciešamajiem cilvēkresursiem un tehniskajiem un finanšu resursiem, lai efektīvi veiktu savus uzdevumus.

Komisija konsekventi uzsvēra dalībvalstu pienākumu piešķirt pietiekamus cilvēkresursus, finanšu un tehniskos resursus valstu datu aizsardzības iestādēm[33]. Lielākajā daļā iestāžu bija novērojams personāla un budžeta pieaugums laikā no 2016. līdz 2019. gadam[34], un Īrijas, Nīderlandes, Islandes, Luksemburgas un Somijas iestādēs bija novērojams vislielākais personāla pieaugums. Ņemot vērā, ka lielākās starptautiskās lielo tehnoloģiju uzņēmējsabiedrību galvenā uzņēmējdarbības vieta ir Īrija un Luksemburga, šo valstu datu aizsardzības iestādes darbojas kā vadošās iestādes daudzos svarīgos pārrobežu gadījumos, un tām var būt vajadzīgi lielāki resursi nekā to iedzīvotāji varētu domāt. Tomēr situācija starp dalībvalstīm joprojām ir nevienmērīga un kopumā vēl nav apmierinoša. Datu aizsardzības iestādēm ir būtiska loma, lai nodrošinātu, ka VDAR tiek īstenota valsts līmenī un Kolēģijā efektīvi tiek realizēti sadarbības un konsekvences mehānismi, jo īpaši vienas pieturas aģentūras mehānisms pārrobežu gadījumos. Tāpēc dalībvalstis tiek aicinātas sev nodrošināt pietiekamus resursus, kā to prasa VDAR[35].

Saskaņoti noteikumi, taču joprojām ir zināma sadrumstalotība un atšķirīgas pieejas

Komisija uzrauga VDAR ieviešanu valstu tiesību aktos. Šī ziņojuma sagatavošanas laikā, izņemot Slovēniju, visas dalībvalstis pieņēma jaunus tiesību aktus vai pielāgoja savus datu aizsardzības likumus. Slovēnijai[36] ir lūgts sniegt paskaidrojumus Komisijai par šī procesa pabeigšanu[37].

VDAR nodrošina konsekventu pieeju datu aizsardzības noteikumiem visā ES. Tomēr tā nosaka pienākumu dalībvalstīm pieņemt tiesību aktus dažās jomās[38] un dod tām iespēju sīkāk precizēt VDAR citās jomās[39]. Tā rezultātā joprojām pastāv zināma sadrumstalotība, kas ir īpaši saistīta ar fakultatīvo specifikāciju klauzulu plašu izmantošanu. Piemēram, atšķirības starp dalībvalstīm attiecībā uz bērnu piekrišanas vecumu saistībā ar informācijas sabiedrības pakalpojumiem rada neskaidrības

[31] Tie papildina 10 pamatnostādnes, kuras pieņēma 29. panta darba grupa, gatavojoties regulas piemērošanas sākumam, un kuras apstiprināja Kolēģija. No 2020. gada janvārim līdz maija beigām Kolēģija ir pieņēmusi arī 4 papildu pamatnostādnes un atjauninājusi vienu no esošajām.

[32] 42 no šiem atzinumiem tika pieņemti saskaņā ar VDAR 64. pantu, un viens tika pieņemts saskaņā ar VDAR 70. panta 1. punkta s) apakšpunktu, un tie attiecas uz atbilstības lēmumu Japānai.

[33] Komisijas paziņojums Eiropas Parlamentam un Padomei "Datu aizsardzības noteikumi kā uzticības vairotājs ES un ārpus tās – izvērtējums", COM(2019) 374 final, 24.7.2019.

[34] Kopumā EEZ laikposmā no 2016. līdz 2019. gadam par 42 % ir palielinājies personāla apjoms valstu datu aizsardzības iestādēs un par 49 % ir palielināts valstu datu aizsardzības iestāžu budžets.

[35] Skatīt dienestu darba dokumenta 2.4. punktu.

[36] Pēdējoreiz ar komisāra Reindersa vēstuli 2020. gada martā.

[37] Jāatzīmē, ka Slovēnijas valsts datu aizsardzības iestāde ir izveidota, pamatojoties uz pašreizējiem valsts datu aizsardzības likumiem un uzraugot VDAR piemērošanu šajā dalībvalstī.

[38] Skatīt dienestu darba dokumenta 3.1. punktu.

[39] Skatīt dienestu darba dokumenta 3.2. punktu.

bērniem un viņu vecākiem par bērnu datu aizsardzības tiesību piemērošanu vienotajā tirgū. Šī sadrumstalotība rada problēmas arī pārrobežu uzņēmējdarbības veikšanai, inovācijām, joīpaši attiecībā uz jaunu tehnoloģiju attīstību un kiberdrošības risinājumiem. Lai efektīvi darbotos iekšējais tirgus un izvairītos no nevajadzīga apgrūtinājuma uzņēmējsabiedrībām, ir arī svarīgi, lai valstu tiesību akti nepārsniegtu VDAR noteiktās robežas vai neieviestu papildu prasības, ja robežas nav noteiktas.

Īpaša problēma valstu tiesiskajiem regulējumiem ir tiesību uz personas datu aizsardzību saskaņošana ar vārda un informācijas brīvību un šo tiesību pareiza līdzsvarošana. Dažos valstu tiesiskajos regulējumos ir noteikts vārda brīvības prioritātes princips, savukārt citos – personas datu aizsardzības prioritāte un atbrīvošana no datu aizsardzības noteikumu piemērošanas ir pieļaujama tikai īpašās situācijās, piemēram, ja tas attiecas uz publisku personu. Visbeidzot, attiecībā uz atkāpēm no dažiem VDAR noteikumiem citas dalībvalstis paredz zināmu līdzsvaru starp likumdevēju un / vai katra atsevišķa gadījuma izvērtēšanu.

