



Briselē, 24.1.2018.
COM(2018) 43 final

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

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

Ievads

2016. gada 6. aprīlī ES vienojās veikt būtisku datu aizsardzības sistēmas reformu, pieņemot datu aizsardzības reformu paketi, kurā ietilpst Vispārīgā datu aizsardzības regula (VDAR)¹, ar ko aizstāj divdesmit gadus veco Direktīvu 95/46/EK² (“Datu aizsardzības direktīvu”), un Policijas direktīva³. Jaunais ES mēroga datu aizsardzības instruments, Vispārīgā datu aizsardzības regula (“Regula”), būs jāsāk tieši piemērot no 2018. gada 25. maija — divus gadus pēc tā pieņemšanas un stāšanās spēkā⁴.

Jaunā Regula stiprinās fizisko personu tiesības uz personas datu aizsardzību, atspoguļojot datu aizsardzības būtību kā Eiropas Savienības pamattiesības⁵.

Nodrošinot tādu noteikumu vienotu kopumu, kas ir tieši piemērojami dalībvalstu tiesību sistēmās, tiks garantēta personas datu brīva aprīte starp ES dalībvalstīm un stiprināta patērētāju uzticība un drošība, kas ir divi obligāti elementi, lai eksistētu reāls digitālais vienotais tirgus. Tādējādi Regula pavērs jaunas iespējas uzņēmumiem, jo īpaši mazākajiem, arī padarot skaidrākus noteikumus par datu starptautisku nosūtīšanu.

Kaut gan jaunā datu aizsardzības sistēma ir veidota uz esošo tiesību aktu pamata, tai būs plaša ietekme un noteiktos aspektos būs nepieciešami būtiski pielāgojumi. Tāpēc Regulā bija paredzēts divu gadu pārejas periods — līdz 2018. gada 25. maijam —, lai dalībvalstīm un ieinteresētajām personām dotu laiku pilnībā sagatavoties jaunā tiesiskā regulējuma piemērošanai.

Pēdējos divos gados visas ieinteresētās personas — no valstu pārvaldēm un valsts datu aizsardzības iestādēm līdz datu pārzinīem un apstrādātājiem — ir iesaistījušās vairākās aktivitātēs ar mērķi nodrošināt, ka tiek izprasta jaunā datu aizsardzības regulējuma izmaiņu nozīme un apmērs un ka visi dalībnieki ir gatavi tā piemērošanai. Tā kā noteiktais termiņš — 25. maijs — tuvojas, Komisija uzskata, ka šis darbs ir kritiski jānovērtē un ir jāapsver, kādi turpmāki pasākumi varētu būt lietderīgi, lai garantētu, ka ir nodrošināti visi elementi, lai sekmīgi sāktu piemērot jauno regulējumu⁶.

Šajā paziņojumā:

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 aprīti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula), OV L 119, 4.5.2016.

² Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīva 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu aprīti, OV L 281, 23.11.1995.

³ 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 aprīti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI, OV L 119, 4.5.2016.

⁴ Regula ir spēkā kopš 2016. gada 24. maija un būs piemērojama no 2018. gada 25. maija.

⁵ ES Pamattiesību hartas 8. pants un LESD 16. pants.

⁶ https://ec.europa.eu/commission/sites/beta-political/files/letter-of-intent-2017_lv.pdf.

- ir aplūkotas galvenās inovācijas un iespējas, ko paver jaunais ES datu aizsardzības regulējums;
- ir izvērtēts līdz šim ES līmenī veiktais sagatavošanās darbs;
- ir izklāstīts, kas vēl ir jādara Eiropas Komisijai, valstu datu aizsardzības iestādēm un valstu pārvaldes iestādēm, lai sekmīgi pabeigtu sagatavošanos;
- ir noteikti pasākumi, kurus Komisija plāno īstenot tuvākajos mēnešos.

Turklāt vienlaikus ar šā paziņojuma pieņemšanu Komisija laiž klajā tiešsaistes rīku kopumu, kas palīdzēs ieinteresētajām personām sagatavoties Regulas piemērošanai, un ar pārstāvniecību atbalstu īsteno informatīvu kampaņu visās dalībvalstīs.

1. JAUNAIS ES DATU AIZSARDZĪBAS REGULĒJUMS — STIPRĀKA AIZSARDZĪBA UN JAUNAS IESPĒJAS

Regulā vēl arvien ir īstenota Datu aizsardzības direktīvas pieeja, taču datu aizsardzības noteikumi ir precizēti un modernizēti, balstoties uz 20 gadu pieredzi ES datu aizsardzības regulējuma jomā un attiecīgo judikatūru; ar to tiek ieviesti vairāki jauni elementi, kas stiprina fizisko personu tiesību aizsardzību un paver iespējas uzņēmumiem, proti:

- **saskaņots tiesiskais regulējums, kas liek pamatus vienotai prasību piemērošanai, sekmējot ES digitālo vienoto tirgu.** Tas nozīmē: viens vienīgs noteikumu kopums — gan iedzīvotājiem, gan uzņēmumiem. Tas risinās pašreizējo situāciju, kad ES dalībvalstis Direktīvas noteikumus ir piemērojušas dažādi. Lai nodrošinātu vienotu un konsekventu piemērošanu visās dalībvalstīs, ir ieviests vienas pieturas aģentūras mehānisms;
- **vienlīdzīgi apstākļi visiem uzņēmumiem, kas darbojas ES tirgū.** Regula paredz, ka uzņēmumiem, kas reģistrēti ārpus ES, piemēro tāds pašus noteikumus kā ES reģistrētiem uzņēmumiem, ja tie piedāvā preces un pakalpojumus, kas saistīti ar personas datiem, vai veic iedzīvotāju uzvedības novērošanu Savienībā. Uzņēmumiem, kas reģistrēti ārpus ES un darbojas vienotajā tirgū, noteiktos gadījumos ir jāieceļ pārstāvis ES, pie kura iedzīvotāji un iestādes var vērsties, papildus ārzemēs esošajam uzņēmumam vai tā vietā;
- **datu aizsardzības principi, kas paredz integrētu datu aizsardzību un datu aizsardzību pēc noklusējuma,** rada stimulus inovatīviem risinājumiem, lai jau no paša sākuma risinātu datu aizsardzības jautājumus;
- **spēcīgākas personu tiesības:** ar Regulu tiek ieviestas jaunas pārredzamības prasības; tiek stiprinātas tiesības uz informāciju, piekļuvi datiem un to dzēšanu (“tiesības tikt aizmirstam”); klusēšana vai atturēšanās no darbības vairs netiks uzskatīta par derīgu piekrišanu, jo piekrišana ir jāsniedz skaidri apstiprinošas darbības veidā; bērnu aizsardzība tiešsaistē;
- **personām ir lielāka kontrole pār saviem personas datiem.** Ar Regulu izveido **jaunas tiesības uz datu pārnesamību**, kas ļauj iedzīvotājiem pieprasīt, lai uzņēmums vai organizācija atdod atpakaļ personas datus, kurus viņi ir iesnieguši uzņēmumam vai organizācijai uz piekrišanas vai līguma pamata; tajā ir atļauts arī šādus personas datus nosūtīt tieši citam uzņēmumam vai organizācijai, ja tas ir tehniski iespējams. Tā kā Regulā ir atļauta personas datu tieša nosūtīšana no viena uzņēmuma vai organizācijas citam, arī šīs tiesības atbalsta personas datu brīvu apriti ES, izvairoties no personas datu iestrēgšanas, un sekmē konkurenci starp uzņēmumiem. Atvieglojot iedzīvotājiem pāreju

starp dažādiem pakalpojumu sniedzējiem, tiks veicināta jaunu pakalpojumu izstrāde digitālā vienotā tirgus stratēģijas kontekstā;

