

**Komisijas paziņojums Eiropas Parlamentam un Padomei**

**Datu aizsardzības noteikumi kā uzticības vairotājs ES un ārpus tās — izvērtējums**

1. **Ievads**

Vispārīgā datu aizsardzības regula[[1]](#footnote-2) (turpmāk “Regula”) jau vairāk nekā gadu tiek piemērota visā Eiropas Savienībā. Tā ir pamatā saskaņotai un modernizētai ES datu aizsardzības sistēmai, kas ietvar arī Tiesībaizsardzības direktīvu[[2]](#footnote-3) un Regulu par datu aizsardzību ES iestādēs un struktūrās[[3]](#footnote-4). Šis regulējums tiks pabeigts ar E-privātuma regulu, kas patlaban atrodas likumdošanas procesā.

Spēcīgi datu aizsardzības noteikumi ir ļoti svarīga pamattiesību uz personas datu aizsardzību garantija. Tiem ir būtiska loma demokrātiskā sabiedrībā[[4]](#footnote-5), un tie ir svarīga daļa no arvien augošās datu ekonomikas. ES cenšas izmantot daudzās iespējas, ko pakalpojumu, darbvietu un inovācijas jomā piedāvā digitālā transformācija, vienlaikus cīnoties ar šo pārmaiņu radītajām problēmām. Identitātes zādzības, sensitīvu datu noplūdes, personu diskriminācija, integrēta neobjektivitāte, dalīšanās ar nelegālu saturu un invazīvu novērošanas rīku izstrāde ir tikai daži problēmu piemēri, par ko notiek arvien plašākas sabiedrības diskusijas, no kurām ir skaidrs, ka iedzīvotāji sagaida, ka to dati tiks aizsargāti.

Datu aizsardzība ir ieguvusi patiesi globālu nozīmi — cilvēki visā pasaulē arvien vairāk sargā un novērtē savu datu aizsardzību un to drošību. Daudzas valstis ir pieņēmušas vai patlaban pieņem visaptverošus datu aizsardzības noteikumus, balstoties uz principiem, kas līdzinās Regulā ietvertajiem, un tādējādi veidojas globāla datu aizsardzības noteikumu konverģence. Tas sniedz jaunas iespējas atvieglot datu plūsmas starp komercuzņēmumiem vai publiskā sektora iestādēm, vienlaikus paaugstinot personas datu aizsardzības līmeni ES un visā pasaulē.

Datu aizsardzība tiek uztverta nopietnāk nekā jebkad agrāk, un tam ir plaša ietekme uz dažādām ieinteresētajām personām un nozarēm. Komisija ir apņēmības pilna panākt, ka ES tiek sekmīgi īstenots jaunais datu aizsardzības režīms, un atbalstīt visus tā darbības pilnīgas uzsākšanas aspektus. Šajā paziņojumā Komisija izvērtē līdz šim sasniegtos rezultātus attiecībā uz datu aizsardzības noteikumu konsekventu īstenošanu visā ES, jaunās pārvaldības sistēmas darbību, ietekmi uz iedzīvotājiem un uzņēmumiem, kā arī ES centieniem veicināt datu aizsardzības režīmu konverģenci pasaulē. Tas seko Komisijas 2018. gada janvāra paziņojumam par Regulas piemērošanu[[5]](#footnote-6), un tajā ir izmantots daudzpusējās ieinteresēto personu grupas[[6]](#footnote-7) paveiktais, jo īpaši tās ieguldījums gada novērtējumā, un Komisijas 2019. gada 13. jūnijā organizētajā novērtēšanas pasākumā notikušās apspriedes[[7]](#footnote-8). Šis paziņojums ir arī ieguldījums pārskatīšanā, kuru Komisija plāno veikt līdz 2020. gada maijam[[8]](#footnote-9).

ES datu aizsardzības tiesiskais regulējums ir Eiropas uz cilvēku vērstās pieejas inovācijai stūrakmens. Tas kļūst par daļu no pamata regulējuma arvien lielākam politikas jomu lokam, ieskaitot veselības aprūpi un pētniecību, mākslīgo intelektu, transportu, enerģētiku, konkurenci un tiesībaizsardzību. Komisija ir konsekventi uzsvērusi, cik svarīgi ir pienācīgi īstenot un piemērot jaunos datu aizsardzības noteikumus, kā norādīts tās 2018. gada janvārī publicētajā paziņojumā par Regulas piemērošanu un 2018. gada septembrī publicētajās vadlīnijās par personas datu izmantošanu vēlēšanu kontekstā[[9]](#footnote-10). Šā paziņojuma publicēšanas brīdī minētā mērķa sasniegšanā ir panākts ievērojams progress, tomēr neapšaubāmi ir jāturpina strādāt, lai Regula sāktu pilnībā darboties.

# Viens kontinents, viens likums: dalībvalstīs ir ieviests datu aizsardzības regulējums

Viens no svarīgākajiem Regulas mērķiem bija likvidēt sadrumstaloto sistēmu, ko veidoja 28 dažādi valstu tiesību akti, kuri bija spēkā saskaņā ar iepriekšējo Datu aizsardzības direktīvu[[10]](#footnote-11), un nodrošināt juridisko noteiktību privātpersonām un uzņēmumiem visā ES. Šis mērķis lielā mērā ir ticis sasniegts.

*Tiesiskā regulējuma saskaņošana*

Lai gan Regula dalībvalstīs ir tieši piemērojama, ar to tām tika noteikts pienākums veikt vairākus juridiskus pasākumus valstu līmenī — izveidot un pilnvarot valsts datu aizsardzības iestādes[[11]](#footnote-12), pieņemt noteikumus attiecībā uz konkrētiem jautājumiem, piemēram, personas datu aizsardzības saskaņošanu ar vārda un informācijas brīvību, kā arī grozīt vai atcelt nozaru tiesību aktus, kuros ir datu aizsardzības aspekti. Šā paziņojuma sagatavošanas laikā visas dalībvalstis, izņemot trīs[[12]](#footnote-13), bija atjauninājušas datu aizsardzības valsts tiesību aktus. Valstu līmenī joprojām turpinās nozaru tiesību aktu pielāgošanas darbs. Pēc Regulas iekļaušanas Līgumā par Eiropas Ekonomikas zonu tās piemērošana tika attiecināta arī uz Norvēģiju, Islandi un Lihtenšteinu, kuras arī ir pieņēmušas savus valsts līmeņa datu aizsardzības tiesību aktus.

Tomēr ieinteresētās personas aicina dažās jomās panākt vēl lielāku saskaņošanu[[13]](#footnote-14). Regulas ļauj dalībvalstīm zināmā mērā sīkāk noteikt Regulas piemērošanu konkrētās jomās, piemēram, attiecībā uz vecumu, no kura bērni var piekrist tiešsaistes pakalpojumiem[[14]](#footnote-15), vai personas datu apstrādi medicīnas, sabiedrības veselības un līdzīgās jomās. Šajā gadījumā dalībvalstu rīcību ierobežo divi elementi:

1. valsts konkretizējošajiem tiesību aktiem ir jāatbilst Pamattiesību hartas prasībām[[15]](#footnote-16) (nepārsniedzot Regulā, kas ir balstīta uz hartu, noteiktos ierobežojumus);
2. tie nedrīkst kavēt personas datu brīvu apriti ES[[16]](#footnote-17).

Dažos gadījumos dalībvalstis papildus Regulai ir ieviesušas valstu prasības, jo īpaši pieņēmušas daudzus nozaru tiesību aktus, kas noved pie sadrumstalotības un rada nevajadzīgus šķēršļus. Viens no gadījumiem, kad dalībvalstis līdztekus Regulai ir ieviesušas papildu prasības, ir Vācijas tiesību aktos paredzētais pienākums uzņēmumiem, kuros ir 20 vai vairāk darbinieku un kuri ir pastāvīgi iesaistīti automatizētā personas datu apstrādē, iecelt datu aizsardzības speciālistu.

*Centienu turpināšana virzienā uz lielāku saskaņošanu*

Komisija iesaistās divpusējos dialogos ar valstu iestādēm, īpašu uzmanību pievēršot valstu pasākumiem, kas ir saistīti ar:

* datu aizsardzības iestāžu faktisko neatkarību, tostarp pienācīgu finanšu resursu, cilvēkresursu un tehnisko resursu nodrošināšanu,
* valstu tiesību aktu ierobežojumiem attiecībā uz datu subjektu tiesībām,
* faktu, ka valsts tiesību aktos nedrīkst ieviest prasības, kas pārsniedz Regulā noteiktās, ja nav paredzēta rīcības brīvība konkretizēšanai, piemēram, papildu apstrādes nosacījumus,
* pienākumu saskaņot tiesības uz personas datu aizsardzību ar vārda un informācijas brīvību, ņemot vērā, ka šo pienākumu nedrīkst izmantot ļaunprātīgi, lai bremzētu žurnālistu darbu.

Jauno noteikumu konsekventu piemērošanu būtiski sekmē datu aizsardzības iestāžu darbs, tām sadarbojoties Eiropas Datu aizsardzības kolēģijā (turpmāk “kolēģija”): izpildes darbības, kas skar vairākas dalībvalstis, iziet kolēģijas sadarbības un konsekvences mehānismu[[17]](#footnote-18), savukārt kolēģijas pieņemtās pamatnostādnes palīdz vienoti izprast Regulu. Tomēr ieinteresētās personas sagaida, lai datu aizsardzības iestādes šajā virzienā ietu tālāk.