Komisija turpinās novērtēt valstu tiesisko regulējumu. Saskaņošanai ir jābūt paredzētai likumā, ievērojot šo pamattiesību būtību, un tai ir jābūt samērīgai un nepieciešamai[40]. Datu aizsardzības noteikumiem (kā arī to interpretācijai un piemērošanai) nevajadzētu ietekmēt vārda un informācijas brīvības izmantošanu, piemēram, radot atturošu efektu vai izdarot spiedienu uz žurnālistiem atklāt savus avotus. Šo divu tiesību līdzsvarošana ar valstu likumiem būtu jāiekļauj Tiesas un Eiropas Cilvēktiesību tiesas judikatūrā[41].

Dalībvalstu tiesiskajā regulējumā tiek ievērotas dažādas pieejas, ieviešot atkāpes no vispārējā aizlieguma apstrādāt īpašas personas datu kategorijas attiecībā uz specifikācijas līmeni un drošības pasākumiem, tostarp veselības un pētniecības mērķiem. Lai risinātu šo jautājumu, Komisija kā pirmo soli apraksta dalībvalstu dažādās pieejas[42] un kā nākamo soli atbalstīs tādu rīcības kodeksu(-u) izveidi, kas veicinātu konsekventāku pieeju šajā jomā un atvieglotu personas datu pārrobežu apstrādi[43]. Turklāt Kolēģijas turpmākās pamatnostādnes par personas datu izmantošanu zinātniskās pētniecības jomā sekmēs saskaņotu pieeju. Komisija sniegs ieguldījumu Kolēģijai, jo īpaši saistībā ar veselības pētniecību, tostarp konkrētu jautājumu veidā un atsevišķu scenāriju analīzes veidā, ko tā ir saņēmusi no pētniecības kopienas.

[40] Hartas 52. panta 1. punkts.
[41] Skatīt dienestu darba dokumenta 3.1. punkta. Tiesību uz personas datu aizsardzību saskaņošana ar vārda un informācijas brīvību.
[42] Komisija ir sākusi pētījumu "Dalībvalstu noteikumu novērtējums par veselības datiem saistībā ar VDAR", Chafea/2018/Health/03, īpašais līgums Nr. 2019 70 01.
[43] Skatīt darbības, kas ir minētas Eiropas datu stratēģijā, 30. lpp.

Personām piešķir tiesības kontrolēt savus datus

Saskaņā ar Pamattiesību pētījumu[44] 69% ES iedzīvotāju, kas ir vecāki par 16 gadiem, ir dzirdējuši par VDAR, un 71% cilvēku ES zina par savu valsts datu aizsardzības iestādi.

Personas arvien vairāk apzinās savas tiesības: tiesības piekļūt saviem personas datiem, tos labot, dzēst un pārvietot, tiesības iebilst pret apstrādi, kā arī informēti par datu uzlabotu pārredzamību. VDAR ir nostiprinājusi procesuālās tiesības, ietverot tiesības iesniegt sūdzību datu aizsardzības iestādei, tostarp izmantojot pārstāvības prasības un tiesisko aizsardzību. Personas arvien vairāk izmanto šīs tiesības, taču ir nepieciešams atvieglot to izmantošanu un pilnīgu izpildi. Kolēģijas vadītais pārdomu process ieviesīs skaidrību un vēl vairāk atvieglos personīgo tiesību izmantošanu, savukārt ierosinātā direktīva par pārstāvības prasībām[45] pēc tās pieņemšanas ļaus indivīdiem iesniegt kolektīvās prasības visās dalībvalstīs un pazeminās pārrobežu prasību izmaksas.

Tiesībām uz datu pārnešanu ir skaidrs potenciāls, kas joprojām netiek pilnībā izmantots, tas ir, padarīt cilvēkus par datu ekonomikas centru, dodot tiem iespēju pārslēgties starp dažādiem pakalpojumu sniedzējiem, apvienot dažādus pakalpojumus, izmantot citus inovatīvus pakalpojumus un izvēlēties datu aizsardzībai visdraudzīgākos pakalpojumi. Tas netiešā veidā veicinās konkurenci un atbalstīs inovācijas. Šī potenciāla izmantošana ir viena no Komisijas prioritātēm, jo īpaši tāpēc, ka, arvien vairāk izmantojot lietu interneta ierīces, arvien vairāk datu tiek iegūts no patērētājiem, kuri riskē saskarties ar negodīgu praksi un "iestrēgšanas" efektu. Pārnešana varētu sniegt ievērojamu ieguvumu attiecībā uz veselību un labsajūtu, samazinātu ietekmi uz vidi un piekļuvi sabiedriskajiem un privātajiem pakalpojumiem, augstāku produktivitāti ražošanā un lielāku produktu kvalitāti un drošību.

Datu stratēģija uzsvērta vajadzību risināt tādas grūtības kā standartu trūkums, kas ļauj iesniegt datus mašīnlasāmā formātā, lai palielinātu datu pārnešanas tiesību efektīvu izmantošanu, kas pašlaik aprobežojas tikai ar dažiem sektoriem (piemēram, bankas un telekomunikācijas). To jo īpaši varētu izdarīt, izstrādājot atbilstošus instrumentus, standartizētu formātu un saskarnes[46]. Šo pieaugošo izmantošanu varētu arī panākt, jo īpaši attīstot tehniskās saskarnes un mašīnlasāmus formātus, kas nodrošinātu datu pārnešanu reāllaikā. Plašāka tiesību uz pārnešanu izmantošana personām cita starpā varētu atvieglot iespēju ļaut izmantot savus datus sabiedrības labā (piemēram, lai veicinātu pētījumus veselības sektorā), ja viņas to vēlas ("datu altruisms"). Gatavojot Digitālo pakalpojumu likuma paketi[47], Komisija plašāk izpētīs datu un ar tiem saistītās prakses nozīmi platformas ekosistēmā.