- **spēcīgāka aizsardzība pret datu aizsardzības pārkāpumiem.** Regulā ir noteikts visaptverošs noteikumu kopums par personas datu aizsardzības pārkāpumiem. Tajā ir skaidri definēts, kas ir “personas datu aizsardzības pārkāpums”, ir ieviests pienākums ne vēlāk kā 72 stundās no brīža, kad datu aizsardzības pārkāpums varētu radīt risku personas tiesībām un brīvībām, paziņot par to uzraudzības iestādei. Noteiktos apstākļos ir pienākums informēt to personu, uz kuras datiem attiecas pārkāpums. Tas lielā mērā uzlabo aizsardzību, salīdzinot ar pašreizējo situāciju ES, kur tikai elektronisko komunikāciju pakalpojumu sniedzējiem, būtisko pakalpojumu operatoriem un digitālo pakalpojumu sniedzējiem ir pienākums paziņot par datu aizsardzības pārkāpumiem attiecīgi saskaņā ar Direktīvu par privāto dzīvi un elektronisko komunikāciju (“E-privātuma direktīva”)⁷ un Direktīvu par tīklu un informācijas sistēmu drošību (*NIS* direktīva)⁸;
- **Regula piešķir visām datu aizsardzības iestādēm pilnvaras uzlikt sodus pārzīņiem un apstrādātājiem.** Pašlaik šīs pilnvaras nav piešķirtas visām iestādēm. Tas ļaus labāk īstenot noteikumus. Sodu var noteikt apmērā līdz 20 miljoniem euro vai, uzņēmuma gadījumā, līdz 4 % no tā visā pasaulē gūtā gada apgrozījuma;
- **lielāka elastība pārzīņiem un apstrādātājiem, apstrādājot personas datus, pateicoties viennozīmīgiem atbildības noteikumiem (pārskatatbildības princips).** Ar Regulu tiek veikta pāreja no paziņošanas sistēmas uz pārskatatbildības principu. To īsteno, nosakot mērogojamu atbildību atkarībā no riska (piem., datu aizsardzības speciālista klātbūtne vai pienākums veikt novērtējumus par ietekmi uz datu aizsardzību). Lai palīdzētu novērtēt risku pirms datu apstrādes sākšanas, ir ieviests jauns instruments: novērtējums par ietekmi uz datu aizsardzību. Tas ir jāveic tad, ja apstrāde varētu radīt augstu risku personu tiesībām un brīvībām. Regulā īpaši ir izceltas šādas trīs situācijas: ja uzņēmums sistemātiski un plaši novērtē ar fizisku personu saistītus personiskus aspektus (tostarp veic profilēšanu), ja tas plašā mērogā apstrādā sensitīvus datus vai sistemātiski uzrauga plašā mērogā publiski pieejamas zonas. Valstu datu aizsardzības iestādēm būs jāpublisko tādu gadījumu saraksti, attiecībā uz kuriem ir jāveic novērtējums par ietekmi uz datu aizsardzību⁹;
- **lielāka skaidrība par apstrādātāju pienākumiem un pārzīņu atbildību, izvēloties apstrādātāju;**

⁷ 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. Saskaņā ar VDAR 95. pantu šī regula neuzliek papildu pienākumus fiziskām vai juridiskām personām attiecībā uz apstrādi jautājumos, saistībā ar kuriem tām ir piemērojami Direktīvas 2002/58/EK īpašie noteikumi ar to pašu mērķi. Tas nozīmē, piemēram, to, ka subjektiem, uz kuriem attiecas E-privātuma direktīva, ir saistošs minētajā direktīvā noteiktais pienākums paziņot par personas datu aizsardzības pārkāpumu, ciktāl pārkāpums attiecas uz pakalpojumu, kas ietilpst E-privātuma direktīvas materiālajā piemērošanas jomā. Šiem subjektiem ar VDAR netiek noteikti papildus pienākumi.

⁸ Eiropas Parlamenta un Padomes 2016. gada 6. jūlija Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā, OV L 194, 19.7.2016., 1.–30. lpp. Vienībām, kas ietilpst *NIS* direktīvas darbības jomā, ir jāpaziņo par incidentiem, kuriem ir traucējoša vai būtiska ietekme uz dažu to pakalpojumu sniegšanu. Paziņošana par incidentiem saskaņā ar *NIS* direktīvu neskar paziņošanu par pārkāpumiem saskaņā ar Regulu.

⁹ Regulas 35. pants.

- **moderna pārvaldības sistēma, lai nodrošinātu noteikumu konsekventāku un stingrāku izpildi.** Tas ietver datu aizsardzības iestāžu saskaņotas pilnvaras, tostarp attiecībā uz sodiem, un jaunus mehānismus, kas ļauj šīm iestādēm sadarboties tīklā;
- **personas datu aizsardzība, ko garantē Regula, turpinās, kad datus nosūta ārpus ES, nodrošinot augstu aizsardzības līmeni¹⁰.** Lai gan Regulā izklāstītā starptautiskās nosūtīšanas noteikumu arhitektūra būtībā saglabājas tāda pati kā 1995. gada Direktīvā, ar reformu tiek precizēta un vienkāršota minēto noteikumu izmantošana un tiek ieviesti jauni nosūtīšanas instrumenti. Attiecībā uz lēmumiem par aizsardzības līmeņa pietiekamību — ar Regulu tiek ieviests precīzs un detalizēts elementu katalogs, kas Komisijai ir jāņem vērā, novērtējot, vai ārvalstu sistēma pietiekami aizsargā personas datus. Regulā arī formalizēti un paplašināti vairāki alternatīvi nosūtīšanas instrumenti, piemēram, līguma standartklauzulas un saistoši uzņēmuma noteikumi.

Ar pārstrādāto Regulu ES iestādēm, struktūrām, birojiem un aģentūrām¹¹ un Privātuma un elektronisko sakaru regulu (“E-privātuma regulu”)¹², kas pašlaik tiek apspriestas, pēc to pieņemšanas tiks nodrošināts, ka ES rīcībā ir spēcīgs un visaptverošs datu aizsardzības noteikumu kopums¹³.

2. LĪDZ ŠIM ES LĪMENĪ VEIKTAIS SAGATAVOŠANĀS DARBS

Lai Regulas piemērošana noritētu sekmīgi, ir nepieciešams, lai sadarbotos visas datu aizsardzībā iesaistītās personas: dalībvalstis, tostarp valsts pārvaldes iestādes, valstu datu aizsardzības iestādes (DAI), uzņēmumi, organizācijas, kas pārstrādā personas datus, un iedzīvotāji, kā arī Komisija.

2.1. Eiropas Komisijas veiktie pasākumi

Neilgi pēc Regulas stāšanās spēkā 2016. gada vidū Komisija uzsāka sadarbību ar dalībvalstu iestādēm, datu aizsardzības iestādēm un ieinteresētajām personām, lai sagatavotos Regulas piemērošanai un sniegtu atbalstu un padomus.

a) Atbalsts dalībvalstīm un to iestādēm

Komisija cieši sadarbojās ar dalībvalstīm, atbalstot to darbu pārejas periodā, lai nodrošinātu visaugstāko iespējamo konsekvences līmeni. Tāpēc Komisija izveidoja ekspertu grupu, kas palīdz dalībvalstīm to centienos sagatavoties Regulas piemērošanai. Minētā grupa, kas ir rīkojusi apspriedes jau 13 reizes, darbojas kā forums, kurā dalībvalstis var dalīties ar pieredzi

¹⁰ Komisijas Paziņojums par apmaiņu ar personas datiem un šo datu aizsardzību globalizētā pasaulē, COM(2017) 7 *final*.

¹¹ Priekšlikums Eiropas Parlamenta un Padomes regulai par personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK, COM(2017) 8 *final*.

¹² 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) 10 *final*.