Datu aizsardzības noteikumu konsekventu interpretāciju palīdz nodrošināt arī valstu tiesu un Eiropas Savienības Tiesas darbs. Valstu tiesas nesen ir pieņēmušas spriedumus, ar kuriem atceļ valstu tiesību normas, kas neatbilst Regulai[[18]](#footnote-19).

# Visi jaunās pārvaldības sistēmas elementi nostājas savās vietās

Ar Regulu tika izveidota jauna pārvaldības struktūra, tās centrā izvirzot neatkarīgas valstu datu aizsardzības iestādes kā Regulas piemērotājas un ieinteresēto personu pirmos kontaktpunktus. Lai gan vairums datu aizsardzības iestāžu pagājušajā gadā ir saņēmušas lielākus resursus, dalībvalstu vidū joprojām pastāv lielas atšķirības[[19]](#footnote-20).

### Datu aizsardzības iestādes izmanto jaunās pilnvaras

Ar Regulu datu aizsardzības iestādēm piešķirtas plašākas pilnvaras izpildes panākšanas jomā. Pretēji bažām, ko dažas ieinteresētās personas pauda pirms 2018. gada maija, valstu datu aizsardzības iestādes saistībā ar izpildes panākšanas pilnvarām ir izvēlējušās līdzsvarotu pieeju. Tās ir vairāk orientējušās uz dialogu nekā sankcijām, jo īpaši attiecībā uz mazākiem uzņēmumiem, kuru pamatdarbība nav personas datu apstrāde. Vienlaikus tās nav vairījušās reāli izmantot savas jaunās pilnvaras, kad tas ir bijis nepieciešams, tostarp ierosinot izmeklēšanas sociālo plašsaziņas līdzekļu jomā[[20]](#footnote-21) un piemērojot administratīvus naudas sodus, kuru apmērs bijis no dažiem tūkstošiem līdz vairākiem miljoniem euro atkarībā no datu aizsardzības noteikumu pārkāpumu smaguma.

Datu aizsardzības iestāžu piemēroto naudas sodu piemēri[[21]](#footnote-22):

* naudas sods 5000 EUR apmērā sporta derību kafejnīcai Austrijā par nelikumīgu videonovērošanu,
* naudas sods 220 000 EUR apmērā datu brokeru uzņēmumam Polijā par personu neinformēšanu, ka to dati tiek apstrādāti,
* naudas sods 250 000 EUR apmērā Spānijas futbola līgai *LaLiga* par pārredzamības trūkumu tās viedtālruņa lietotnes dizainā,
* naudas sods 50 miljonu EUR apmērā uzņēmumam *Google* Francijā par nosacījumiem, kādos tika saņemta lietotāju piekrišana.

Ir svarīgi, lai, veicot izmeklēšanu, datu aizsardzības iestādes ievāktu attiecīgus pierādījumus, ievērotu visus valsts tiesību aktos paredzētos procesuālos pasākumus un nodrošinātu pienācīgu procesu bieži vien sarežģītās lietās. Tas prasa laiku un būtisku darba apjomu, tādēļ lielākā daļa izmeklēšanu, kas sāktas pēc tam, kad sākta Regulas piemērošana, joprojām nav pabeigtas.

Tomēr Regulas panākumi nebūtu jāvērtē pēc piemēroto naudas sodu skaita, bet gan pēc visu iesaistīto personu kultūras un uzvedības izmaiņām. Šajā saistībā datu aizsardzības iestāžu rīcībā ir citi instrumenti, piemēram, pagaidu vai galīgu apstrādes ierobežojumu, tostarp aizliegumu, uzlikšana vai rīkojums apturēt datu plūsmu pie saņēmēja trešā valstī[[22]](#footnote-23).

Dažas datu aizsardzības iestādes ir izveidojušas jaunus instrumentus, piemēram, palīdzības līnijas un rīku kopumus uzņēmumiem, savukārt citas ir izstrādājušas novatorisku pieeju, piemēram, regulējuma izmēģināšanas vidi[[23]](#footnote-24), lai palīdzētu uzņēmumiem, kas cenšas nodrošināt atbilstību. Tomēr vairākas ieinteresētās personas, jo īpaši dažu dalībvalstu mazie un vidējie uzņēmumi, joprojām uzskata, ka nav saņēmušas pietiekamu atbalstu un informāciju[[24]](#footnote-25). Lai palīdzētu atrisināt šo situāciju, Komisija datu aizsardzības iestādēm piešķir dotācijas ieinteresēto personu, jo īpaši privātpersonu un mazo un vidējo uzņēmumu, uzrunāšanai[[25]](#footnote-26).

### Eiropas Datu aizsardzības kolēģija ir sākusi darbu

Datu aizsardzības iestādes aktīvāk līdzdarbojas Eiropas Datu aizsardzības kolēģijā[[26]](#footnote-27). Šis intensīvais darbs ir ļāvis kolēģijai pieņemt aptuveni 20 pamatnostādnes par svarīgākajiem Regulas aspektiem[[27]](#footnote-28). Kolēģijas darba turpmākās jomas ir izklāstītas divu gadu programmā[[28]](#footnote-29) atbilstīgi Regulā paredzētajam.

Pārrobežu lietās katra datu aizsardzības iestāde vairs nav tikai valsts iestāde, bet veido daļu no ES mēroga procesa visos tā posmos — no izmeklēšanas līdz lēmuma pieņemšanai. Šāda cieša sadarbība ir kļuvusi par normu: līdz 2019. gada jūnija beigām sadarbības mehānisma ietvaros bija pārvaldītas 516 pārrobežu lietas.

Komisija aktīvi piedalās kolēģijas darbā[[29]](#footnote-30), ar ko tiek veicināta Regulas burta un gara ievērošana, un atgādina ES tiesību pamatprincipus[[30]](#footnote-31).

*Ceļā uz ES datu aizsardzības kultūras izveidošanu*

Jaunajai pārvaldības sistēmai vēl ir jāsasniedz tās pilnīgais potenciāls. Ir svarīgi, lai kolēģija vēl vairāk racionalizētu lēmumu pieņemšanu un attīstītu vienotu ES datu aizsardzības kultūru tās dalībnieku vidū. Datu aizsardzības iestāžu iespējas kopīgi rīkoties[[31]](#footnote-32) jautājumos, kas skar vairāk nekā vienu dalībvalsti, piemēram, veikt kopīgus izmeklēšanas un izpildes pasākumus, var sniegt ieguldījumu šāda mērķa sasniegšanā, vienlaikus mazinot resursu radītos ierobežojumus.

Daudzas ieinteresētās personas vēlas, lai valstu datu aizsardzības iestādes sadarbotos vēl plašāk un ievērotu vienotu pieeju[[32]](#footnote-33). Tās arī aicina datu aizsardzības iestādes sniegt konsekventākus padomus[[33]](#footnote-34) un pilnībā saskaņot valstu pamatnostādnes ar kolēģijas pieņemtajām. Dažas no tām arī sagaida sīkākus skaidrojumus tādiem nozīmīgiem Regulas jēdzieniem kā, piemēram, uz risku balstīta pieeja, īpaši ņemot vērā mazo un vidējo uzņēmumu bažas.

Šajā saistībā ir ļoti svarīgi ļaut ieinteresētajām personām vairāk ietekmēt kolēģijas darbu. Šā iemesla dēļ Komisija atzinīgi vērtē sistemātiskās pamatnostādņu sabiedriskās apspriešanas, ko organizē kolēģija. Šī prakse, kā arī darbsemināru organizēšana ieinteresētajām personām par mērķtiecīgi izvēlētiem tematiem sākotnējo pārdomu posmā būtu jāturpina un jāpaplašina, lai nodrošinātu, ka kolēģijas darbs ir pārredzams, iekļaujošs un nozīmīgs.

# Cilvēki izmanto savas tiesības, taču jāturpina uzlabot informētību

Cits svarīgs Regulas mērķis bija personu tiesību nostiprināšana. Daudzas pilsonisko tiesību apvienības un patērētāju organizācijas uzskata Regulu par svarīgu ieguldījumu uz savstarpēju uzticēšanos balstītas taisnīgas digitālās sabiedrības veidošanā.

*Labāka datu aizsardzības tiesību apzināšanās*

Privātpersonas ES arvien labāk izprot datu aizsardzības noteikumus un apzinās savas tiesības: 67 % respondentu 2019. gada maija Eirobarometra aptaujā[[34]](#footnote-35) norādīja, ka ir informēti par Regulu, savukārt 57 % zina, ka pastāv valsts datu aizsardzības iestāde, kurā tie var vērsties, lai saņemtu informāciju vai iesniegtu sūdzības. 73 % respondentu atbildēja, ka ir dzirdējuši par vismaz kādu no tiesībām, ko piešķir Regula. Tomēr daudzas ES privātpersonas, piekļūstot internetam, joprojām neveic aktīvus pasākumus savu personas datu aizsardzībai. Piemēram, 44 % privātpersonu sociālajos tīklos nav nomainījušas noklusētos privātuma iestatījumus.