---

[44] Eiropas Savienības Pamattiesību aģentūra (*FRA*) (2020): 2019. gada Pamattiesību pētījums Datu aizsardzība un tehnoloģijas: https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection

[45] Paredzams, ka ierosinātā Direktīva par pārstāvības prasībām patērētāju kolektīvo interešu aizsardzībai (COM/2018/0184 final, 2018/089 (COD)) pēc tās pieņemšanas stiprinās pārstāvības prasību sistēmu arī datu aizsardzības jomā.

[46] Šie instrumenti var ietvert piekrišanas pārvaldības instrumentus un personiskās informācijas pārvaldības mobilās lietotnes.

[47] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_962

Iespējas un izaicinājumi organizācijām, jo īpaši maziem un vidējiem uzņēmumiem

VDAR, kā arī Regula par nepersondatu brīvu apriti[48] piedāvā iespējas uzņēmumiem, veicinot konkurenci un inovācijas, nodrošinot brīvu datu plūsmu ES un radot līdzvērtīgus konkurences apstākļus uzņēmumiem, kas ir reģistrēti ārpus ES.[49]. Tiesībām uz pārnešanu kopā ar arvien pieaugošo personu skaitu, kas meklē privātumam draudzīgākus risinājumus, ir potenciāls samazināt šķēršļus uzņēmumu ienākšanai tirgū un pavērt iespējas izaugsmei, kas ir balstīta uz uzticēšanos un inovācijām. Dažas ieinteresētās personas ziņo, ka VDAR piemērošana ir problemātiska, jo īpaši maziem un vidējiem uzņēmumiem (MVU). Saskaņā ar pieeju, kas balstīta uz risku, nebūtu lietderīgi paredzēt atkāpes, pamatojoties uz ekonomikas dalībnieku lielumu, jo to lielums pats par sevi nenorāda uz riskiem, kurus personas datu apstrāde, ko tie veic, var radīt indivīdiem. Vairākas datu aizsardzības iestādes ir nodrošinājušas praktiskus instrumentus, lai atvieglotu VDAR īstenošanu MVU, kuri veic zema riska apstrādes darbības. Šie centieni būtu jāpastiprina un jāizplata, vēlams, izmantojot kopēju Eiropas pieeju, lai neradītu šķēršļus vienotajam tirgum.

Datu aizsardzības iestādes ir izstrādājušas vairākus pasākumus, lai palīdzētu MVU ievērot VDAR, piemēram, nodrošinot līgumu apstrādes veidnes un apstrādes darbību ierakstus, seminārus un konsultāciju līnijas. Vairākas no šīm iniciatīvām saņēma ES finansējumu[50]. Būtu jāapsver turpmāki pasākumi, lai atvieglotu VDAR piemērošanu MVU.

VDAR ievieš instrumentu kopumu, kas ir pieejams visiem uzņēmumiem un organizācijām, lai palīdzētu tiem pierādīt atbilstību, piemēram, rīcības kodeksus, sertifikācijas mehānismus un standarta līguma klauzulu. Šis instrumentu kopums būtu jāizmanto pilnā apjomā. MVU īpaši uzsver to situācijai pielāgotu rīcības kodeksu, kuri neizraisa nesamērīgas izmaksas, nozīmi un lietderību. Attiecībā uz sertifikācijas shēmām drošība (ieskaitot kiberdrošību) un integrēta datu aizsardzība ir galvenie elementi, kas jāņem vērā saskaņā VDAR, un tiem būtu noderīga kopīga un vērienīga pieeja visā ES. Komisija šobrīd strādā pie standarta līguma klauzulām starp pārziņiem un apstrādātājiem[51], balstoties uz pašreizējo darbu standarta līguma noteikumu starptautiskiem pārsūtījumiem modernizēšanu[52].

VDAR piemērošana jaunām tehnoloģijām

Tā kā VDAR ir izstrādāta tehnoloģiski neitrālā veidā, tā balstās uz principiem, un tādējādi tā ir sastādīta, lai aptvertu jaunās tehnoloģijas to attīstības laikā.

---

[48] Eiropas Parlamenta un Padomes Regula (ES) 2018/1807 (2018. gada 14. novembris) par satvaru nepersondatu brīvai apritei Eiropas Savienībā (OV L 303, 28.11.2018., 59.-68. lpp.).

[49] Skatīt dienestu darba dokumenta 5. punktu. Skatīt arī Regulas par satvaru nepersondatu brīvai apritei Eiropas Savienībā vadlīnijas (COM/2019/250 final), izskaidrojot noteikumus, kas regulē jauktu datu kopu, kas sastāv gan no personīgiem, gan nepersonas datiem, apstrādi, padarot tās praktiskas uzņēmumiem, ieskaitot MVU.

[50] Komisija sniedza finansiālu atbalstu, izmantojot trīs piešķīrumu veidus, kopsummā 5 miljonu EUR apmērā, no kuriem pēdējie divi bija īpaši paredzēti, lai atbalstītu valsts datu aizsardzības iestādes to centienos sazināties ar privātpersonām un maziem un vidējiem uzņēmumiem: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en. 2020. gadā tiks papildus piešķirts 1 miljons EUR.

[51] Saskaņā ar VDAR 28. pantu.

[52] Saskaņā ar VDAR 46. pantu.

To uzskata par būtisku un elastīgu instrumentu, lai nodrošinātu, ka jauno tehnoloģiju attīstība notiek saskaņā ar pamattiesībām. Datu aizsardzības un privātuma tiesiskais regulējums pierādīja tā nozīmi un elastīgumu Covid-19 krīzes laikā, jo īpaši saistībā ar izsekošanas mobilo lietotņu un citu tehnoloģisko risinājumu izstrādi cīņā pret pandēmiju. Nākotnē ir gaidāmi izaicinājumi, lai noskaidrotu, kā pārbaudītos principus piemērot tādām specifiskām tehnoloģijām kā mākslīgais intelekts, blokķēde, lietu internets vai sejas atpazīšana, kurām ir nepieciešama pastāvīga uzraudzība. Piemēram, Komisijas Baltā grāmata par mākslīgo intelektu[53] aizsāka publiskas debates par īpašiem apstākļiem, ja tādi ir, kas varētu attaisnot mākslīgā intelekta izmantošanu attālās biometriskās identifikācijas nolūkos (piemēram, sejas atpazīšanā) sabiedriskās vietās un kopīgiem aizsardzības pasākumiem. Šajā ziņā datu aizsardzības iestādēm jābūt gatavām jau drīzumā pavadīt tehniskā projekta procesus.