¹³ Līdz E-privātuma regulas pieņemšanai un piemērošanas sākšanai kā *lex specialis* saistībā ar Regulu ir piemērojama Direktīva 2002/58/EK.

un kompetenci¹⁴. Komisija arī iesaistījās divpusējās sanāksmēs ar dalībvalstu iestādēm, lai pārrunātu valstu līmenī radušos jautājumus.

b) Atbalsts atsevišķām datu aizsardzības iestādēm un Eiropas Datu aizsardzības iestādes izveide

Komisija aktīvi atbalstīja 29. panta darba grupas darbu, arī ar mērķi nodrošināt veiksmīgu pāreju uz Eiropas Datu aizsardzības kolēģiju¹⁵.

c) Starptautiski pasākumi

Ar Regulu papildus tiks stiprināta ES spēja aktīvi veicināt datu aizsardzības vērtības un tiks sekmēta pārrobežu datu aprīte, aicinot uz tiesību sistēmu konvergenci globālā mērogā¹⁶. ES datu aizsardzības noteikumus arvien plašāk atzīst starptautiskā līmenī kā tādus, kas nosaka vienus no visaugstākajiem datu aizsardzības standartiem pasaulē. Tiek modernizēta arī Eiropas Padomes Konvencija Nr. 108, kas ir vienīgais juridiski saistošais daudzpusējais instruments personas datu aizsardzības jomā. Komisija strādā, lai tajā tiktu atspoguļoti tie paši principi kā tie, kas nostiprināti jaunajos ES datu aizsardzības noteikumos, un tādējādi palīdz ieviest vienotu augstu datu aizsardzības standartu kopumu. Komisija aktīvi veicinās Konvencijas modernizētā teksta ātru pieņemšanu, lai ES varētu kļūt par tās līgumslēdzēju pusi¹⁷. Komisija aicina valstis, kas nav ES dalībvalstis, ratificēt Eiropas Padomes Konvenciju Nr. 108 un tās Papildprotokolu.

Turklāt vairākas valstis un reģionālās organizācijas ārpus ES — no tuvākās apkārtnes līdz Āzijai, Latīņamerikai un Āfrikai — pieņem jaunu datu aizsardzības regulējumu vai aktualizē spēkā esošo, lai izmantotu globālās digitālās ekonomikas sniegtās iespējas un reaģētu uz pieaugošo pieprasījumu pēc lielākas datu drošības un privātuma aizsardzības. Lai arī valstu pieeja un to tiesiskā regulējuma izstrādes līmenis ir atšķirīgs, ir vērojamas pazīmes, ka Regulu arvien biežāk izmanto par atsauces punktu un iedvesmas avotu¹⁸.

Šajā kontekstā Komisija īsteno starptautiskus pasākumus atbilstoši tās 2017. gada janvāra Paziņojumam¹⁹, aktīvi sadarbojoties ar galvenajiem tirdzniecības partneriem, īpaši Austrumāzijā, Dienvidaustrumāzijā un Latīņamerikā, lai izvērtētu iespēju pieņemt lēmumus par aizsardzības līmeņa pietiekamību²⁰.

Jo īpaši Komisija sadarbojas ar Japānu, lai abas puses vienlaicīgi sasniegtu pietiekamas aizsardzības līmeni līdz 2018. gada sākumam, kā paziņojis priekšsēdētājs Ž. K. Junkers un

¹⁴ Pilnu sarakstu par sanāksmēm un darba kārtību, pārrunu kopsavilkumu un pārskatu par regulējuma stāvokli dažādās dalībvalstīs skatīt vietnē <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3461&Lang=LV>.

¹⁵ Piemēram, Komisija sniegs iespēju Eiropas Datu aizsardzības kolēģijai izmantot Iekšējā tirgus informācijas sistēmu (*IMI*), lai veiktu saziņu starp tās dalībniekiem.

¹⁶ Pārdomu dokuments par globalizācijas iespēju izmantošanu COM(2017) 240.

¹⁷ Eiropas Padomes 1981. gada 28. janvāra Konvencija par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (ETS Nr. 108) un 2001. gada Papildprotokols Konvencijai par personu aizsardzību attiecībā uz personas datu automātisko apstrādi attiecībā uz uzraudzības iestādēm un pārrobežu datu apriti (ETS Nr. 181). Konvencija ir pieejama pusēm, kas nav Eiropas Padomes dalībnieces, un to jau ir ratificējusi 51 valsts (tostarp Urugvaja, Maurīcija, Senegāla un Tunisija).

¹⁸ Sk., piem., "Ibērijas pussalas un Latīņamerikas valstu datu aizsardzības standarti", http://www.redipd.es/documentacion/common/Estandares_eng_Con_logo_RIPD.pdf.

¹⁹ COM(2017) 7.

²⁰ COM(2017) 7, turpat 10. un 11. lpp.

premjermministrs Š. Abe kopīgajā 2017. gada 6. jūlija deklarācijā²¹. Ir uzsāktas sarunas arī ar Dienvidkoreju, ņemot vērā iespēju pieņemt lēmumu par aizsardzības līmeņa pietiekamību. Lēmuma par aizsardzības līmeņa pietiekamību pieņemšana nodrošinātu brīvu datu apriti ar attiecīgajām trešām valstīm, vienlaikus nodrošinot augsta vajadzīgo personas datu aizsardzības līmeņa piemērošanu gadījumos, kad no ES tiek nosūtīti dati uz šīm valstīm.

Vienlaikus Komisija sadarbojas ar iesaistītajām pusēm nolūkā pilnvērtīgi pielietot VDAR ietvertu starptautiskai datu pārsūtīšanai piemērojamo instrumentu kopumu, izstrādājot alternatīvus nosūtīšanas mehānismus, kas pielāgoti konkrētu nozaru un/vai dalībnieku īpašajām vajadzībām²².

d) Ieinteresēto personu iesaistīšana

Komisija ir organizējusi vairākus pasākumus, lai iesaistītu ieinteresētās personas²³. Ir plānots, ka 2018. gada pirmajā ceturksnī notiks jauns darbseminārs patērētājiem. Ir notikušas arī īpašas nozaru apspriedes tādās jomās kā pētniecība un finanšu pakalpojumi.

Komisija ir izveidojusi arī daudzpusējo ieinteresēto personu grupu saistībā ar Regulas jautājumiem, kurā piedalās pilsoniskās sabiedrības un uzņēmumu pārstāvji, akadēmiķi un praktizējoši speciālisti. Šī grupa konsultēs Komisiju jo īpaši par to, kā panākt, lai ieinteresētās personas būtu pienācīgi informētas par Regulu²⁴.

Visbeidzot, Eiropas Komisija ar tās Pētniecības un inovāciju pamatprogrammas “Apvārsnis 2020”²⁵ starpniecību ir finansējusi darbības ar mērķi izstrādāt instrumentus, kas atbalsta noteikumu efektīvu piemērošanu saskaņā ar Regulu saistībā ar piekrišanu un datu analītikas privātuma saglabāšanas metodēm, piemēram, daudzpusēju skaitļošanu un homomorfisku šifrēšanu.

2.2. Pasākumi, ko veic 29. panta darba grupa / Eiropas Datu aizsardzības kolēģija

29. panta darba grupai, kas apvieno visas valsts datu aizsardzības iestādes, tostarp Eiropas Datu aizsardzības uzraudzītāju, ir liela nozīme, sagatavojoties Regulas piemērošanai, jo tā izdod pamatnostādnes uzņēmumiem un citām ieinteresētajām personām. Valsts datu aizsardzības iestādes kā Regulas izpildītāji un tieša kontakta nodrošinātāji ar ieinteresētajām personām ir vislabākajā situācijā, lai vairotu tiesisko paļāvību attiecībā uz Regulas interpretāciju.

29. panta darba grupas pamatnostādnes / darba dokumenti, ņemot vērā Regulas piemērošanas sākšanu ²⁶	
Tiesības uz datu pārnesamību	Pieņemts 2017. gada 4. un 5. aprīlī.
Datu aizsardzības speciālisti	

²¹ http://europa.eu/rapid/press-release_STATEMENT-17-1917_en.htm.