*Cilvēki arvien biežāk izmanto savas tiesības*

Arvien pieaugošā tiesību apzināšanās ir likusi privātpersonām aktīvāk tās izmantot, uzdodot jautājumus kā klientiem un biežāk vēršoties datu aizsardzības iestādēs, lai saņemtu informāciju vai iesniegtu sūdzības[[35]](#footnote-36). Arī uzņēmumi ziņo, ka vairākās nozarēs, piemēram, banku un telesakaru nozarē, ir palielinājies pieprasījumu skaits attiecībā uz piekļuvi personas datiem. Personas arī biežāk ir atsaukušas piekrišanu un izmantojušas tiesības iebilst pret komercpaziņojumiem[[36]](#footnote-37).

Tomēr daži uzņēmumi ziņoja, ka privātpersonas ir pārpratušas datu aizsardzības noteikumus, piemēram, uzskatot, ka personai jāpiekrīt ikvienai datu apstrādei vai ka tiesības uz dzēšanu ir absolūtas (lai gan uzņēmumiem personas dati dažkārt jāglabā, piemēram, juridisku pienākumu dēļ)[[37]](#footnote-38). Pilsoniskās sabiedrības organizācijas savukārt sūdzas par dažu uzņēmumu un datu aizsardzības iestāžu ilgo kavēšanos sniegt atbildes.

Svarīgi atzīmēt, ka nevalstiskas organizācijas ierosināja vairākas pārstāvības prasības pēc fizisku personu pilnvarojuma, izmantojot jauno Regulā paredzēto iespēju[[38]](#footnote-39). Pārstāvības prasību izmantošana būtu bijusi vieglāka, ja vairāk dalībvalstu būtu izmantojušas Regulā noteikto iespēju ļaut nevalstiskām organizācijām ierosināt prasības bez pilnvarojuma[[39]](#footnote-40).

*Jāturpina informētības uzlabošanas centieni*

Ņemot vērā iepriekš minēto, valstu un ES līmenī ir jāturpina uz plašāku sabiedrību vērsts dialogs un informētības uzlabošanas centieni. Šajā nolūkā Komisija 2019. gada jūlijā sāka jaunu tiešsaistes kampaņu[[40]](#footnote-41), kurā privātpersonas tiek mudinātas lasīt paziņojumus par privātumu un pielāgot privātuma iestatījumus.

# Uzņēmumi pielāgo savu praksi

Regulas mērķis ir atbalstīt darījumdarbību digitālajā ekonomikā, piedāvājot nākotnes prasībām atbilstošus risinājumus. Uzņēmumi lielākoties atzinīgi vērtē Regulā lietoto pārskatatbildības principu, kas atkāpjas no agrākās apgrūtinošās *ex ante* pieejas (paziņošanas prasību atcelšana, pienākumu mērogošana, principa “datu aizsardzība integrēti un pēc noklusējuma” elastīgums, kas ļauj konkurēt privātumu aizsargājošu risinājumu ziņā). Vienlaikus daži no tiem aicina datu aizsardzības iestādes paaugstināt juridisko noteiktību un sniegt papildu vai skaidrākus norādījumus[[41]](#footnote-42).

### Pareiza datu pārvaldība

Lai gan uzņēmumi ziņo par vairākām problēmām, kas radušās, pielāgojoties jaunajiem noteikumiem[[42]](#footnote-43), daudzi no tiem uzsver, ka šie noteikumi arī snieguši iespēju pievērst datu aizsardzības jautājumiem uzņēmuma valdes uzmanību, sakārtot situāciju ar glabātajiem datiem, uzlabot drošību, būt gatavākiem starpgadījumiem, mazināt nevajadzīgu risku un veidot ar klientiem un darījumu partneriem attiecības, kurās ir vairāk uzticēšanās. Attiecībā uz pārredzamību uzņēmējdarbības un pilsoniskās sabiedrības organizācijas min smalko līdzsvaru, kas jāpanāk starp visas Regulā noteiktās informācijas sniegšanu privātpersonām un skaidras, vienkāršas valodas, kā arī privātpersonām saprotamas formas lietošanu. Uzņēmumi izstrādā novatoriskus risinājumus, lai to panāktu.

Kopumā uzņēmumi norādīja, ka tiem ir izdevies ieviest jaunās datu subjektu tiesības, lai gan lielāka pieprasījumu skaita un to lielākas daudzveidības dēļ[[43]](#footnote-44) dažkārt bijis grūti ievērot termiņus, turklāt bijušas arī grūtības sakarā ar pieprasījumu iesniedzēju identitātes pārbaudi.

### Ietekme uz inovāciju

Regula ne tikai atļauj, bet arī mudina izstrādāt jaunas tehnoloģijas, vienlaikus ievērojot pamattiesības uz personas datu aizsardzību. Tas tā ir, piemēram, mākslīgā intelekta jomā.

Uzņēmumi ir sākuši izstrādāt un piedāvāt jaunus pakalpojumus, kas vairāk aizsargā privātumu. Piemēram, dažās dalībvalstīs arvien lielāku tirgus daļu iekaro meklētājprogrammas, kuras neizseko lietotājus un neizmanto uz uzvedību balstītu reklāmu. Citi uzņēmumi izstrādā pakalpojumus, kas balstās uz jaunajām privātpersonu tiesībām, piemēram, personas datu pārnesamību. Arvien vairāk uzņēmumu, lai atšķirtos no konkurentiem un sevi reklamētu, atsaucas uz personas datu aizsardzību. Šī notikumu attīstība nav vērojama tikai ES, bet arī tādu ārvalstu ekonomikā, kam raksturīgs liels novatoriskums[[44]](#footnote-45).

### “Zema riska” mikrouzņēmumu un mazo uzņēmumu īpašā situācija

Lai gan situācija dalībvalstīs atšķiras, mikrouzņēmumi un mazie uzņēmumi[[45]](#footnote-46), kuru pamatdarbība nav personas datu apstrāde, ir bijuši starp ieinteresētajām personām, kas uzdevušas visvairāk jautājumu par Regulas piemērošanu. Lai gan daļa jautājumu, šķiet, ir radušies datu aizsardzības noteikumu nepārzināšanas dēļ, šo uzņēmumu bažas dažkārt arī pastiprina konsultāciju dienestu kampaņas ar mērķi sniegt maksas konsultāciju pakalpojumus, kā arī nepareizas informācijas izplatīšanās, piemēram, par nepieciešamību sistemātiski saņemt fizisku personu piekrišanu[[46]](#footnote-47), un valsts līmenī noteiktas papildu prasības.

Šajā ziņā mikrouzņēmumi un mazie uzņēmumi vēlas pamatnostādnes, kas būtu pielāgotas to īpašajai situācijai un sniegtu ļoti praktisku informāciju. Dažas datu aizsardzības iestādes valsts līmenī jau ir sagatavojušas šādas pamatnostādnes[[47]](#footnote-48). Papildinot valstu iniciatīvas, Komisija ir publicējusi informatīvu materiālu, lai palīdzētu šādiem uzņēmumiem ievērot jaunos noteikumus, veicot virkni praktisku pasākumu[[48]](#footnote-49).

### Regulā paredzēto instrumentu kopuma izmantošana

Regula paredz instrumentus, ar ko var pierādīt atbilstību, piemēram, līguma standartklauzulas, rīcības kodeksus un jaunieviestos sertifikācijas mehānismus.

Līguma standartklauzulas ir paraugklauzulas, ko var brīvprātīgi iekļaut līgumā, piemēram, starp datu pārzini un datu apstrādātāju, un kas paredz līgumslēdzēju pušu pienākumus atbilstīgi Regulai. Regula paplašina līguma standartklauzulu izmantošanas iespējas datu nosūtīšanai gan starptautiski, gan ES iekšienē[[49]](#footnote-50). Starptautiskās nosūtīšanas jomā to plašā izmantošana rāda[[50]](#footnote-51), ka tās ļoti palīdz uzņēmumiem nodrošināt atbilstību un īpaši noder uzņēmumiem, kam nav resursu, lai vestu individuālas sarunas par līgumiem ar katru datu apstrādes jomas līgumslēdzēju.

Vairāku nozaru pārstāvji arī uzskata, ka līguma standartklauzulu pieņemšana ir lietderīgs saskaņotības sekmēšanas veids, jo īpaši tad, ja tās pieņem Komisija. Komisija sadarbosies ar ieinteresētajām personām, lai izmantotu Regulas sniegtās iespējas un atjauninātu esošās klauzulas.

Rīcības kodeksu ievērošana ir vēl viens funkcionējošs, praktisks instruments, ko nozare var izmantot, lai vieglāk pierādītu atbilstību Regulas prasībām[[51]](#footnote-52). Šādi kodeksi ir jāizstrādā arodasociācijām vai struktūrām, kas pārstāv pārziņu un apstrādātāju kategorijas, un tajos jāapraksta, kā konkrētā nozarē var īstenot datu aizsardzības noteikumus. Ja kodeksos nosaka pienākumus, kas atšķiras atkarībā no riska[[52]](#footnote-53), tie var izrādīties arī ļoti noderīgs un izmaksu ziņā efektīvs veids, kā maziem un vidējiem uzņēmumiem izpildīt tiem uzliktos pienākumus.