Turklāt spēcīga un efektīva VDAR ieviešana attiecībā pret lielām digitālajām platformām un integrētām uzņēmējsabiedrībām, tostarp tādās jomās kā tiešsaistes reklāma un smalka mērķauditorijas atlase, ir būtisks elements personu aizsardzībā.

Mūsdienīga un starptautiska datu nosūtīšanas instrumentu kopuma izstrāde

VDAR piedāvā modernizētu instrumentu kopumu, lai atvieglotu personas datu nosūtīšanu no ES uz trešo valsti vai starptautisku organizāciju, vienlaikus nodrošinot, ka datiem joprojām tiek piemērots augsts aizsardzības līmenis. Iepriekšējos divos gados Komisija ir pastiprinājusi veicamās darbības, lai pilnībā izmantotu to instrumentu potenciālu, kuri ir pieejami saskaņā ar VDAR.

Tas ietvēra aktīvu iesaistīšanos attiecībās ar galvenajiem partneriem, lai panāktu "atbilstības lēmumu". Šāda lēmuma mērķis ir nodrošināt drošu un brīvu personas datu apriti uz attiecīgo trešo valsti bez nepieciešamības datu eksportētājam sniegt papildu garantijas vai saņemt atļauju. It īpaši ES un Japānas savstarpējie atbilstības lēmumi, kas stājās spēkā 2019. gada februārī, izveidoja vislielāko brīvo un drošo datu aprites zonu pasaulē. Turklāt atbilstības nodrošināšanas process ar Korejas Republiku ir pavirzījies uz priekšu, un notiek izpētes sarunas ar citiem svarīgiem partneriem Āzijā un Latīņamerikā.

Atbilstībai ir liela nozīme arī turpmākajās attiecībās ar Apvienoto Karalisti, ja tiek ievēroti piemērojamie nosacījumi. Tas ir labvēlīgs faktors tirdzniecībai, ieskaitot digitālo tirdzniecību, un būtisks priekšnosacījums ciešai un vērienīgai sadarbībai tiesiskās aizsardzības un drošības jomā. Turklāt augsta konverģences pakāpe datu aizsardzībā ir svarīgs elements, lai nodrošinātu līdzvērtīgus konkurences apstākļus starp divām tik cieši integrētām ekonomikām. Saskaņā ar Politisko deklarāciju par turpmākajām attiecībām starp ES un Apvienoto Karalisti Komisija pašlaik veic atbilstības novērtējumu atbilstoši VDAR un Datu aizsardzības tiesību aktu izpildes direktīvai[54].

---

[53] Baltā grāmata par mākslīgo intelektu "Eiropiska pieeja - izcilība un uzticēšanās", COM/2020/65 final.

[54] 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 krimināsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI (OV L 119, 4.5.2016., 89.–131. lpp.).

Pirmā VDAR novērtējuma ietvaros Komisijai arī jāpārskata lēmumi par atbilstību, kas tika pieņemti saskaņā ar iepriekšējiem noteikumiem.[55]. Komisijas dienesti ir uzsākuši intensīvu dialogu ar katru no 11 attiecīgajām trešām valstīm un teritorijām[56], lai novērtētu, kā viņu datu aizsardzības sistēmas ir attīstījušās kopš atbilstības lēmuma pieņemšanas un vai tās atbilst VDAR noteiktajiem standartiem. Vajadzība nodrošināt šādu lēmumu nepārtrauktību kā galveno tirdzniecības un starptautiskās sadarbības instrumentu ir viens no faktoriem, kas vairākas no šīm valstīm un teritorijām ir pamudinājis modernizēt un stiprināt savus privātuma likumus. Ar dažām no šīm valstīm un teritorijām tiek apspriesti papildu aizsardzības pasākumi, lai novērstu būtiskas aizsardzības atšķirības. Tomēr, ņemot vērā to, ka Tiesa spriedumā, kas pasludināms 16. jūlijā, var sniegt paskaidrojumus, kas varētu būt būtiski attiecībā uz konkrētiem atbilstības standarta elementiem, Komisija atsevišķi ziņos par pašreizējo atbilstības lēmumu novērtējumu pēc tam, kad Tiesa būs pasludinājusi spriedumu šajā lietā.[57]

Papildus tās atbilstības darbam Komisija strādā pie visaptverošas standarta līguma klauzulu modernizācijas, lai tās atjauninātu, ņemot vērā jaunās prasības, kuras ir ieviesusi VDAR. Mērķis ir labāk atspoguļot apstrādes darbību realitāti mūsdienu digitālajā ekonomikā un apsvērt iespējamo vajadzību, tostarp, ņemot vērā gaidāmo Tiesas judikatūru, sīkāk izskaidrot dažus aizsardzības pasākumus.[58] Šīs klauzulas ir līdz šim visplašāk izmantotais datu nosūtīšanas mehānisms, ar tūkstošiem ES uzņēmumiem, kas uz tām paļaujas, lai sniegtu plašu pakalpojumu klāstu saviem klientiem, piegādātājiem, partneriem un darbiniekiem.

Kolēģijai ir bijusi arī aktīva loma VDAR starptautisko aspektu attīstīšanā. Tas ietver vadlīniju atjaunināšanu attiecībā uz esošajiem nodošanas mehānismiem, piemēram, saistošajiem korporatīvajiem noteikumiem un tā saucamajām "atkāpēm", kā arī tiesiskās infrastruktūras attīstību, lai izmantotu jaunus instrumentus, ko ir ieviesusi VDAR, t.i., rīcības kodeksus un sertifikāciju.