²² COM(2017)7, ibid, 10-11. lpp.

²³ Divi darbsemināri ar nozares pārstāvjiem 2016. gada jūlijā un 2017. gada aprīlī, divas apaļā galda diskusijas par uzņēmējdarbību 2016. gada decembrī un 2017. gada maijā, darbseminārs par veselības datiem 2017. gada oktobrī un darbseminārs ar MVU pārstāvju dalību 2017. gada novembrī.

²⁴ <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537>.

²⁵ <https://ec.europa.eu/programmes/horizon2020/h2020-sections>

²⁶ Visas pieņemtās pamatnostādnes ir pieejamas vietnē: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

Vadošās uzraudzības iestādes iecelšana	
Novērtējums par ietekmi uz datu aizsardzību	Pieņemts 2017. gada 3. un 4. oktobrī.
Administratīvie sodi	Pieņemts 2017. gada 3. un 4. oktobrī.
Profilēšana	Darbs turpinās.
Datu aizsardzības pārkāpums	Darbs turpinās.
Piekrišana	Darbs turpinās.
Pārredzamība	Darbs turpinās.
Sertifikācija un akreditācija	Darbs turpinās.
Pietiekamības atsauces	Darbs turpinās.
Saistoši uzņēmuma noteikumi pārziņiem	Darbs turpinās.
Saistoši uzņēmuma noteikumi apstrādātājiem	Darbs turpinās.

29. panta darba grupa strādā, lai aktualizētu esošos atzinumus, tostarp par instrumentiem datu nosūtīšanai uz valstīm, kas nav ES dalībvalstis.

Tā kā ir būtiski, lai operatoriem būtu saskaņots un vienots pamatnostādņu kopums, pašreizējās pamatnostādnes valstu līmenī ir vai nu jāatceļ, vai jāpielīdzina pamatnostādņēm, ko par to pašu tēmu ir pieņēmusi 29. panta darba grupa / Eiropas Datu aizsardzības kolēģija.

Komisija lielu nozīmi piešķir tam, ka pirms šo pamatnostādņu pabeigšanas notiek to sabiedriskā apspriešana. Ir būtiski, lai ieinteresēto personu ieguldījums šajā procesā būtu pēc iespējas precīzāks un konkrētāks, jo tas palīdzēs noskaidrot paraugprakses un pievērsīs 29. panta darba grupas uzmanību nozarei un tās iezīmēm. Galīgo atbildību par šīm pamatnostādņēm saglabā 29. panta darba grupa un nākotnes Eiropas Datu aizsardzības kolēģija, un datu aizsardzības iestādes, īstenojot Regulu, vērsīsies pie tām.

Vajadzētu būt iespējai grozīt pamatnostādnes, ņemot vērā attīstības tendences un praksi. Šai nolūkā ir būtiski, lai datu aizsardzības iestādes veicinātu dialoga kultūru ar visām ieinteresētajām personām, tostarp uzņēmumiem.

Ir svarīgi atcerēties, ka gadījumos, ja radīsies jautājumi par Regulas interpretāciju un piemērošanu, dalībvalstu un ES līmeņa tiesām būs jāsniedz Regulas galīgā interpretācija.

3. PASĀKUMI, KAS VĒL JĀVEIC, LAI SAGATAVOŠANĀS BŪTU SEKMĪGA

3.1. Dalībvalstīm ir jāpabeidz tiesiskā regulējuma izveide valsts līmenī

Šā Regula ir tieši piemērojama visās dalībvalstīs²⁷. Tas nozīmē, ka tā stājas spēkā un ir piemērojama neatkarīgi no valsts tiesību pasākumiem: iedzīvotāji, uzņēmumi, valsts pārvaldes iestādes un citas organizācijas, kas apstrādā personas datus, parasti var tieši paļauties uz Regulas noteikumiem. Taču saskaņā ar Regulu dalībvalstīm ir jāveic nepieciešamie pasākumi,

²⁷ LESD 288. pants.

lai pielāgotu savus tiesību aktus, atceļot un grozot esošos tiesību aktus, kā arī izveidojot valsts datu aizsardzības iestādes²⁸, izvēloties akreditācijas struktūru²⁹ un pieņemot noteikumus, lai saglabātu līdzsvaru starp vārda brīvību un datu aizsardzību³⁰.

Regulā dalībvalstīm ir dota arī iespēja papildus precizēt datu aizsardzības noteikumu piemērošanu konkrētās nozarēs: valsts sektorā³¹, nodarbinātības un sociālā nodrošinājuma jomā³², saistībā ar profilaktisko un arodmedicīnu, sabiedrības veselību³³, arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos vai statistikas nolūkos³⁴, saistībā ar valsts identifikācijas numuru³⁵, publisku piekļuvi oficiāliem dokumentiem³⁶ un pienākumiem ievērot slepenību³⁷. Papildus attiecībā uz ģenētisko datu, biometrisko datu un veselības datu apstrādi Regulā ir noteikts, ka dalībvalstis var saglabāt vai ieviest papildu nosacījumus, tostarp ierobežojumus³⁸.

Dalībvalstu rīcību šajā kontekstā nosaka divi elementi:

- 1) Eiropas Savienības Pamattiesību hartas (“harta”) 8. pants, proti, ka valsts specifikācijas tiesību aktiem ir jāatbilst hartas 8. pantam (un Regulai, kas balstīta uz hartas 8. pantu), un
- 2) LESD 16. panta 2. punkts, kurā noteikts, ka valsts tiesiskais regulējums nedrīkst skart noteikumus par personas datu brīvu apriti ES.

Regula dod iespēju vienkāršot tiesisko vidi, tādējādi samazinot valsts tiesisko regulējumu un uzlabojot skaidrību operatoriem.

Dalībvalstīm, pielāgojot valsts tiesisko regulējumu, ir jāņem vērā tas, ka jebkādi valsts pasākumi, kuru rezultātā rastos šķēršļi Regulas tiešajai piemērojamībai vai tiktu apdraudēta tās vienlaicīga un vienota piemērošana visā ES, ir pretrunā Līgumiem³⁹.

Regulu teksta atkārtošana valsts tiesību aktos arī ir aizliegta (piem., definīciju vai personu tiesību atkārtošana), ja vien šāda atkārtošana ir obligāti vajadzīga saskaņotības dēļ un lai valsts tiesību aktus padarītu saprotamus tām personām, kam tie ir piemērojami⁴⁰. Regulas teksta atkārtošana vārdu pa vārdam valsts specifikācijas tiesiskajā regulējumā ir pieļaujama

²⁸ Regulas 54. panta 1. punkts.

²⁹ Regulas 43. panta 1. punktā ir noteikts, ka dalībvalstis nodrošina divus iespējamus sertifikācijas struktūru akreditācijas veidus, t. i., tās akreditē valsts datu aizsardzības uzraudzības iestāde, kas izveidota saskaņā ar datu aizsardzības regulējumu, un/vai valsts akreditācijas struktūra, kas izveidota saskaņā ar Regulu (EK) Nr. 765/2008 par akreditāciju un tirgus uzraudzību. Šai nolūkā būtu cieši jāsadarbjas Eiropas sadarbībai akreditācijai (“EA”, atzīta saskaņā ar Regulu 765/2008), kas apvieno valstu akreditācijas struktūras, un VDAR uzraudzības iestādēm.

³⁰ Regulas 85. panta 1. punkts.

³¹ Regulas 6. panta 2. punkts.

³² Regulas 88. pants un 9. panta 2. punkta b) apakšpunkts. Arī Eiropas sociālo tiesību pīlārā ir noteikts, ka *“darba ņēmējiem ir tiesības uz viņu personas datu aizsardzību darba sakarā”*. (2017/C 428/09, OV C 428, 13.12.2017., 10.–15. lpp.).