Visbeidzot, arī sertifikācija var būt noderīgs instruments, ar kuru apliecināt atbilstību konkrētām Regulas prasībām. Tā var paaugstināt juridisko noteiktību uzņēmumiem un popularizēt Regulu pasaulē. Eiropas Datu aizsardzības kolēģijas nesen pieņemtās sertifikācijas un akreditācijas pamatnostādnes[[53]](#footnote-54) ļaus Savienībā veidot sertifikācijas shēmas. Komisija sekos līdzi šīm norisēm un, ja tas būs nepieciešams, izmantos Regulā paredzētās pilnvaras noteikt sertifikācijas prasību satvaru. Komisija var arī vērsties pie ES standartizācijas struktūrām ar lūgumu standartizēt Regulai svarīgus elementus.

# Starptautiskā līmenī attīstās augšupēja konverģence

Pieprasījums pēc personas datu aizsardzības pastāv ne tikai ES. Kā liecina nesena pasaules mēroga aptauja par drošību internetā, visā pasaulē pieaug neuzticēšanās, un tas liek cilvēkiem mainīt savu izturēšanos tiešsaistē[[54]](#footnote-55). Arvien vairāk uzņēmumu uz šīm bažām reaģē, ar Regulu izveidotās tiesības pēc savas iniciatīvas attiecinot arī uz klientiem, kas atrodas ārpus ES.

Turklāt, valstīm visā pasaulē arvien biežāk risinot līdzīgas problēmas, tās ievieš jaunus datu aizsardzības noteikumus vai modernizē esošos. Šiem tiesību aktiem bieži ir kopīgas iezīmes, kādas ir arī ES datu aizsardzības režīmam, piemēram, visaptveroši tiesību akti nozaru noteikumu vietā, piemērojamas individuālās tiesības un neatkarīga uzraudzības iestāde. Šī tendence ir patiesi globāla — tā vērojama no Dienvidkorejas līdz Brazīlijai, no Čīles līdz Taizemei, no Indijas līdz Indonēzijai. Vēl viena skaidra pazīme, ka pastāv šādas augšupējas konverģences tendence, ir arvien plašākā dalība Eiropas Padomes 108. konvencijā[[55]](#footnote-56), kas nesen modernizēta[[56]](#footnote-57) ar būtisku Komisijas ieguldījumu.

*Drošu un brīvu datu plūsmu veicināšana ar lēmumiem par aizsardzības līmeņa pietiekamību u. c.*

Šī jaunā konverģence sniedz jaunas iespējas atvieglot datu plūsmas un līdz ar to tirdzniecību, kā arī publiskā sektora iestāžu sadarbību, vienlaikus uzlabojot ES fizisku personu datu aizsardzību, kad šie dati tiek nosūtīti uz ārvalstīm.

Īstenojot 2017. gada paziņojumā “Apmaiņa ar personas datiem un šo datu aizsardzība globalizētā pasaulē”[[57]](#footnote-58) izklāstīto stratēģiju, Komisija pastiprināja sadarbību ar trešām valstīm un citiem starptautiskajiem partneriem, balstoties uz privātuma sistēmu konverģences elementiem un turpinot tos attīstīt. Cita starpā tika izvērtēta iespēja pieņemt pietiekamas aizsardzības atzinumus attiecībā uz konkrētām trešām valstīm[[58]](#footnote-59). Šis darbs ir devis svarīgus rezultātus, jo īpaši 2019. gada februārī spēkā stājušos ES un Japānas abpusējas aizsardzības līmeņa pietiekamības pasākumu, ar ko izveidota pasaulē lielākā brīvas un drošas datu aprites telpa. Sarunas par pietiekamību ar Dienvidkoreju ir krietni pavirzījušās uz priekšu, un tiek veikts izpētes darbs ar mērķi uzsākt sarunas par pietiekamību ar vairākām Latīņamerikas valstīm, piemēram, Čīli vai Brazīliju, atkarībā no notiekošo likumdošanas procesu pabeigšanas. Arī dažviet Āzijā, piemēram, Indijā, Indonēzijā un Taivānā, kā arī Eiropas austrumu un dienvidu kaimiņreģionos notikumi attīstās daudzsološi, un tas varētu pavērt durvis turpmākiem lēmumiem par aizsardzības līmeņa pietiekamību.

Vienlaikus Komisija atzinīgi vērtē faktu, ka citas valstis, kas ir ieviesušas Regulā paredzētajai aizsardzības līmeņa pietiekamībai līdzvērtīgus nosūtīšanas instrumentus, ir atzinušas, ka ES un valstis, kuru garantēto aizsardzību ES ir atzinusi par pietiekamu, nodrošina nepieciešamo aizsardzības līmeni[[59]](#footnote-60). Tādējādi potenciāli varētu veidoties valstu tīkls, kurā dati var plūst brīvi.

Līdztekus tam notiek intensīvs darbs ar citām trešām valstīm, piemēram, Kanādu, Jaunzēlandi, Argentīnu un Izraēlu, lai atbilstīgi Regulai nodrošinātu pēctecību attiecībā uz tiem lēmumiem par aizsardzības līmeņa pietiekamību, kas pieņemti uz 1995. gada Datu aizsardzības direktīvas pamata. Tikmēr ir pierādījies, ka ES un ASV privātuma vairogs ir noderīgs instruments transatlantisko datu plūsmu nodrošināšanai ar augstu aizsardzības līmeni; tajā piedalās vairāk nekā 4700 uzņēmumu[[60]](#footnote-61). Tā ikgadējā pārskatīšana nodrošina, ka regulējuma pareiza darbība tiek regulāri pārbaudīta un jaunas problēmas var tikt savlaicīgi risinātas.

Tā kā attiecībā uz datu plūsmām nav universāli izmantojamu risinājumu, Komisija kopā ar ieinteresētajām personām un kolēģiju arī strādā, lai Regulā paredzēto starptautiskās nosūtīšanas instrumentu kopuma potenciāls tiktu izmantots pilnībā. Tas attiecas uz tādiem instrumentiem kā līguma standartklauzulas, sertifikācijas shēmu veidošana, rīcības kodeksi vai administratīvi pasākumi publiskām struktūrām. Šajā saistībā Komisija ir ieinteresēta pieredzes un paraugprakses apmaiņā ar citu sistēmu veidotājiem, kas varētu būt ieguvuši konkrētu pieredzi saistībā ar dažiem no šiem instrumentiem. Komisija apsvērs iespēju izmantot Regulā paredzētās pilnvaras attiecībā uz šiem nosūtīšanas instrumentiem, jo īpaši līguma standartklauzulām.

Laikā, kad datu plūsmas kļūst par arvien svarīgāku tirdzniecības, sakaru un sociālo kontaktu sastāvdaļu, papildus tīri divpusējiem instrumentiem varētu būt vērts pētīt, vai līdzīgi domājošas valstis varētu šajā jomā izveidot daudznacionālu regulējumu. Šāds instruments nodrošinātu datu brīvu apriti starp līgumslēdzējām pusēm, vienlaikus nodrošinot nepieciešamo aizsardzības līmeni uz kopīgu vērtību un saskaņotu sistēmu pamata. To varētu izstrādāt, piemēram, balstoties uz modernizēto 108. konvenciju vai iedvesmojoties no Japānas šā gada sākumā uzsāktās iniciatīvas “brīvas datu plūsmas uzticoties”.

*Jaunu sinerģiju veidošana tirdzniecības un datu aizsardzības instrumentu starpā*

Vienlaikus ar datu aizsardzības standartu konverģences veicināšanu starptautiskā līmenī Komisija ir arī apņēmusies cīnīties ar digitālo protekcionismu. Šim nolūkam tā ir izstrādājusi īpašus tirdzniecības nolīgumu noteikumus par datu plūsmām un datu aizsardzību, kurus tā sistemātiski iekļauj divpusējo un daudzpusējo sarunu, piemēram, pašreizējo PTO sarunu par e-komerciju, darba kārtībā. Šie horizontālie noteikumi izslēdz tīri protekcionistisku pasākumu, tostarp datu teritoriālas ierobežošanas piespiedu prasību, piemērošanu, vienlaikus saglabājot pušu regulatīvo autonomiju aizsargāt pamattiesības uz datu aizsardzību.

Lai gan dialogiem par datu aizsardzību un tirdzniecības sarunām ir jānotiek nošķirti, tie var viens otru papildināt: labākais šādas sinerģijas piemērs ir ES un Japānas abpusējas aizsardzības līmeņa pietiekamības pasākums, kas papildus atvieglo tirdzniecību un tādējādi pastiprina ieguvumus no ekonomisko partnerattiecību nolīguma. Principā šāda konverģence, kas balstās uz kopīgām vērtībām un augstiem standartiem un ko papildina efektīva izpildes nodrošināšana, ir visstingrākais personas datu apmaiņas pamats, un to arvien vairāk atzīst mūsu starptautiskie partneri[[61]](#footnote-62). Tā kā uzņēmumi arvien vairāk darbojas pāri robežām un vēlas piemērot līdzīgus noteikumus darījumdarbībā visā pasaulē, šāda konverģence palīdz veidot tiešajiem ieguldījumiem labvēlīgu vidi, kas atvieglo tirdzniecību un uzlabo uzticēšanos darījumu partneru starpā.