Lai ļautu ieinteresētajām personām pilnībā izmantot VDAR nodošanas instrumentu kopumu, ir svarīgi, lai Kolēģija pastiprinātu pašreizējo darbu pie dažādiem nodošanas mehānismiem, tostarp turpinot pilnveidot saistošo korporatīvo noteikumu apstiprināšanas procesu, pabeidzot norādījumus par rīcības kodeksiem un sertifikāciju kā nosūtīšanas instrumentiem un izskaidrojot mijiedarbību starp noteikumiem par starptautisko datu pārsūtīšanu (V nodaļa) un VDAR teritoriālo piemērošanas jomu (3. pants).

Vēl viens svarīgs ES datu aizsardzības noteikumu starptautiskās dimensijas aspekts ir VDAR paplašinātā teritoriālā darbības joma, kas attiecas arī uz ārvalstu tirgus dalībnieku, kas darbojas ES tirgū, apstrādes darbībām. Lai nodrošinātu efektīvu

---

[55] 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., 31.–50. lpp.).

[56] Šīs valstis un teritorijas ir: Andora, Argentīna, Kanāda, Fēru salas, Gērnsija, Džērsija, Menas sala, Izraēla, Jaunzēlande, Šveice un Urugvaja.

[57] Skatīt lietu C-311/18, Datu aizsardzības komisārs pret *Facebook Ireland Limited, Maximillian Schrems* ("Schrems II"), kas attiecas uz lūgumu sniegt prejudiciālu nolēmumu par tā saucamajām standarta līguma klauzulām. Tomēr dažus papildu atbilstības standarta elementus var arī sīkāk izskaidrot Tiesa.

[58] Skatīt *Schrems II* lietu.

VDAR ievērošanu un patiesi līdzvērtīgus konkurences apstākļus, ir svarīgi, lai šis paplašinājums tiktu pienācīgi atspoguļots datu aizsardzības iestāžu izpildes darbībās. Tajos, jo īpaši vajadzības gadījumā, ir jāiesaista pārziņa vai apstrādātāja pārstāvis ES, kuru var uzrunāt papildus uzņēmumam, kas atrodas ārpus ES, vai tā vietā. Šī pieeja būtu jāīsteno enerģiskāk, lai nosūtītu skaidru vēstījumu, ka uzņēmuma neesamība Savienībā neatbrīvo ārvalstu operatorus no viņu pienākumiem saskaņā ar VDAR.

Konverģences un starptautiskās sadarbības veicināšana datu aizsardzības jomā

VDAR jau ir kļuvusi par galveno atskaites punktu starptautiskā līmenī un tā darbojās kā katalizators, liekot daudzām pasaules valstīm apsvērt iespēju ieviest mūsdienīgus privātuma noteikumus. Šī globālās konverģences tendence ir ļoti pozitīva attīstība, kas sniedz jaunas iespējas labāk aizsargāt personas ES, kad viņu datus nosūta uz ārzemēm, vienlaikus atvieglojot datu apriti.

Balstoties uz šo tendenci, Komisija ir pastiprinājusi dialogu vairākos divpusējos, reģionālos un daudzpusējos forumos, lai veicinātu privātuma ievērošanas globālo kultūru un attīstītu dažādu privātuma sistēmu konverģences elementus. Savos centienos Komisija ir paļāvusies un turpinās paļauties uz Eiropas Ārējās darbības dienesta un ES delegāciju trešajās valstīs un misiju starptautiskajās organizācijās tīkla aktīvu atbalstu. Tas ir ļāvis arī panākt lielāku konsekvenci un savstarpēju papildinātību starp dažādiem ES politikas ārējās dimensijas aspektiem – sākot ar tirdzniecību un beidzot ar jaunajām ES un Āfrikas partnerattiecībām. G20 un G7 nesen arī ir atzinuši datu aizsardzības ieguldījumu digitālās ekonomikas un datu aprites uzticamības vairošanā, jo īpaši izmantojot jēdzienu "Datu brīva plūsma ar uzticēšanās", ko sākotnēji ierosināja Japānas G20 prezidentūra.[59] Datu stratēģija uzsver Komisijas nodomu turpināt veicināt datu apmaiņu ar uzticamiem partneriem, vienlaikus cīnoties pret tādiem ļaunprātīgas izmantošanas gadījumiem kā (ārvalstu) valsts iestāžu nesamērīga piekļuve personas datiem.

Veicinot datu aizsardzības standartu konverģenci starptautiskā līmenī, kā veidu, lai atvieglotu datu apriti un tādējādi tirdzniecību, Komisija ir arī apņēmusies cīnīties pret digitālo protekcionismu, kā nesen uzsvērts Datu stratēģijā.[60] Šajā nolūkā tā ir izstrādājusi īpašus noteikumus par datu apriti un datu aizsardzību tirdzniecības nolīgumos[61], kurus tā sistemātiski iesniedz divpusējās – starp pēdējām ar Austrāliju, Jaunzēlandi un Apvienoto Karalisti – un daudzpusējās sarunās, piemēram, pašreizējā PTO e-komercijas sarunas[62]. Šie horizontālie noteikumi izslēdz nepamatotu ierobežojumu, tostarp datu teritoriālas ierobežošanas piespiedu prasību, piemērošanu, vienlaikus saglabājot pušu regulatīvo autonomiju aizsargāt pamattiesības uz datu aizsardzību.

---

[59] Skatīt G20 Osakas līderu Deklarācijas tekstu: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf

[60] Datu stratēģija, 23. lpp.