³³ Regulas 9. panta 2. punkta h) un i) apakšpunkts.

³⁴ Regulas 9. panta 2. punkta j) apakšpunkts.

³⁵ Regulas 87. pants.

³⁶ Regulas 86. pants.

³⁷ Regulas 90. pants.

³⁸ Regulas 9. panta 4. punkts.

³⁹ Spriedums lietā 94/77, *Fratelli Zerbone Snc / Amministrazione delle finanze dello Stato*, ECLI:EU:C:1978:17 un 101.

⁴⁰ Regulas 8. apsvērums.

tikai izņēmuma kārtā, un tam ir jābūt pamatotam, un to nedrīkst izmantot, lai Regulas tekstam pievienotu papildu nosacījumus vai interpretācijas.

Regulas interpretēšana ir Eiropas tiesu (valstu tiesu un pēdējā instancē — Eiropas Savienības Tiesas), nevis dalībvalstu likumdevēju ziņā. Tāpēc valsts likumdevējs nedrīkst ne kopēt Regulas tekstu, kad tas nav nepieciešams, ņemot vērā judikatūrā paredzētos kritērijus, ne interpretēt to vai pievienot papildu nosacījumus noteikumiem, kas ir tieši piemērojami saskaņā ar Regulu. Ja tā notiktu, dalībnieki Savienībā atkal sastaptos ar sadrumstalotību un nezinātu, kuri noteikumi viņiem ir jāpilda.

Šajā posmā tikai divas dalībvalstis jau ir pieņēmušas atbilstošo valsts tiesisko regulējumu⁴¹; pārējās dalībvalstis ir to likumdošanas procedūru dažādos posmos⁴², un tām ir izstrādāti laika grafiki tiesību aktu pieņemšanai līdz 2018. gada 25. maijam. Ir svarīgi dot dalībniekiem pietiekami daudz laika sagatavoties visu to prasību izpildei, kas tiem ir jāievēro.

Ja dalībvalstis neveic nepieciešamās darbības saskaņā ar Regulu, kavējas tās veikt vai izmanto Regulā paredzētās specifiskāciju klauzulas tā, ka tas ir pretrunā Regulai, Komisija izmantos visus tās rīcībā esošos instrumentus, tostarp pārkāpuma procedūras.

3.2. Datu aizsardzības iestādēm ir jānodrošina, ka jaunā neatkarīgā Eiropas Datu aizsardzības kolēģija ir pilnībā darboties spējīga

Ir būtiski, lai jaunā, ar Regulu izveidotā struktūra, Eiropas Datu aizsardzības kolēģija⁴³, kas ir 29. panta darba grupas pēctece, būtu pilnībā darboties spējīga no 2018. gada 25. maija.

Eiropas Datu aizsardzības uzraudzītājs, kas ir datu aizsardzības iestāde, kura ir atbildīga par ES iestāžu un struktūru uzraudzību, nodrošinās Eiropas Datu aizsardzības kolēģijas sekretariātu, lai vairotu sinerģijas un efektivitāti. Pēdējos mēnešos Eiropas Datu aizsardzības uzraudzītājs ir sācis nepieciešamos sagatavošanās darbus šai nolūkā.

Eiropas Datu aizsardzības kolēģija būs Eiropas datu aizsardzības procesa centrā. Tas veicinās datu aizsardzības tiesību konsekventu piemērošanu un nodrošinās spēcīgu pamatu sadarbībai starp datu aizsardzības iestādēm, tostarp ar Eiropas Datu aizsardzības uzraudzītāju. Eiropas Datu aizsardzības kolēģija ne vien sagatavos pamatnostādnes par to, kā interpretēt Regulas pamatjēdzienus, bet pie tās vērsīsies arī, lai pieņemtu saistošus lēmumus strīdos par pārrobežu apstrādi. Tas nodrošinās ES noteikumu vienotu piemērošanu un novērsīs iespēju, ka vienādi gadījumi dažādās dalībvalstīs tiek risināti atšķirīgi.

Tāpēc netraucēta un efektīva Eiropas Datu aizsardzības kolēģijas darbība ir priekšnosacījums, lai sistēma kopumā darbotos labi. Vairāk nekā jebkad agrāk Eiropas Datu aizsardzības kolēģijai būs jāiedibina kopēja datu aizsardzības kultūra visās valstu datu aizsardzības iestādēs, lai nodrošinātu, ka Regulas noteikumi tiek interpretēti konsekventi. Regula veicina datu aizsardzības iestāžu sadarbību, piešķirot tām instrumentus, lai sadarbība būtu efektīva un

⁴¹ Austrija (http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdf); Vācija

(https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D#_bgbl_%2F%2F%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D_1513091793362).

⁴² Pārskatu par likumdošanas procesa stāvokli dažādās dalībvalstīs skatīt vietnē <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3461>.

⁴³ Eiropas Datu aizsardzības kolēģija būs ES struktūra ar juridiskas personas statusu, kas ir atbildīga par Regulas konsekventu piemērošanu. Tajā darbosies katras datu aizsardzības iestādes vadītājs un Eiropas Datu aizsardzības uzraudzītājs vai to pārstāvji.

lietderīga: jo īpaši tās varēs veikt kopīgus pasākumus, pieņemot lēmumus pēc vienošanās un novērst atšķirības, kādas kolēģijā var rasties attiecībā uz Regulas interpretāciju, izmantojot atzinumus un saistošus lēmumus. Komisija aicina datu aizsardzības iestādes pieņemt šīs izmaiņas un pielāgot savu darbību, finansējumu un darba kultūru, lai tās spētu izmantot jaunās tiesības un pildīt jaunus pienākumus.

3.3. Dalībvalstīm ir jānodrošina nepieciešamie finanšu un cilvēkresursi valsts datu aizsardzības iestādēm

Pilnībā neatkarīgu uzraudzības iestāžu izveide katrā dalībvalstī ir būtiska, lai nodrošinātu fizisko personu aizsardzību saistībā ar viņu personas datu apstrādi ES⁴⁴. Uzraudzības iestādes nespēj efektīvi nodrošināt personu tiesības un brīvības, ja vien tās nedarbojas pilnībā neatkarīgi. Ja neizdodas nodrošināt to neatkarību un efektīvu pilnvaru izmantošanu, tad tas negatīvi ietekmē datu aizsardzības tiesību aktu izpildi⁴⁵.

Regulā ir kodificēta prasība visām datu aizsardzības iestādēm rīkoties pilnīgi neatkarīgi⁴⁶. Tas pastiprina valsts datu aizsardzības iestāžu neatkarību un nodrošina tām vienotas pilnvaras visā ES, lai tām būtu pienācīgas iespējas efektīvi risināt sūdzības, veikt efektīvu izmeklēšanu, pieņemot saistošus lēmumus un piemērot efektīvas un atturošas sankcijas. Tām ir piešķirtas arī pilnvaras piemērot administratīvus naudas sodus pārzīņiem un apstrādātājiem apmērā līdz 20 miljoniem euro vai, uzņēmuma gadījumā, līdz 4 % no tā kopējā visā pasaulē iepriekšējā finanšu gadā gūtā gada apgrozījuma atkarībā no tā, kuras summas apmērs ir lielāks.

Datu aizsardzības iestādes ir dabiski sarunu partneri un pirmais kontaktpunkts plašākai sabiedrībai, uzņēmumiem un valsts pārvaldes iestādēm, lai uzdotu jautājumus saistībā ar Regulu. Datu aizsardzības iestāžu pienākums ir informēt pārzīņus un apstrādātājus par to pienākumiem un uzlabot plašākas sabiedrības informētību par riskiem, noteikumiem, garantijām un tiesībām saistībā ar datu apstrādi. Taču tas nenozīmē, ka pārzīņiem un apstrādātājiem ir jāsapņūda, ka datu aizsardzības iestādes sniegs tādas pielāgotas, individuālas juridiskās konsultācijas, kādas var sniegt tikai jurists vai datu aizsardzības speciālists.