### Informācijas apmaiņas veicināšana cīņai pret noziedzību un terorismu, balstoties uz pienācīgiem aizsardzības pasākumiem

Datu aizsardzības režīmu lielāka savstarpējā saderība var arī būtiski atvieglot tik nepieciešamo informācijas apmaiņu ES un ārvalstu regulatīvo, policijas un tiesu iestāžu starpā, tādējādi veicinot efektīvāku un ātrāku sadarbību tiesībaizsardzības jomā[[62]](#footnote-63). Šim mērķim Komisija apsver izmantot iespēju pieņemt lēmumus par aizsardzības līmeņa pietiekamību saskaņā ar datu aizsardzības jomas Tiesībaizsardzības direktīvu, lai padziļinātu sadarbību ar svarīgākajiem partneriem cīņā pret noziedzību un terorismu. Turklāt ES un ASV “jumta nolīgums”[[63]](#footnote-64), kas stājās spēkā 2017. gada februārī, var tikt izmantots kā paraugs līdzīgiem nolīgumiem ar citiem svarīgiem drošības partneriem.

To, ka augstiem datu aizsardzības standartiem ir liela nozīme, jo tie ir pamats stabilai tiesībaizsardzības sadarbībai ar trešām valstīm, apliecina arī, piemēram, pasažieru datu reģistra (PDR) datu nosūtīšana[[64]](#footnote-65) un operatīvās informācijas apmaiņa starp Eiropolu un svarīgiem starptautiskajiem partneriem. Šajā sakarā pašlaik notiek vai tūdaļ sāksies sarunas par starptautisku nolīgumu noslēgšanu ar vairākām dienvidu kaimiņreģiona valstīm[[65]](#footnote-66).

Stingri datu aizsardzības pasākumi būs arī jebkuras turpmākas vienošanās par pārrobežu piekļuvi elektroniskiem pierādījumiem kriminālprocesā svarīga daļa gan divpusējā (ES un ASV nolīgums), gan daudzpusējā līmenī (Eiropas Padomes Budapeštas konvencijas par kibernoziegumiem otrais papildu protokols)[[66]](#footnote-67).

*Datu aizsardzības īstenotāju sadarbības veicināšana*

Laikā, kad problēmas ar privātuma ievērošanu vai informācijas drošības incidenti var vienlaikus ietekmēt daudzus cilvēkus dažādās jurisdikcijās, uzraudzības iestāžu ciešāka sadarbība starptautiskā līmenī var palīdzēt nodrošināt gan privātpersonu tiesību efektīvāku aizsardzību, gan stabilāku vidi uzņēmumiem. Ņemot vērā šo situāciju un cieši sadarbojoties ar kolēģiju, Komisija pētīs veidus, kā atvieglot ES un ārvalstu uzraudzības iestāžu sadarbību izpildes panākšanas jomā un savstarpēju palīdzību, tostarp izmantojot jaunās pilnvaras, ko šajā ziņā paredz Regula[[67]](#footnote-68). Minētais varētu aptvert dažādas sadarbības formas — no kopīgu interpretējošu vai praktisku instrumentu izstrādes[[68]](#footnote-69) līdz informācijas apmaiņai par notiekošajām izmeklēšanām.

Visbeidzot, Komisija arī plāno aktivizēt dialogu ar reģionālajām organizācijām un tīkliem, piemēram, Dienvidaustrumāzijas valstu asociāciju (*ASEAN*), Āfrikas Savienību, Āzijas un Klusā okeāna valstu privātuma iestāžu forumu (*APPA*) vai Ibērijas pussalas un Amerikas datu aizsardzības tīklu, kam ir arvien lielāka nozīme vienotu datu aizsardzības standartu veidošanā, labākās prakses apmaiņas veicināšanā un piemērotāju sadarbības veicināšanā. Komisija arī sadarbosies ar Ekonomiskās sadarbības un attīstības organizāciju un Āzijas un Klusā okeāna valstu ekonomiskās sadarbības organizāciju, lai veidotu konverģenci, kas sekmē augstu datu aizsardzības līmeni.

# Datu aizsardzības regulējums kā daudzu politikas jomu neatņemama daļa

Personas datu aizsardzība ir garantēta un integrēta vairākās Savienības politikas jomās.

### Telesakari un elektronisko sakaru pakalpojumi

Komisija 2017. gada janvārī pieņēma Privātuma un elektronisko sakaru regulas priekšlikumu[[69]](#footnote-70). Priekšlikuma mērķis ir aizsargāt sakaru konfidencialitāti, kā paredzēts Pamattiesību hartā, kā arī aizsargāt personas datus, kas varētu būt daļa no saziņas, un galalietotāju galiekārtas.

Ierosinātā E-privātuma regula konkretizē un papildina Regulu, paredzot īpašus noteikumus minētajiem mērķiem. Tā modernizē esošos ES e-privātuma noteikumus[[70]](#footnote-71), lai atspoguļotu tehnisko un juridisko progresu. Tā uzlabo privātpersonu privātumu, paplašinot jauno noteikumu piemērošanas jomu, lai tie būtu attiecināmi arī uz “*over-the-top*” sakaru pakalpojumu sniedzējiem un tādējādi tiktu nodrošināti vienlīdzīgi konkurences apstākļi visiem elektronisko sakaru pakalpojumiem. Lai gan Eiropas Parlaments 2017. gada oktobrī apstiprināja pilnvaras trialogu sākšanai, Padome vēl nav vienojusies par kopējo pieeju. Komisija joprojām pilnībā atbalsta E-privātuma regulu un sniegs atbalstu likumdevējiem to centienos panākt ierosinātās regulas raitu pieņemšanu.

### Veselības aprūpe un pētniecība

Sabiedrības interešu dēļ veselības aprūpes datu, kas saskaņā ar Regulu ir sensitīvi dati, apmaiņas atvieglošanai dalībvalstu starpā ir arvien lielāka nozīme sabiedrības veselības jomā. Šo interešu vidū ir veselības aprūpes vai ārstēšanas nodrošināšana, aizsardzība pret nopietniem pārrobežu veselības apdraudējumiem, kā arī augstu veselības aprūpes, zāļu un medicīnisku ierīču kvalitātes un drošības standartu nodrošināšana. Regula paredz noteikumus, kas nodrošina veselības aprūpes datu likumīgu un uzticamu apstrādi un apmaiņu visā ES. Šie noteikumi attiecas arī uz trešo personu piekļuvi pacientu medicīniskajiem datiem, ieskaitot datus, kas glabājas pacientu kartēs, e-receptēs, kā arī — ilgtermiņā — visaptverošās elektroniskās pacienta medicīniskajās kartēs, un to izmantošanu zinātniskās pētniecības mērķiem. Klīnisko pārbaužu jomā Komisija ir arī sagatavojusi īpašu jautājumu un atbilžu dokumentu par Klīnisko pārbaužu regulas[[71]](#footnote-72) un Vispārīgās datu aizsardzības regulas mijiedarbību[[72]](#footnote-73).

### Mākslīgais intelekts (MI)

MI iegūstot stratēģisku nozīmi, ir svarīgi veidot globālus noteikumus par tā izstrādi un izmantošanu. Komisija ir izvēlējusies uz cilvēku orientētu pieeju MI izstrādes un izmantošanas veicināšanā — tas nozīmē, ka MI lietojumiem ir jāatbilst pamattiesībām[[73]](#footnote-74). Šajā kontekstā Regulas noteikumi paredz vispārēju satvaru un ietver konkrētus pienākumus un tiesības, kam ir īpaša nozīme attiecībā uz personas datu apstrādi ar MI. Piemēram, Regula ietver tiesības nebūt tāda lēmuma subjektam, kas pieņemts tikai automatizēti, izņemot atsevišķās situācijās[[74]](#footnote-75). Tā arī ietver īpašas pārredzamības prasības automatizētas lēmumu pieņemšanas izmantošanā, proti, pienākumu informēt par to, ka šādi lēmumi pastāv, sniegt jēgpilnu informāciju un paskaidrot tās nozīmi, kā arī apstrādes radītās paredzamās sekas privātpersonai[[75]](#footnote-76). Mākslīgā intelekta augsta līmeņa ekspertu grupa[[76]](#footnote-77), Ekonomiskās sadarbības un attīstības organizācija[[77]](#footnote-78) un G20 valstis[[78]](#footnote-79) ir atzinušas, ka Regulas pamatprincipi ir īpaši nozīmīgi ar MI saistīto problēmu risināšanā un iespēju izmantošanā. Eiropas Datu aizsardzības kolēģija ir noteikusi MI kā vienu no iespējamajiem tematiem 2019.–2020. gada darba programmā[[79]](#footnote-80).