[61] Skatīt horizontālo noteikumu tekstu par pārrobežu datu apriti un personas datu aizsardzību (ES tirdzniecības un ieguldījumu nolīgumos): https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf

[62] 84 PTO locekļi tagad ir iesaistījušies daudzpusējās sarunās par e-komerciju saskaņā ar Kopīgā paziņojuma iniciatīvu, kuru ministri pieņēma 2019. gada 25. janvārī Davosā. Šī procesa ietvaros ES 2019. gada 3. maijā iesniedza savu teksta priekšlikumu par turpmākajiem noteikumiem un pienākumiem e-komercijā. Priekšlikumā ir iekļauti horizontālie noteikumi par datu apriti un personas datu aizsardzību: https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf.

Tāpēc tirdzniecības un datu aizsardzības instrumentu sinerģija būtu tālāk jāpēta, lai nodrošinātu brīvu un drošu starptautisku datu apriti, kas ir būtiska Eiropas uzņēmējsabiedrību, tostarp MVU, uzņēmējdarbībai, konkurētspējai un izaugsmei arvien digitalizētākā ekonomikā.

Tāpat ir svarīgi nodrošināt, ka gadījumos, kad uzņēmumi, kas darbojas Eiropas tirgū, tiek aicināti izpaust datus tiesībaizsardzības nolūkos, tie var to darīt, nesaskaroties ar tiesību normu kolīzijām un pilnībā ievērojot ES pamattiesības. Nolūkā uzlabot šādus darījumus, Komisija ir apņēmusies kopā ar saviem starptautiskajiem partneriem izstrādāt piemērotu tiesisko regulējumu, lai izvairītos no tiesību normu kolīzijām un atbalstītu efektīvus sadarbības veidus, jo īpaši nodrošinot nepieciešamos datu aizsardzības pasākumus, un tādējādi sekmējot efektīvāku cīņu pret noziedzību.

Visbeidzot, laikā, kad privātuma ievērošanas jautājumi vai datu drošības negadījumi var ietekmēt lielu skaitu personu vienlaikus vairākās jurisdikcijās, būtu jāturpina stiprināt Eiropas un starptautisko regulatoru sadarbība "uz vietas". Jo īpaši tas prasa atbilstošu juridisko instrumentu izstrādi ciešākiem sadarbības un savstarpējas palīdzības veidiem, tostarp ļaujot veikt vajadzīgo informācijas apmaiņu izmeklēšanas kontekstā. Šajā kontekstā Komisija izveido arī "Datu aizsardzības akadēmiju" – platformu, kurā ES un ārvalstu datu aizsardzības iestādes dalītos zināšanās, pieredzē un paraugpraksē, lai atvieglotu un atbalstītu privātuma nodrošinātāju sadarbību.

3 TURPMĀKĀS DARBĪBAS

Lai pilnībā izmantotu VDAR potenciālu, ir svarīgi izveidot saskaņotu pieeju un Eiropas kopējo datu aizsardzības kultūru un veicināt efektīvāku un saskaņotāku pārrobežu lietu izskatīšanu. To sagaida cilvēki un uzņēmumi, un tas ir būtisks mērķis ES datu aizsardzības noteikumu reformā. Tikpat svarīgi ir nodrošināt, ka visi VDAR minētie instrumenti tiek pilnībā izmantoti, lai nodrošinātu efektīvu piemērošanu privātpersonām un uzņēmumiem.

Komisija turpinās tās divpusējās sarunas ar dalībvalstīm par VDAR ieviešanu un nepieciešamības gadījumā turpinās izmantot visus tās rīcībā esošos instrumentus, lai veicinātu to, ka dalībvalstis ievēro savas no VDAR izrietošās saistības.

Ņemot vērā notiekošo valstu tiesību aktu novērtēšanu, īso praktiskās pieredzes periodu kopš VDAR spēkā stāšanās un faktu, ka daudzās dalībvalstīs joprojām tiek pārskatīti specifisku sektoru tiesību akti, vēl ir par agru izdarīt galīgus secinājumus par esošo sadrumstalotības līmeni. Attiecībā uz iespējamo tiesību normu kolīziju, ko rada speciālu klauzulu ieviešana dalībvalstīs, vispirms ir svarīgāk izprast sekas pārziņiem un apstrādātājiem[63].

Pievēršoties šiem jautājumiem, attiecīgā valstu tiesu un Tiesas judikatūra palīdz radīt konsekventu datu aizsardzības noteikumu interpretāciju. Valstu tiesas nesen ir pieņēmušas spriedumus, ar kuriem atceļ valstu tiesību normas, kas neatbilst VDAR[64].

Attiecībā uz starptautisko dimensiju Komisija arī turpmāk koncentrēsies uz datu aizsardzības noteikumu konverģences veicināšanu kā veidu, lai nodrošinātu drošu

[63] Sal. Padomes nostāja un secinājumi par VDAR piemērošanu.
[64] Tas ir noticis Vācijā un Spānijā, kā arī Austrijā, novēršot trūkumus valstu tiesību aktos.

datu apriti. Tas ietver dažādas "iepriekšējā posma" darba formas, piemēram, saistībā ar notiekošajām jauno vai atjauninātu datu aizsardzības likumu reformām vai virzību uz koncepciju "Datu brīva plūsma uzticēšanās gaisotnē" daudzpusējos forumos. Tas aptver arī dažādus dialogus par piemērotību un mūsu nosūtīšanas instrumentu kopuma modernizāciju un paplašināšanu, atjauninot standarta līguma klauzulas un sagatavojot pamatu sertifikācijas mehānismiem. Šis darbs ietver arī starptautiskas sarunas, piemēram, elektronisku pierādījumu pārrobežu piekļuves jomā, lai nodrošinātu, ka datu nosūtīšana notiks, ievērojot attiecīgus datu aizsardzības pasākumus. Visbeidzot, iesaistoties sarunās par starptautisko sadarbību un savstarpējo palīdzību starp datu aizsardzības nodrošinātājiem, Komisija centīsies panākt konverģenci "no teorijas uz praksi".