Tāpēc valsts datu aizsardzības iestādēm ir svarīga loma, taču salīdzinošā nelīdzsvarotība starp cilvēkresursiem un finanšu resursiem, kas tām piešķirti dažādās dalībvalstīs, var apdraudēt to efektivitāti un pilnīgo neatkarību, kas noteikta Regulā. Turklāt tas var negatīvi ietekmēt veidu, kā datu aizsardzības iestādes var izmantot savas pilnvaras, piemēram, izmeklēšanas pilnvaras. Dalībvalstis tiek aicinātas pildīt savu juridisko pienākumu piešķirt savai valsts datu aizsardzības iestādei cilvēkresursus, tehniskos un finanšu resursus, telpas un infrastruktūru, kas nepieciešami efektīvai tās uzdevumu izpildei un pilnvaru īstenošanai⁴⁷.

3.4. Uzņēmumiem, valsts pārvaldes iestādēm un citām organizācijām, kas apstrādā datus, ir jāgatavojas piemērot jaunus noteikumus

Regulā nav būtiski mainīti 1995. gadā ieviestie datu aizsardzības regulējuma pamatjēdzieni un principi. Tam vajadzētu nozīmēt, ka lielākajai daļai pārzīņu un apstrādātāju – ar nosacījumu, ka viņi jau šobrīd ir nodrošinājuši atbilstību spēkā esošajiem ES tiesību aktiem datu

⁴⁴ Regulas 117. apsvēruma; un iepriekš jau minēts Direktīvas 95/46 62. apsvērumā.

⁴⁵ Komisijas paziņojums Eiropas Parlamentam un Padomei par Darba programmas labākai Datu aizsardzības direktīvas īstenošanai gaitu, COM(2007) 87 galīgā redakcija, 2007. gada 7. marts.

⁴⁶ Regulas 52. pants.

⁴⁷ Regulas 52. panta 4. punkts.

aizsardzības jomā, - nebūs jāveic būtiskas izmaiņas datu apstrādes darbībās, lai nodrošinātu atbilstību Regulai.

Regula visvairāk ietekmē operatorus, kuru uzņēmējdarbības pamatā ir datu apstrāde un/vai darbs ar sensitīviem datiem. Tā ietekmē arī tos, kas regulāri un sistemātiski veic novērošanu plašā mērogā. Šiem operatoriem, visticamāk, būs jāieceļ datu aizsardzības speciālists, jāveic novērtējums par ietekmi uz datu aizsardzību un jāziņo par datu aizsardzības pārkāpumiem, ja pastāv risks personu tiesībām un brīvībām. Turpretim operatoriem, jo īpaši MVU, kas savas pamatdarbības ietvaros neveic augsta riska apstrādi, parasti netiks piemērotas šīs specifiskās Regulas saistības.

Ir svarīgi, lai pārziņi un apstrādātāji vispusīgi pārskatītu savu datu politikas ciklu, lai precīzi noskaidrotu, kādi dati ir viņu rīcībā, kādā nolūkā un uz kāda juridiskā pamata (piem., mākoņdatošanas vide; operatori finanšu nozarē). Tiem ir jānovērtē arī noslēgtie līgumi, jo īpaši tie, kas noslēgti starp pārziņiem un apstrādātājiem, starptautiskās pārsūtīšanas iespējas un vispārējā pārvaldība (kādi IT un organizatoriskie pasākumi ir vajadzīgi), tostarp jāieceļ datu aizsardzības speciālists. Būtisks šā procesa elements ir nodrošināt, ka šādā pārskatīšanā ir iesaistīts augstākais vadības līmenis, sniedzot pienesumu, un ka to regulāri atjaunina un ņem vērā, ieviešot izmaiņas uzņēmuma datu politikā.

Šai nolūkā daži operatori izmanto atbilstības kontrolosarakstus (iekšējos vai ārējos), lūdz padomu konsultantu firmām un juristu birojiem un meklē produktus, kas var nodrošināt atbilstību integrētās datu aizsardzības un datu aizsardzības pēc noklusējuma prasībām. Katrā nozarē ir jāizstrādā kārtība, kas piemērota konkrētās jomas būtībai un pielāgota uzņēmējdarbības modelim.

Uzņēmumi un citas organizācijas, kas pārstrādā datus, varēs gūt labumu no Regulā paredzētajiem jaunajiem instrumentiem, piemēram, rīcības kodeksiem un sertifikācijas mehānismiem, izmantojot tos kā elementu, lai demonstrētu atbilstību. Tās ir augšupējas pieejas, kas izriet no uzņēmēju aprindām, biedrībām vai citām organizācijām, kuras pārstāv pārziņu vai apstrādātāju kategorijas un atspoguļo paraugpraksi, svarīgas norises noteiktā nozarē vai var informēt par datu aizsardzības līmeni, kas nepieciešams noteiktiem produktiem un pakalpojumiem. Regulā noteikts vienkāršots noteikumu kopums šādiem mehānismiem, vienlaikus ņemot vērā faktisko tirgus situāciju (piem., sertifikācija, ko veic sertifikācijas struktūra vai datu aizsardzības iestāde).

Taču, kamēr lielie uzņēmumi aktīvi gatavojas jauno noteikumu piemērošanai, daudzi MVU vēl arvien nav informēti par gaidāmajiem datu aizsardzības noteikumiem.

Īsāk sakot, operatoriem ir jā sagatavojas un jāpielāgojas jaunajiem noteikumiem un jāuztver Regula kā:

- iespēja sakārtot situāciju attiecībā uz to, kādus personas datus tie apstrādā un kā pārvalda šo procesu;
- pienākums izstrādāt produktus, kas ir vērsti uz privātuma un datu aizsardzību, un nodibināt jaunas attiecības ar saviem klientiem, balstoties uz pārredzamību un uzticību; un
- iespēja pārskatīt attiecības ar datu aizsardzības iestādēm, īstenojot pārskatatbildību un proaktīvu izpildi.

3.5. Ir jāinformē ieinteresētās personas, jo īpaši iedzīvotāji un mazie un vidējie uzņēmumi

Regulas panākumi ir atkarīgi no tā, ka visas puses, ko ietekmē jaunie noteikumi (uzņēmēju aprindas un citas organizācijas, kas apstrādā datus, valsts sektors un iedzīvotāji), ir pienācīgi informētas. Valstu līmenī informētības veicināšana un pirmā kontaktpunkta nodrošināšana pārziņiem, apstrādātājiem un personām, ir galvenokārt datu aizsardzības iestāžu pienākums. Datu aizsardzības iestādes kā datu aizsardzības noteikumu izpildītāji savā teritorijā vislabāk var paskaidrot ar Regulu ieviestās izmaiņas uzņēmumiem un valsts sektoram, kā arī iepazīstināt iedzīvotājus ar viņu tiesībām.

Datu aizsardzības iestādes ir sākušas informēt ieinteresētās personas saskaņā ar konkrētās valsts pieeju. Dažas organizē seminārus ar valsts pārvaldes iestāžu līdzdalību, tostarp reģionālā un vietējā līmenī, un vada darbseminārus, sadarbojoties ar dažādām uzņēmējdarbības nozarēm, lai veicinātu informētību par Regulas galvenajiem noteikumiem. Dažas iestādes organizē īpašas apmācību programmas datu aizsardzības speciālistiem. Vairums iestāžu nodrošina informatīvus materiālus dažādos formātos savā tīmekļa vietnē (kontROLSaraksti, video utt.).

Taču pagaidām iedzīvotājiem vēl nav pietiekami plaša līmeņa izpratnes par izmaiņām un uzlabotajām tiesībām, ko radīs jaunie datu aizsardzības noteikumi. Datu aizsardzības iestāžu uzsāktā apmācību un informētības uzlabošanas iniciatīva ir jāturpina un jāpastiprina, īpaši pievēršoties MVU. Turklāt valsts nozaru pārvaldes iestādes var atbalstīt datu aizsardzības iestāžu darbību un atkarībā no to ieguldījuma pašas vērsties pie dažādām ieinteresētajām personām.