### Transports

Tīklam pieslēgtu automobiļu un viedo pilsētu attīstība arvien vairāk balstās uz liela personas datu apjoma apstrādi un apmaiņu dažādu pušu starpā, t. sk. automobiļu, autoražotāju, telemātikas pakalpojumu sniedzēju, kā arī par ceļu infrastruktūru atbildīgo publiskā sektora iestāžu starpā. Šāda daudzpusēja vide nozīmē, ka personas datu apstrādē iesaistīto dažādo pušu funkciju un atbildības sadale un visu pušu veiktās apstrādes likumības nodrošināšana ir visai sarežģīta. Regulas un e-privātuma tiesību aktu ievērošana ir ļoti svarīga, lai intelektiskas transporta sistēmas sekmīgi ieviestu visiem transporta veidiem un lai izplatītos digitāli rīki un pakalpojumi, kas palielinātu iedzīvotāju un preču mobilitāti[[80]](#footnote-81).

### Enerģētika

Digitālo risinājumu izstrāde enerģētikas nozarē arvien vairāk balstās uz personas datu apstrādi. Tiesību akti, kas pieņemti kā daļa no tiesību aktu kopuma “Tīru enerģiju ikvienam Eiropā”[[81]](#footnote-82), ietver jaunus noteikumus, kuri ļaus digitalizēt elektroenerģijas nozari, un noteikumus par piekļuvi datiem, datu pārvaldību un sadarbspēju, tā ļaujot patērētāju datus apstrādāt reāllaikā, lai panāktu ietaupījumus, veicinātu pašražošanu un dalību enerģijas tirgū. Tādēļ šo noteikumu sekmīgai īstenošana ir ļoti svarīgi ievērot datu aizsardzības noteikumus.

### Konkurence

Personas datu aizsardzība arvien biežāk ir konkurences politikas jomā izvērtējams elements[[82]](#footnote-83). Tā kā datu aizsardzības iestādes ir vienīgās iestādes ar pilnvarām vērtēt datu aizsardzības noteikumu pārkāpumus, konkurences, patērētāju un datu aizsardzības iestādes sadarbojas un turpinās sadarboties, kad tas būs nepieciešams to attiecīgo kompetenču saskares gadījumos. Komisija veicinās šādu sadarbību un cieši sekos notikumu attīstībai.

### Vēlēšanu konteksts

Vadlīnijās par personas datu izmantošanu vēlēšanu kontekstā[[83]](#footnote-84), kas tika izdotas 2018. gada septembrī kā daļa no vēlēšanu tiesību aktu kopuma[[84]](#footnote-85), Komisija vērsa uzmanību uz noteikumiem, kas ir īpaši svarīgi vēlēšanās iesaistītajām personām, tostarp uz vēlētāju individualizētas uzrunāšanas problēmām. Šie norādījumi tika atkārtoti Eiropas Datu aizsardzības kolēģijas paziņojumā[[85]](#footnote-86), un vairākas datu aizsardzības iestādes izdeva norādījumus valsts līmenī. Vēlēšanu tiesību aktu kopumā bija arī ietverts aicinājums ikvienai dalībvalstij izveidot valsts vēlēšanu tīklu, iesaistot valsts iestādes, kam ir kompetence vēlēšanu jautājumos, un iestādes, kas atbild par tādu noteikumu pārraudzību un piemērošanu, kuri attiecas uz tiešsaistes darbībām, kam ir nozīme no vēlēšanu viedokļa, piemēram, datu aizsardzības noteikumu piemērošanu šajā jomā. Tika pieņemti arī jauni pasākumi, ar ko ieviesa Eiropas politiskajām partijām un nodibinājumiem piemērojamas sankcijas par datu aizsardzības noteikumu pārkāpumiem. Komisija ieteica dalībvalstīm īstenot tādu pašu pieeju valstu līmenī. Datu aizsardzības aspekti tiks aplūkoti arī 2019. gada Eiropas Parlamenta vēlēšanu izvērtējumā, kas tiks publicēts 2019. gada oktobrī.

### Tiesībaizsardzība

Efektīvu un īstu drošības savienību var izveidot, vienīgi pilnībā ievērojot ES hartā un sekundārajos ES tiesību aktos nostiprinātās pamattiesības, tostarp īstenojot pienācīgus datu aizsardzības pasākumus, lai tiesībaizsardzības vajadzībām būtu iespējams droši apmainīties ar personas datiem. Jebkuriem pamattiesību uz privāto dzīvi un datu aizsardzību ierobežojumiem piemēro stingru nepieciešamības un samērīguma pārbaudi.

# Nobeigums

Balstoties uz līdz šim pieejamo informāciju un dialogu ar ieinteresētajām personām, Komisijas sākotnējais vērtējums ir tāds, ka pirmais Regulas piemērošanas gads kopumā ir bijis sekmīgs. Tomēr, kā redzams šajā paziņojumā, vairākās jomās ir nepieciešams turpmāks progress.

*Tiesiskā regulējuma īstenošana un papildināšana*

* Trim dalībvalstīm, kuras vēl nav atjauninājušas savus datu aizsardzības valsts tiesību aktus, tas steidzami jāizdara. Visām dalībvalstīm ir jāpabeidz nozaru tiesību aktu saskaņošana ar Regulas prasībām.
* Komisija izmantos visus tās rīcībā esošos instrumentus, ieskaitot pārkāpuma procedūras, lai nodrošinātu, ka dalībvalstis ievēro Regulu, un mazinātu datu aizsardzības regulējuma sadrumstalotību.

*Jaunās pārvaldības sistēmas potenciāla pilnīga izmantošana*

* Dalībvalstīm jāpiešķir valstu datu aizsardzības iestādēm pietiekami cilvēkresursi, finanšu un tehniskie resursi.
* Datu aizsardzības iestādēm jāuzlabo sadarbība, piemēram, veicot kopīgas izmeklēšanas. Dalībvalstīm jāatbalsta šādu izmeklēšanu veikšana.
* Kolēģijai ir jāturpina attīstīt ES datu aizsardzības kultūru un pilnībā jāizmanto Regulā paredzētie instrumenti, lai nodrošinātu noteikumu saskaņotu piemērošanu. Tai jāturpina izstrādāt pamatnostādnes, jo īpaši mazajiem un vidējiem uzņēmumiem paredzētās.
* Ir jāstiprina kolēģijas sekretariāta kompetence, lai tas efektīvāk atbalstītu un vadītu kolēģijas darbu.
* Komisija turpinās sniegt atbalstu datu aizsardzības iestādēm un kolēģijai, jo īpaši aktīvi piedaloties kolēģijas darbā un vēršot tās uzmanību uz ES tiesību aktu prasībām Regulas īstenošanas gaitā.
* Komisija atbalstīs sadarbību starp datu aizsardzības iestādēm un citām iestādēm, jo īpaši konkurences jomā, pilnībā ievērojot to attiecīgās pilnvaras.

*Atbalsts ieinteresētajām personām un to iesaiste*

* Kolēģijai jāuzlabo ieinteresēto personu iesaiste tās darbā. Komisija turpinās sniegt finansiālo atbalstu datu aizsardzības iestādēm, lai palīdzētu tām uzrunāt ieinteresētās personas.
* Komisija turpinās informētības uzlabošanas darbības, kā arī darbu ar ieinteresētajām personām.

*Starptautiskās konverģences veicināšana*

* Komisija turpinās pastiprināt dialogu par aizsardzības līmeņa pietiekamību ar atbilstīgiem galvenajiem partneriem, tostarp tiesībaizsardzības jomā. Tās mērķis jo īpaši ir tuvāko mēnešu laikā pabeigt notiekošās sarunas ar Dienvidkoreju. Tā 2020. gadā ziņos par to, kā pārskatīti 11 saskaņā ar Datu aizsardzības direktīvu pieņemtie lēmumi par aizsardzības līmeņa pietiekamību.
* Komisija turpinās sadarboties ar valstīm, kas ir ieinteresētas modernu privātuma tiesību aktu pieņemšanā, cita starpā sniedzot tām tehnisko palīdzību un apmainoties ar informāciju un paraugpraksi, kā arī veicinās sadarbību ar trešo valstu uzraudzības iestādēm un reģionālajām organizācijām.
* Komisija sadarbosies ar daudzpusējām un reģionālajām organizācijām, lai veicinātu augstus datu aizsardzības standartus, kas sekmē tirdzniecību un atvieglo sadarbību (piemēram, Japānas G20 ietvaros sāktajā iniciatīvā “Brīva datu plūsma uzticoties”).

Regula[[86]](#footnote-87) paredz Komisijas pienākumu 2020. gadā ziņot par tās īstenošanu. Tā būs iespēja izvērtēt panākto progresu un to, vai jaunā datu aizsardzības režīma dažādie komponenti pēc diviem piemērošanas gadiem pilnībā funkcionē. Šajā saistībā Komisija sadarbosies ar Eiropas Parlamentu, Padomi, dalībvalstīm, Eiropas Datu aizsardzības kolēģiju, attiecīgām ieinteresētajām personām un iedzīvotājiem.

1. Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.): [https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX%3A32016R0679](https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:32016R0679). [↑](#footnote-ref-2)
2. Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Direktīva (ES) 2016/680 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.):

   <https://eur-lex.europa.eu/legal-content/LV/ALL/?uri=celex:32016L0680>. Dalībvalstīm šī direktīva bija jātransponē līdz 2018. gada 6. maijam. Situācija transponēšanas jomā ir atspoguļota ziņojumos par drošības savienību. [↑](#footnote-ref-3)
3. Eiropas Parlamenta un Padomes 2018. gada 23. oktobra Regula (ES) 2018/1725 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39.–98. lpp.): [https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX%3A32018R1725](https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:32018R1725). Tā ir piemērojama no 2018. gada 11. decembra. [↑](#footnote-ref-4)
4. Indijas Augstākā tiesa 2017. gada 24. augustā nozīmīgā spriedumā atzina privātumu par pamattiesībām — “cilvēka cieņas svarīgu elementu”. [↑](#footnote-ref-5)
5. Komisijas paziņojums Eiropas Parlamentam un Padomei “Spēcīgāka aizsardzība, jaunas iespējas — Komisijas norādes par Vispārīgās datu aizsardzības regulas tiešu piemērošanu, sākot ar 2018. gada 25. maiju” (COM(2018) 43 final):

   [https://eur-lex.europa.eu/legal-content/LV/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043](https://eur-lex.europa.eu/legal-content/LV/TXT/?qid=1517578296944&uri=CELEX:52018DC0043). [↑](#footnote-ref-6)
6. Komisijas izveidotās Regulas daudzpusējās ieinteresēto personu grupas sastāvā ir pilsoniskās sabiedrības un uzņēmēju pārstāvji, akadēmiķi un praktizējoši speciālisti:

   <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537>. [↑](#footnote-ref-7)
7. <http://europa.eu/rapid/press-release_IP-19-2956_lv.htm>. [↑](#footnote-ref-8)
8. Regulas 97. pants. [↑](#footnote-ref-9)
9. Komisijas vadlīnijas par Savienības datu aizsardzības regulējuma piemērošanu vēlēšanu kontekstā (COM(2018) 638 final): <https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf>. [↑](#footnote-ref-10)
10. Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīva 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti:

    <https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=celex:31995L0046>. [↑](#footnote-ref-11)
11. Piemēram, piešķirt tām pilnvaras piemērot administratīvus naudas sodus. [↑](#footnote-ref-12)
12. 2019. gada 23. jūlijā valsts tiesību aktu pieņemšanas procesu vēl nav pabeigušas Grieķija, Portugāle un Slovēnija. [↑](#footnote-ref-13)
13. Sk. Regulas daudzpusējās ieinteresēto personu grupas 2019. gada 13. jūnija ziņojumu: <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670>. [↑](#footnote-ref-14)
14. Beļģijā, Dānijā, Igaunijā, Somijā, Latvijā, Maltā, Zviedrijā un Apvienotajā Karalistē šis vecums ir 13 gadi, Austrijā, Bulgārijā, Kiprā, Spānijā, Itālijā un Lietuvā — 14 gadi, Čehijā un Francijā — 15 gadi, Vācijā, Ungārijā, Horvātijā, Īrijā, Luksemburgā, Nīderlandē, Polijā, Rumānijā un Slovākijā — 16 gadi. [↑](#footnote-ref-15)
15. 8. pants. [↑](#footnote-ref-16)
16. Saskaņā ar Līguma par Eiropas Savienības darbību 16. panta 2. punktu. [↑](#footnote-ref-17)
17. Regulas 60. pants paredz datu aizsardzības iestāžu sadarbību ar mērķi konkrētās lietās piemērot vienādu Regulas interpretāciju. 64. pants paredz, ka kolēģija noteiktos gadījumos sniedz atzinumu, lai nodrošinātu Regulas konsekventu piemērošanu. Visbeidzot, kolēģija ir pilnvarota pieņemt datu aizsardzības iestādēm adresētus saistošus lēmumus, ja to starpā radušās domstarpības. [↑](#footnote-ref-18)
18. Tā ir noticis Vācijā un Spānijā. [↑](#footnote-ref-19)
19. <https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf> [↑](#footnote-ref-20)
20. Piemēram, Īrijas Datu aizsardzības komisija sāka 15 oficiālas izmeklēšanas par daudznacionālu tehnoloģiju uzņēmumu atbilstību Regulai. Sk. Īrijas Datu aizsardzības komisijas 2018. gada pārskata 49. lpp.:

    <https://www.dataprotection.ie/en/news-media/press-releases/dpc-publishes-annual-report-25-may-31-december-2018>. [↑](#footnote-ref-21)
21. Vairāki lēmumi, ar kuriem ir piemēroti naudas sodi, vēl var tikt pārskatīti tiesā. [↑](#footnote-ref-22)
22. 58. panta 2. punkta f) un j) apakšpunkts. [↑](#footnote-ref-23)
23. <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/ico-call-for-views-on-creating-a-regulatory-sandbox/> [↑](#footnote-ref-24)
24. Sk. VDAR daudzpusējās ieinteresēto personu grupas ziņojumu: <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670> [↑](#footnote-ref-25)
25. Deviņām datu aizsardzības iestādēm 2018. gadā piešķirti 2 miljoni EUR darbībām 2018.–2019. gadā: Beļģijai, Bulgārijai, Dānijai, Ungārijai, Lietuvai, Latvijai, Nīderlandei, Slovēnijai un Islandei: <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2017>;   
    2019. gadā tiks piešķirts 1 miljons EUR:  
    <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2019>. [↑](#footnote-ref-26)
26. Kolēģijai ir juridiskas personas statuss, tās sastāvā ir valstu datu aizsardzības uzraudzības iestāžu vadītāji un Eiropas Datu aizsardzības uzraudzītājs. [↑](#footnote-ref-27)
27. <https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_lv> [↑](#footnote-ref-28)
28. <https://edpb.europa.eu/our-work-tools/our-documents/publication-type/work-program_en> [↑](#footnote-ref-29)
29. Kā dalībnieks bez balsstiesībām. [↑](#footnote-ref-30)
30. Komisija ir arī palīdzējusi izlīdzināt kolēģijas izveides gaitu un sniedz atbalstu tās darbībā, nodrošinot komunikācijas sistēmu. [↑](#footnote-ref-31)
31. Regulas 62. pants. [↑](#footnote-ref-32)
32. Sk. Regulas daudzpusējās ieinteresēto personu grupas ziņojumu: <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670>.

    Piemēram, uzņēmumi uzskata, ka varētu pilnīgāk saskaņot valstu sarakstus, kuros uzskaitītas apstrādes darbības, kam saskaņā ar Regulas 35. pantu ir nepieciešams novērtējums par ietekmi uz datu aizsardzību. [↑](#footnote-ref-33)
33. Tostarp dažādu iestāžu starpā federālās valstīs. [↑](#footnote-ref-34)
34. <http://europa.eu/rapid/press-release_IP-19-2956_lv.htm> [↑](#footnote-ref-35)
35. <https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf> [↑](#footnote-ref-36)
36. Sk. Vispārīgās datu aizsardzības regulas daudzpusējās ieinteresēto personu grupas ziņojumu. [↑](#footnote-ref-37)
37. Sk. Vispārīgās datu aizsardzības regulas daudzpusējās ieinteresēto personu grupas ziņojumu. [↑](#footnote-ref-38)
38. Regulas 80. panta 1. punkts. [↑](#footnote-ref-39)
39. Regulas 80. panta 2. punkts. [↑](#footnote-ref-40)
40. Tā seko agrākai kampaņai, kuras mērķis bija izplatīt informatīvus materiālus privātpersonām un uzņēmumiem; materiāli pieejami šādā vietnē: <https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_lv>. [↑](#footnote-ref-41)
41. Sk. Regulas daudzpusējās ieinteresēto personu grupas ziņojumu. [↑](#footnote-ref-42)
42. Viena no galvenajām problēmām, ko bieži min, ir IT sistēmu atjaunināšana, jo īpaši attiecībā uz to principu ieviešanu, kas paredz integrētu datu aizsardzību un datu aizsardzību pēc noklusējuma, tiesības uz dzēšanu rezerves kopiju gadījumos utt. [↑](#footnote-ref-43)
43. Uzņēmumi arī lūdz kolēģiju izdot pamatnostādnes par nepamatotiem un pārmērīgiem pieprasījumiem. [↑](#footnote-ref-44)
44. Piemēram, saskaņā ar Izraēlas Kiberdrošības nozares apvienības publicētu ziņojumu 2018. gadā kiberdrošības apakšnozare “Datu aizsardzība un privātums” bija visstraujāk augošā apakšnozare — daļēji tādēļ, ka sākās VDAR piemērošana. [↑](#footnote-ref-45)
45. Atbilstīgi MVU definīcijai, kas pieejama šādā vietnē: <https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_lv>. [↑](#footnote-ref-46)
46. Patiesībā Regula nepaļaujas tikai uz piekrišanu, bet paredz vairākus personas datu apstrādes juridiskos pamatus. [↑](#footnote-ref-47)
47. Piemēram, Francijas datu aizsardzības iestādes izstrādātie norādījumi: <https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement>. [↑](#footnote-ref-48)
48. <https://ec.europa.eu/commission/sites/beta-political/files/ds-02-18-544-lv-n.pdf>. [↑](#footnote-ref-49)
49. Sk. Regulas 28. pantu. Komisijas pieņemtās līguma standartklauzulas ir spēkā visā ES. Turpretī standartklauzulas, ko saskaņā ar 28. panta 8. punktu pieņēmusi datu aizsardzības iestāde, ir saistošas tikai iestādei, kura tās pieņēmusi, un tādējādi tās var izmantot kā līguma standartklauzulas attiecībā uz apstrādes darbībām, kas ir šīs iestādes kompetencē saskaņā ar 55. un 56. pantu. [↑](#footnote-ref-50)
50. Tās ir galvenais instruments, ko uzņēmumi izmanto, veicot datu eksportu. [↑](#footnote-ref-51)
51. Eiropas Datu aizsardzības kolēģija 2019. gada 4. jūnijā ir pieņēmusi pamatnostādnes par rīcības kodeksiem. Tajās ir skaidrotas ar kodeksu iesniegšanu, apstiprināšanu un publicēšanu valsts un ES mērogā saistītās procedūras un noteikumi. [↑](#footnote-ref-52)
52. Regulas 98. apsvērums. [↑](#footnote-ref-53)
53. <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_lv>;