Balstoties uz šo VDAR piemērošanas novērtējumu, kas tika uzsākts 2018. gada maijā, tālāk tiek uzskaitītas sekojošās darbības, kas nepieciešamas, lai atbalstītu tās piemērošanu. Komisija uzraudzīs to īstenošanu, arī ņemot vērā gaidāmo novērtējuma ziņojumu 2024. gadā.

Tiesiskā regulējuma īstenošana un papildināšana

Dalībvalstīm vajadzētu

- pabeigt sektoru tiesību normu saskaņošanu ar VDAR;
- apsvērt iespēju ierobežot speciālu klauzulu izmantošanu, kas varētu radīt sadrumstalotību un apdraudēt brīvu datu apriti ES;
- novērtēt, vai valstu tiesību akti, ar kuriem īsteno VDAR, jebkuros apstākļos iekļaujas dalībvalstu tiesību aktos paredzētajās robežās.

Komisija

- turpinās divpusēju sadarbību ar dalībvalstīm attiecībā uz valsts tiesību aktu atbilstību VDAR, tostarp attiecībā uz valsts datu aizsardzības iestāžu neatkarību un resursiem; izmantos visus tās rīcībā esošos instrumentus, ieskaitot pārkāpumu procedūras, lai nodrošinātu, ka dalībvalstis ievēro VDAR;
- atbalstīs turpmāku viedokļu un valstu prakses apmaiņu starp dalībvalstīm par tēmām, kuras vēl jāprecizē valsts līmenī, lai mazinātu vienotā tirgus sadrumstalotību, piemēram, tādu veselības datu un ar veselību saistītu datu apstrāde vai izpēte, kuras tiek pakļautas līdzsvarošanai ar citām tiesībām, piemēram, vārda brīvību;
- atbalstīs datu aizsardzības sistēmas konsekventu piemērošanu saistībā ar jaunām tehnoloģijām, lai atbalstītu inovācijas un tehnoloģiju attīstību;
- izmantos VDAR dalībvalstu ekspertu grupu (izveidota pārejas posmā pirms VDAR piemērošanas), lai atvieglotu diskusijas un pieredzes apmaiņu starp dalībvalstīm un ar Komisiju;
- izpētīs, vai, ņemot vērā turpmāko pieredzi un atbilstošo judikatūru, varētu būt lietderīgi ierosināt turpmākus mērķtiecīgus grozījumus atsevišķos VDAR noteikumos, jo īpaši attiecībā uz apstrādes ierakstiem, ko veic MVU, kuru

uzņēmējdarbības pamatā nav personas datu apstrāde (zems risks)[65] un attiecībā uz iespējamo bērnu pilngadības vecuma saskaņošanu saistībā ar informācijas sabiedrības pakalpojumiem.

Jaunās pārvaldības sistēmas potenciāla pilnīga izmantošana

Kolēģija un datu aizsardzības iestādes tiek aicinātas

- attīstīt efektīvus pasākumus datu aizsardzības iestāžu starpā attiecībā uz sadarbības un konsekvences mehānismu darbību, ieskaitot procesuālos aspektus, balstoties uz tās locekļu kompetenci un pastiprinot sekretariāta iesaistīšanos;
- atbalstīt VDAR piemērošanas un izpildes saskaņošanu, izmantojot visus tās rīcībā esošos līdzekļus, tostarp sīkāk izskaidrojot VDAR galvenos jēdzienus un nodrošinot, ka valstu norādes pilnībā atbilst Kolēģijas pieņemtajām pamatnostādnēm;
- mudināt izmantot visus VDAR paredzētos instrumentus, lai nodrošinātu to konsekventu piemērošanu;
- pastiprināt sadarbību starp datu aizsardzības iestādēm, piemēram, veicot kopīgu izmeklēšanu.

Komisija

- turpinās cieši uzraudzīt valstu datu aizsardzības iestāžu faktisko un pilnīgo neatkarību;
- veicinās sadarbību starp regulatoriem (jo īpaši tādās jomās kā konkurence, elektroniskie sakari, tīkla un informācijas sistēmu drošība un patērētāju politika);
- atbalstīs Kolēģijas pārdomas par procedūrām, kuras piemēro valsts datu aizsardzības iestādes, lai uzlabotu sadarbību pārrobežu gadījumos.

Dalībvalstis

- piešķirs datu aizsardzības iestādēm pietiekamus resursus, lai tās varētu veikt savus uzdevumus.

Atbalsts ieinteresētajām personām

Kolēģija un datu aizsardzības iestādes tiek aicinātas

- pieņemt papildu praktiskas, viegli saprotamas pamatnostādnes, kas sniedz skaidras atbildes un novērš neskaidrības jautājumos, kas saistīti ar VDAR piemērošanu, piemēram, attiecībā uz bērnu datu un datu subjektu tiesību apstrādi, ieskaitot piekļuves tiesību un tiesību izdzēst izmantošanu, konsultējoties ar procesā ieinteresētajām personām;
- pārskatīt pamatnostādnes, vai ir nepieciešami papildu skaidrojumi, ņemot vērā pieredzi un attīstību, tostarp Tiesas judikatūru;

[65] VDAR 30. panta 5. punkts.

- izstrādāt praktiskus instrumentus, piemēram, saskaņotas datu aizsardzības pārkāpumu veidlapas un vienkāršotu apstrādes darbību uzskaiti, lai palīdzētu zema riska MVU pildīt savus pienākumus.