4. TURPMĀKIE PASĀKUMI

Tuvākajos mēnešos Komisija turpinās aktīvi atbalstīt visus dalībniekus, gatavojoties Regulas piemērošanai.

a) Darbs ar dalībvalstīm

Komisija turpinās sadarboties ar dalībvalstīm, gatavojoties norisēm 2018. gada maijā. No 2018. gada maija Komisija uzraudzīs, kā dalībvalstis piemēro jaunus noteikumus un vajadzības gadījumā veic atbilstošu rīcību.

b) Jaunas norādes tiešsaistē visās ES valodās un informētības veicināšanas pasākumi

Komisija padarīs pieejamus praktiskus norādījumu materiālus⁴⁸, lai palīdzētu uzņēmumiem, jo īpaši MVU, valsts iestādēm un sabiedrībai izpildīt jaunus datu aizsardzības noteikumus un gūt labumu no tiem.

Norādes ir sniegtas praktiska tiešsaistes instrumenta veidā visās ES valodās. Tiešsaistes instrumentu regulāri aktualizēs, un tas ir paredzēts trim galvenajām mērķa grupām — iedzīvotājiem, uzņēmumiem (jo īpaši MVU) un citām organizācijām, kā arī valsts pārvaldes iestādēm. Tajā ir ietverti jautājumi un atbildes, kas izvēlēti atbilstoši atgriezeniskajai saitei, kura saņemta no ieinteresētajām personām, papildinot ar praktiskiem piemēriem un saitēm uz dažādiem informācijas avotiem (piem., Regulas pantiem; 29. panta darba grupas / Eiropas Datu aizsardzības kolēģijas pamatnostādņēm; un dalībvalstu līmenī izstrādātiem materiāliem).

⁴⁸ Norādes veicinās labāku izpratni par ES datu aizsardzības noteikumiem, taču juridisks spēks ir tikai Regulas tekstam. Attiecīgi tikai Regula var personām radīt tiesības un pienākumus.

Komisija šo instrumentu regulāri atjauninās, pievienojot jautājumus un atjaunojot atbildes, pamatojoties uz saņemto atgriezenisko saiti, kā arī ņemot vērā jaunas problēmas, kas izriet piemērošanas rezultātā.

Norādījumus popularizēs informācijas kampaņā un izplatīšanas darbībās visās dalībvalstīs, īpaši pievēršoties uzņēmumiem un sabiedrībai.

Tā kā regulā paredzēts augstāks individuālo tiesību līmenis, Komisija turklāt veiks izpratnes veidošanas pasākumus un piedalīsies pasākumos dalībvalstīs, lai informētu iedzīvotājus par regulas sniegto labumu un ietekmi.

c) Finansiālais atbalsts valstu kampaņām un informētības veicināšanai

Komisija atbalsta informētības veicināšanas un atbildības centienus valstu līmenī, piešķirot dotācijas, ko var izmantot, lai nodrošinātu apmācību datu aizsardzības iestādēs, valsts pārvaldes iestādēs, juridisko profesiju pārstāvjiem un datu aizsardzības speciālistiem⁴⁹ un iepazīstinātu tos ar Regulu.

Aptuveni 1,7 miljoni euro tiks piešķirti sešiem saņēmējiem, kas aptver vairāk nekā pusi ES dalībvalstu. Finansējuma mērķauditorija būs valsts iestādes, tostarp pašvaldības un valsts iestāžu un datu aizsardzības speciālisti, un privātais sektors, tiesneši un juristi. Dotācijas izmantos, lai izstrādātu apmācību materiālus datu aizsardzības iestādēm, datu aizsardzības speciālistiem un citiem profesionāļiem, kā arī pasniedzēju apmācības programmām.

Komisija ir izsludinājusi arī aicinājumu iesniegt priekšlikumus, kas ir īpaši paredzēti datu aizsardzības iestādēm. Tam ir atvēlēts kopējais budžets 2 miljonu euro apmērā, un tas nodrošinās atbalstu, lai sasniegtu ieinteresētās personas⁵⁰. Mērķis ir nodrošināt 80 % no līdzfinansējuma pasākumiem, kurus datu aizsardzības iestādes veiks 2018.–2019. gadā, lai sekmētu uzņēmumu, jo īpaši MVU, informētību un atbildētu uz to prasījumiem. Šo finansējumu var izmantot arī tam, lai veicinātu plašākas sabiedrības informētību.

d) Novērtēt, vai ir nepieciešamība izmantot Komisijas pilnvarojumu

Regula⁵¹ ļauj Komisijai izdot īstenošanas vai deleģētos aktus, lai papildus atbalstītu jauno noteikumu īstenošanu. Komisija šīs pilnvaras izmantos tikai tad, ja būs nepārprotami pierādīta pievienotā vērtība un atbilstoši atgriezeniskajai saitei no konsultācijām ar ieinteresētajām personām. Jo īpaši Komisija aplūkos sertificēšanas jautājumu, pamatojoties uz pētījumu, kas pasūtīts ārējiem ekspertiem, un ieguldījumu un padomiem, kurus par šo jautājumu sniegs

⁴⁹ Dotācijas piešķirtas saskaņā ar 2016. gada programmu “Tiesības un pilsonība”

<https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/rec/calls/rec-data-2016.html#c.topics=callIdentifier/t/REC-DATA-2016/1/1/1/default-group&callStatus/t/Forthcoming/1/1/0/default-group&callStatus/t/Open/1/1/0/default-group&callStatus/t/Closed/1/1/0/default-group&+identifier/desc>.

⁵⁰ <http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/rec/topics/rec-rdat-trai-ag-2017.html>

⁵¹ Deleģētais akts par informāciju, kas sniedzama, izmantojot ikonas, un procedūras standartizētu ikonu nodrošināšanai (Regulas 12. panta 8. punkts); Deleģētais akts par prasībām, kas jāņem vērā attiecībā uz sertifikācijas mehānismiem (Regulas 43. panta 8. punkts); Īstenošanas akts, ar ko nosaka tehniskos standartus sertifikācijas mehānismiem un datu aizsardzības zīmogiem un marķējumiem, un mehānismus minēto sertifikācijas mehānismu, zīmogu un marķējumu popularizēšanai un atzīšanai (Regulas 43. panta 9. punkts); Īstenošanas akts par formātu un procedūram informācijas apmaiņai starp pārziniem, apstrādātājiem un uzraudzības iestādēm attiecībā uz saistošiem uzņēmuma noteikumiem (Regulas 47. panta 3. punkts); Īstenošanas akts par formātu un procedūram savstarpējai palīdzībai un informācijas apmaiņai starp uzraudzības iestādēm, izmantojot elektroniskus līdzekļus (Regulas 62. panta 9. punkts un 67. pants).