    <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_lv> [↑](#footnote-ref-54)
54. Sk. CIGI un *Ipsos* veikto 2019. gada globālo aptauju par drošību un uzticēšanos internetā. Minētajā aptaujā 78 % aptaujāto atzīst, ka viņus satrauc to privātums tiešsaistē, 49 % norāda, ka neuzticēšanās ir likusi tiem tiešsaistē izpaust mazāku personīgās informācijas apjomu, 43 % atklāj, ka pievērš lielāku uzmanību ierīču drošības panākšanai, bet 39 % atbild, ka līdztekus citiem piesardzības pasākumiem internetu izmanto selektīvāk. Aptauja tika veikta 25 valstīs: ASV, Austrālijā, Brazīlijā, Dienvidāfrikā, Ēģiptē, Francijā, Honkongā, Indijā, Indonēzijā, Itālijā, Japānā, Kanādā, Kenijā, Korejas Republikā, Krievijā, Ķīnā, Lielbritānijā, Meksikā, Nigērijā, Pakistānā, Polijā, Tunisijā, Turcijā, Vācijā un Zviedrijā. [↑](#footnote-ref-55)
55. Eiropas Padomes 1981. gada 28. janvāra Konvencija par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (*ETS* Nr. 108) un Konvencijas par personu aizsardzību attiecībā uz personas datu automātisko apstrādi 2001. gada Papildu protokols par uzraudzības institūcijām un pārrobežu datu plūsmām (*ETS* Nr. 181). Tas ir vienīgais saistošais daudzpusējais akts datu aizsardzības jomā. Valstis, kas šo konvenciju ratificējušas visnesenāk, ir Argentīna, Meksika, Kaboverde un Maroka. [↑](#footnote-ref-56)
56. Protokols, ar ko groza Konvenciju par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (*ETS* Nr. 108); vienošanās panākta Ministru komitejas 128. sesijā, kura notika Helsingērā, Dānijā, 2018. gada 17. un 18. maijā. Modernizētās 108. konvencijas konsolidēta versija ir pieejama šādā vietnē: <https://rm.coe.int/16808ade9d>. [↑](#footnote-ref-57)
57. Komisijas paziņojums Eiropas Parlamentam un Padomei “Apmaiņa ar personas datiem un šo datu aizsardzība globalizētā pasaulē” (COM(2017) 7 final). [↑](#footnote-ref-58)
58. Regula ir arī radījusi iespēju pieņemt pietiekamas aizsardzības atzinumus attiecībā uz starptautiskajām organizācijām — tā ir daļa no ES centieniem veicināt datu apmaiņu ar šādām struktūrām. [↑](#footnote-ref-59)
59. Šādu pieeju ir izvēlējušās, piemēram, Argentīna, Kolumbija, Izraēla un Šveice. [↑](#footnote-ref-60)
60. Tas nozīmē, ka privātuma vairogā tā pirmajos trijos darbības gados ir vairāk dalībnieku nekā tā priekšgājējā — “drošības zonā” — bija pēc 13 darbības gadiem. [↑](#footnote-ref-61)
61. Tas atspoguļojas, piemēram, G20 valstu vadītāju Osakas deklarācijā lietotajā atsaucē uz “brīvu datu plūsmu uzticoties”:

    <https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf>. [↑](#footnote-ref-62)
62. Sk. Komisijas paziņojumu Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai “Eiropas Drošības programma” (COM(2015) 185 final). [↑](#footnote-ref-63)
63. Nolīgums starp Amerikas Savienotajām Valstīm un Eiropas Savienību par personas informācijas aizsardzību saistībā ar noziedzīgu nodarījumu novēršanu, izmeklēšanu un atklāšanu, kā arī saukšanu pie kriminālatbildības par tiem: <https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=celex:22016A1210(01)> (“jumta nolīgums”). Jumta nolīgums ir pirmais divpusējais starptautiskais nolīgums tiesībaizsardzības jomā, un tas paredz visaptverošu datu aizsardzības tiesību un pienākumu kopumu atbilstīgi ES *acquis*. Tas ir veiksmīgs piemērs tam, kā, vienojoties par spēcīgu datu aizsardzības pasākumu kopumu, iespējams uzlabot tiesībaizsardzības sadarbību ar svarīgu starptautisko partneri. [↑](#footnote-ref-64)
64. ANO Drošības padomes 2017. gada 21. decembra rezolūcijā Nr. 2396 visas ANO dalībvalstis tiek aicinātas attīstīt spējas ievākt, apstrādāt un analizēt PDR datus, pilnībā ievērojot cilvēktiesības un pamatbrīvības. Sk. arī Komisijas paziņojumu “Eiropas Drošības programma” (COM(2015) 185 final): <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf>. [↑](#footnote-ref-65)
65. <https://ec.europa.eu/home-affairs/news/security-union-strengthening-europols-cooperation-third-countries-fight-terrorism-and-serious_en> [↑](#footnote-ref-66)
66. <http://europa.eu/rapid/press-release_IP-19-2891_lv.htm> [↑](#footnote-ref-67)
67. Sk. Regulas 50. pantu par starptautisko sadarbību datu aizsardzības jomā. Šis pants aptver plašu sadarbības formu loku — no informēšanas par datu aizsardzības tiesību aktiem līdz sūdzību tālākai nosūtīšanai un palīdzībai izmeklēšanā. [↑](#footnote-ref-68)
68. Piemēram, varētu izstrādāt vienotas veidnes ziņošanai par pārkāpumiem. [↑](#footnote-ref-69)
69. [https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX%3A52017PC0010](https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:52017PC0010) [↑](#footnote-ref-70)
70. Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīva 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (Direktīva par privāto dzīvi un elektronisko komunikāciju) (OV L 201, 31.7.2002., 37.–47. lpp.). [↑](#footnote-ref-71)
71. [https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=celex%3A32014R0536](https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=celex:32014R0536) [↑](#footnote-ref-72)
72. <https://ec.europa.eu/health/sites/health/files/files/documents/qa_clinicaltrials_gdpr_en.pdf> [↑](#footnote-ref-73)
73. Komisijas 2019. gada 8. aprīļa paziņojums “Vairojot uzticēšanos antropocentriskam mākslīgajam intelektam”: <https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-human-centric-artificial-intelligence>.

    Augsta līmeņa ekspertu grupas (ALEG) 2019. gada 8. aprīlī prezentētās ētikas vadlīnijas uzticamam MI: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>. Sk. arī ESAO Padomes rekomendāciju par mākslīgo intelektu: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>, G20 valstu vadītāju Osakas deklarācijā atbalstītos G20 MI principus: <https://www.g20.org/pdf/documents/en/annex_08.pdf>, kā arī G20 valstu ministru paziņojumu par tirdzniecību un digitālo ekonomiku: <https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf>. [↑](#footnote-ref-74)
74. Regulas 22. pants. [↑](#footnote-ref-75)
75. Regulas 13. panta 2. punkta f) apakšpunkts. [↑](#footnote-ref-76)
76. <https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence> [↑](#footnote-ref-77)
77. Padomes rekomendācija par mākslīgo intelektu: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>. [↑](#footnote-ref-78)
78. G20 valstu ministru paziņojums par tirdzniecību un digitālo ekonomiku:

    <https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf>. [↑](#footnote-ref-79)
79. <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf> [↑](#footnote-ref-80)
80. Piemēram, atvieglojot ceļojuma plānošanu un dažādu transporta veidu izmantošanu tā laikā. [↑](#footnote-ref-81)
81. Jo īpaši Elektroenerģijas direktīva:

    [https://eur-lex.europa.eu/legal-content/LV/ALL/?uri=CELEX%3A32009L0072](https://eur-lex.europa.eu/legal-content/LV/ALL/?uri=CELEX:32009L0072). [↑](#footnote-ref-82)
82. Piemēram, lietā M. 8788, *Apple*/*Shazam* un lietā M. 8124, *Microsoft*/*LinkedIn*. [↑](#footnote-ref-83)
83. <https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf> [↑](#footnote-ref-84)
84. <http://europa.eu/rapid/press-release_IP-18-5681_lv.htm> [↑](#footnote-ref-85)
85. <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf> [↑](#footnote-ref-86)
86. Regulas 97. pants. [↑](#footnote-ref-87)