Komisija

- nodrošinās standarta līguma klauzulas gan starptautiskai nosūtīšanai, gan attiecībās ar pārzini / apstrādātāju;
- nodrošinās instrumentus, kas izskaidro / atbalsta datu aizsardzības noteikumu piemērošanu bērniem[66];
- saskaņā ar Datu stratēģiju izpētīs praktiskus līdzekļus, lai atvieglotu personu arvien plašāku tiesību uz pārnešanu izmantošanu, piemēram, dodot viņām lielāku kontroli pār to, kurš var piekļūt un izmantot mašīnas radītus datus;
- atbalstīs standartizāciju/sertifikāciju, jo īpaši kiberdrošības aspektos, izmantojot sadarbību starp Eiropas Savienības Kiberdrošības aģentūru (*ENISA*), datu aizsardzības iestādēm un Kolēģiju;
- attiecīgos gadījumos izmantos savas tiesības lūgt Kolēģiju sagatavot pamatnostādnēs un atzinumus par konkrētiem jautājumiem, kas ir svarīgi ieinteresētajām personām;
- nepieciešamības gadījumā sniegs norādes, pilnībā respektējot Kolēģijas lomu;
- atbalstīs datu aizsardzības iestāžu darbības, kas atvieglo VDAR noteikto pienākumu īstenošanu MVU, sniedzot finansiālu atbalstu, jo īpaši attiecībā uz praktiskiem norādījumiem un digitāliem rīkiem, kurus var ieviest arī citās dalībvalstīs.

Inovāciju veicināšana

Komisija

- pārraudzīs VDAR piemērošanu jaunajām tehnoloģijām, ņemot vērā arī iespējamās turpmākās iniciatīvas mākslīgā intelekta jomā un saskaņā ar Datu stratēģiju;
- veicinās, tostarp ar finansiālu atbalstu, ES rīcības kodeksu izstrādāšanu veselības un pētniecības jomā;
- cieši sekos mobilo lietotņu izstrādei un izmantošanai COVID-19 pandēmijas kontekstā.

Kolēģija tiek aicināta

- izdot pamatnostādnes par VDAR piemērošanu zinātnisko pētījumu, mākslīgā intelekta, blokķēdes un citu tehnoloģiju iespējamā attīstības jomā;
- pārskatīt pamatnostādnes, lai nepieciešamības gadījumā sniegtu papildu skaidrojumus, ņemot vērā tehnoloģiju attīstību.

[66] Komisijas projekts par vecuma noteikšanas instrumentiem – izmēģinājuma projekts, lai demonstrētu sadarbspējīgu tehnisko infrastruktūru bērnu aizsardzībai, ieskaitot vecuma pārbaudi un vecāku piekrišanu. Paredzams, ka tas atbalstīs bērnu aizsardzības mehānismu ieviešanu, pamatojoties uz spēkā esošajiem ES tiesību aktiem, kas attiecas uz bērnu aizsardzību tiešsaistē.

Turpmāka datu nosūtīšanas instrumentu kopuma izstrāde

Komisija

- saskaņā ar stratēģiju, kas izklāstīta tās 2017. gada paziņojumā "Personas datu apmaiņa un aizsardzība globalizētā pasaulē", turpinās atbilstības dialogus ar ieinteresētajām trešajām valstīm, ietverot, ja iespējams, datu nosūtīšanas iespējas krimināl̄as tiesībaizsardzības iestādēm (saskaņā ar Datu aizsardzības tiesību aktu izpildes direktīvu) un citām valsts iestādēm; tas ietver atbilstības procesa pabeigšanu ar Korejas Republiku cik vien drīz iespējams;
- pabeigs pašreizējo atbilstības lēmumu novērtēšanu un ziņos Eiropas Parlamentam un Padomei;
- pabeigs darbu pie standarta līguma klauzulu modernizācijas, lai tās atjauninātu, ņemot vērā VDAR, iekļaujot visus attiecīgos nodošanas scenārijus un labāk atspoguļojot mūsdienu uzņēmējdarbības praksi.

Kolēģija tiek aicināta

- turpināt izskaidrot mijiedarbību starp noteikumiem par starptautisko datu nosūtīšanu (V nodaļa) un VDAR teritoriālo piemērošanas jomu (3. pants);
- nodrošināt efektīvu izpildi attiecībā pret operatoriem, kuri veic uzņēmējdarbību trešajās valstīs un uz kuriem attiecas VDAR teritoriālās piemērošanas joma, tostarp vajadzības gadījumā attiecībā uz pārstāvja iecelšanu (27. pants);
- pilnveidot saistošo korporatīvo noteikumu novērtēšanu un iespējamu apstiprināšanu, lai paātrinātu procesu;
- pabeigt darbu pie rīcības kodeksu un sertifikācijas mehānisma kā datu pārsūtīšanas rīka izveides, procedūras un novērtēšanas kritēriju izstrādes.

Konverģences veicināšana un starptautiskās sadarbības attīstīšana

Komisija

- atbalstīs notiekošos trešo valstu reformu procesus saistībā ar jauniem vai modernizētiem datu aizsardzības noteikumiem, daloties pieredzē un paraugpraksē;
- sadarbosies ar Āfrikas partneriem, lai veicinātu regulatīvo konverģenci un atbalstītu uzraudzības iestāžu spēju veidošanu kā daļu no jauno ES un Āfrikas partnerattiecību digitālās nodaļas;
- novērtēs, kā varētu veicināt sadarbību starp privātiem dalībniekiem un tiesībaizsardzības iestādēm, tostarp apspriežot divpusējus un daudzpusējus datu nosūtīšanas pamatprincipus saistībā ar ārvalstu tiesībaizsardzības iestāžu piekļuvi elektroniskiem pierādījumiem, lai izvairītos no tiesību normu kolīzijām, vienlaikus nodrošinot piemērotus datu aizsardzības pasākumus;
- sadarbosies ar starptautiskām un reģionālām organizācijām, piemēram, *ESAO, ASEAN* vai G20, lai veicinātu uzticamu datu apriti, kuras pamatā ir augsti datu

aizsardzības standarti, tostarp saistībā ar iniciatīvu "Datu aprite uzticēšanās gaisotnē";

- izveidos "Datu aizsardzības akadēmiju", lai atvieglotu un atbalstītu apmaiņu starp Eiropas un starptautiskajiem regulatoriem;
- veicinās starptautisku uzraudzības iestāžu sadarbību starp uzraudzības iestādēm, tostarp izmantojot sarunas par sadarbību un savstarpējas palīdzības nolīgumiem.