Regulas daudzpusējo ieinteresēto personu grupa, kas izveidota 2017. gada nogalē. Šajā kontekstā nozīmīgs būs arī Eiropas Tīklu un informācijas drošības aģentūras (*ENISA*) veiktais darbs kibernetikas drošības jomā.

e) Regulas integrēšana EEZ līgumā

Komisija turpinās darbu ar trim EBTA valstīm (Islandi, Lihtenšteinu un Norvēģiju) Eiropas Ekonomikas zonā (EEZ), lai integrētu Regulu EEZ līgumā⁵². Personas datu aprīte varēs brīvi notikt starp ES un EEZ valstīm tāpat kā starp ES dalībvalstīm tikai pēc tam, kad Regula būs integrēta EEZ līgumā.

f) Apvienotās Karalistes izstāšanās no ES

Ņemot vērā sarunas par izstāšanās līgumu starp ES un Apvienoto Karalisti saskaņā ar Līguma par Eiropas Savienību 50. pantu, Komisija turpinās virzīties uz mērķi, lai panāktu, ka Savienības personas datu aizsardzības regulējumu, kas būs spēkā dienā pirms izstāšanās datuma, turpinās piemērot Apvienotajā Karalistē attiecībā uz personas datiem, kas apstrādāti pirms izstāšanās datuma⁵³. Piemēram, attiecīgajām personām vēl arvien vajadzētu būt tiesībām būt informētām, piekļuves tiesībām, labošanas, dzēšanas tiesībām, tiesībām uz apstrādes ierobežošanu, datu pārnesamību, kā arī tiesībām iebilst pret apstrādi un nebūt pakļautām lēmumiem, kas balstīti tikai uz automatisku apstrādi, saskaņā ar attiecīgajām Savienības tiesību normām, kas ir spēkā izstāšanās datumā. Iepriekš minētie personas dati ir jāuzglabā ne ilgāk kā nepieciešams nolūkiem, kuros personas dati tika apstrādāti.

Attiecībā uz izstāšanās datumu un atkarībā no jebkādiem pārejas nosacījumiem, kas var būt iekļauti iespējamajā izstāšanās līgumā, Apvienotajā Karalistē tiks piemēroti Regulas noteikumi par personas datu nosūtīšanu uz trešām valstīm⁵⁴.

g) Izvērtējums 2019. gada maijā

Pēc 2018. gada 25. maija Komisija cieši novēros jauno noteikumu piemērošanu un būs gatava rīkoties, ja radīsies kādas būtiskas problēmas. Gadu pēc Regulas piemērošanas sākuma (2019) Komisija organizēs pasākumu, lai izvērtētu dažādu ieinteresēto personu pieredzi Regulas īstenošanas jomā. Tā rezultāti tiks izmantoti ziņojumā, kas Komisijai ir jāizstrādā līdz 2020. gada maijam par Regulas novērtējumu un pārskatu. Šajā ziņojumā tiks pievērsta īpaša uzmanība starptautiskai datu nodošanai un sadarbības un konsekvences regulējumam, kas attiecas uz datu aizsardzības iestāžu darbu.

Secinājums

25. maijā visā ES stāsies spēkā jauns vienots datu aizsardzības noteikumu kopums. Jaunais regulējums nodrošinās būtiskus labumus personām, uzņēmumiem, valsts pārvaldes iestādēm un citām organizācijām. Tā ir arī iespēja ES kļūt par pasaules līderi personas datu aizsardzības jomā. Taču reforma var būt veiksmīga tikai tad, ja visas iesaistītās puses pieņem savus pienākumus un tiesības.

⁵² Informāciju par pašreizējo stāvokli sk. <http://www.efta.int/eea-lex/32016R0679>.

⁵³ https://ec.europa.eu/commission/publications/position-paper-use-data-and-protection-information-obtained-or-processed-withdrawal-date_en

⁵⁴ Sk. Komisijas Paziņojumu ieinteresētajām personām: Apvienotās Karalistes izstāšanās un ES noteikumi datu aizsardzības jomā (http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245).

Kopš Regulas pieņemšanas 2016. gada maijā Komisija ir aktīvi sadarbojusies ar visām iesaistītajām pusēm — valdībām, valstu iestādēm, uzņēmumiem, pilsonisko sabiedrību — saistībā ar jauno noteikumu piemērošanu. Ir ieguldīts nozīmīgs darbs, lai nodrošinātu plašu informētību un pilnīgu sagatavotību, tomēr joprojām ir daudz kas jāpaveic. Sagatavošanās darbi dažādās dalībvalstīs un starp dažādām ieinteresētajām personām progresē dažādā ātrumā. Turklāt zināšanas par ieguvumiem un iespējām, ko sniegs jaunie noteikumi, nav izplatītas vienmērīgi. Īpaši jāveicina informētība un atbilstības centieni MVU.

Tāpēc Komisija aicina visas iesaistītās puses pastiprināt pašreizējo darbu, lai nodrošinātu jauno noteikumu konsekventu piemērošanu un interpretāciju visā ES un uzlabotu gan uzņēmumu, gan iedzīvotāju informētību. Komisija šos centienus atbalstīs ar finansējumu un administratīvo atbalstu un palīdzēs vairojot vispārējo informētību, jo īpaši ieviešot tiešsaistes norāžu instrumentu kopumu.

Mūsdienu ekonomikā dati kļūst ārkārtīgi svarīgi, un tiem iedzīvotāju ikdienas dzīvē ir liela nozīme. Jaunie noteikumi piedāvā unikālu iespēju gan uzņēmumiem, gan sabiedrībai. Uzņēmumi, jo īpaši mazie, varēs gūt labumu no vienotā noteikumu kopuma, kas ir draudzīgs inovācijām, un sakārtot situāciju attiecībā uz personas datiem, lai atgūtu patērētāju uzticību un izmantotu to kā konkurences priekšrocību visā ES. Iedzīvotāji varēs gūt labumu no personas datu spēcīgākas aizsardzības un saņemt labāku kontroli pār to, kā uzņēmumi lieto datus.

Modernajā pasaulē ar plaukstošu digitālo ekonomiku Eiropas Savienībai, tās iedzīvotājiem un uzņēmumiem ir jābūt pilnībā gataviem izmantot priekšrocības un izprast datu ekonomikas sekas. Jaunā regula piedāvā nepieciešamos instrumentus, kas ļaus Eiropai būt gatavai 21. gadsimtam.

Komisija īstenoš šādas darbības:

Attiecībā uz dalībvalstīm:

- Komisija turpinās sadarboties ar dalībvalstīm, lai veicinātu Regulas piemērošanas konsekveni un mazinātu sadrumstalotību, ņemot vērā dalībvalstīm sniegtās specifikāciju iespējas saskaņā ar jauno regulējumu;
- pēc 2018. gada maija Komisija cieši novēros Regulas piemērošanu dalībvalstīs un veiks nepieciešamos pasākumus, tostarp izmantos pārkāpuma procedūru.

Attiecībā uz datu aizsardzības iestādēm:

- līdz 2018. gada maijam Komisija atbalstīs datu aizsardzības iestāžu darbu 29. panta darba grupas kontekstā un pārejā uz nākamo Eiropas Datu aizsardzības kolēģiju; pēc 2018. gada maija Komisija veicinās Eiropas Datu aizsardzības kolēģijas darbu;
- 2018.–2019. gadā Komisija līdzfinansēs (kopējais budžets 2 miljoni euro) informētības veicināšanas darbības, ko īstenoš datu aizsardzības iestādes valstu līmenī (projekti, ko īstenoš, sākot no 2018. gada vidus).

Attiecībā uz ieinteresētajām personām:

- Komisija uzsāks tiešsaistes praktisko norādījumu instrumenta darbību, kurā ietilps jautājumi un atbildes, kuru mērķauditorija ir iedzīvotāji, uzņēmumi un valsts pārvaldes iestādes. Komisija plāno veicināt šos norādījumus mērķauditorijai informācijas

kampaņā, kas paredzēta uzņēmumiem un sabiedrībai, līdz 2018. gada maijam un vēlāk;

- 2018. gadā un pēc tam Komisija turpinās aktīvi sadarboties ar ieinteresētajām personām, jo īpaši caur daudzpusējo ieinteresēto personu grupu, attiecībā uz Regulas īstenošanu un informētības līmeni par jaunajiem noteikumiem.

Attiecībā uz visiem dalībniekiem:

- 2018.–2019. gadā Komisija izvērtēs nepieciešamību izmantot savas pilnvaras pieņemt deleģētos vai īstenošanas aktus;
- 2019. gada maijā Komisija novērtēs Regulas īstenošanas gaitu un 2020. gadā ziņos par jauno noteikumu piemērošanu.