Atzinums 23/2018 par Komisijas priekšlikumu “Par Eiropas elektronisko pierādījumu sniegšanas un saglabāšanas rīkojumiem elektronisko pierādījumu gūšanai krimināllietās” (70. panta 1. punkta b) apakšpunkts)

Pieņemts 2018. gada 26. septembrī

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Saturs

Eiropas Datu aizsardzības kolēģija,

ņemot vērā Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regulas (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, 70. panta 1. punkta b) apakšpunktu,

IR PIEŅĒMUSI ŠĀDU ATZINUMU.

Ievads

2018. gada aprīlī Komisija iesniedza priekšlikumu regulai par Eiropas elektronisko pierādījumu sniegšanas un saglabāšanas rīkojumiem elektronisko pierādījumu gūšanai krimināllietās un priekšlikumu direktīvai, ar ko paredz saskaņotus noteikumus juridisko pārstāvju iecelšanai ar mērķi iegūt pierādījumus kriminālprocesā. Šie abi priekšlikumi, COM(2018) 225 *final* un COM(2018) 226 *final*, ir savstarpēji papildinoši. Komisijas vispārējais mērķis ir uzlabot sadarbību starp dalībvalstu iestādēm un pakalpojumu sniedzējiem, tostarp tādiem, kuri atrodas ārpus ES, un ierosināt risinājumus problēmai, kas saistīta ar jurisdikcijas noteikšanu un izpildes panākšanu kibertelpā.

Regulas projektā ir paredzēti noteikumi un procedūras, kas piemērojami elektronisko sakaru pakalpojumu sniedzējiem attiecībā uz elektronisko pierādījumu sniegšanas un saglabāšanas rīkojumu izdošanu, apkalpošanu un izpildes panākšanu, savukārt direktīvas projektā paredzēti minimālie noteikumi, kā iecelt juridisko pārstāvi pakalpojumu sniedzējiem, kas nav reģistrēti ES.

2017. gada novembrī[1], pirms vēl Komisija nāca klajā ar savu priekšlikuma projektu, 29. panta darba grupa (DG29) atgādināja par nepieciešamību nodrošināt jebkāda tiesību akta priekšlikuma pilnīgu atbilstību jo īpaši spēkā esošajam ES datu aizsardzības *acquis*, kā arī ES tiesību aktiem un judikatūrai kopumā.

Jo īpaši DG29 brīdināja par ierobežojumiem attiecībā uz tiesībām uz datu aizsardzību un privātumu saistībā ar datiem, kurus apstrādā telekomunikāciju un informācijas sabiedrības pakalpojumu sniedzēji, jo īpaši, kad tos tālāk apstrādā tiesībaizsardzības iestādes, un atgādināja par nepieciešamību nodrošināt jebkura ES instrumenta konsekvenci attiecībā uz esošo Eiropas Padomes Budapeštas Konvenciju par kibernoziegumiem un ES direktīvu par Eiropas izmeklēšanas rīkojumu (EIR), kā arī ieteica precizēt attiecīgos procesuālos noteikumus, kas reglamentē piekļuvi e-pierādījumiem valsts un ES līmenī, lai nodrošinātu, ka jaunais instruments nesniegtu iestādēm tādas jaunas pilnvaras, kuras tām nebūtu iekšēji. Papildus šīm vispārīgajām piezīmēm DG29 komentēja likumdošanas iespējas, ko Komisija šajā laikā izskatīja saistībā ar attiecīgo datu kategorijām un atbilstošajiem aizsardzības pasākumiem attiecībā uz piekļuvi tiem, par iespēju izmantot elektronisko pierādījumu sniegšanas rīkojumus/pieprasījumus, lai pakalpojumu sniedzējiem uzliktu saistības sniegt datus, kas atrodas ārpus ES, kā arī par materiālajiem un procesuālajiem nosacījumiem, kas nepieciešami, lai nodrošinātu tiešu piekļuvi datiem.

Saņemot konkrētus priekšlikumus e-pierādījumiem, EDAK vēlas sniegt padziļinātu ierosināto juridisko instrumentu analīzi no datu aizsardzības viedokļa.

[1] Skatīt DG29 paziņojumu (http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801).

1. Regulas priekšlikuma juridiskais pamats (LESD 82. pants)

Regulas par e-ierādījumiem projektam ierosinātais juridiskais pamats ir LESD 82. panta 1. punkts attiecībā uz tiesu iestāžu sadarbību krimināllietās, ar kuru nosaka:

> *"1.* Savienībā tiesu iestāžu sadarbība krimināllietās pamatojas uz tiesas spriedumu un lēmumu savstarpējas atzīšanas principu, un tā ietver dalībvalstu normatīvo aktu tuvināšanu jomās, kas minētas 2. punktā un 83. pantā.
>
> Eiropas Parlaments un Padome saskaņā ar parasto likumdošanas procedūru paredz pasākumus, lai:
>
> a) ieviestu noteikumus un procedūras, kuru mērķis ir visu veidu spriedumu un tiesas lēmumu atzīšana visā Savienībā,
>
> b) novērstu un atrisinātu jurisdikcijas kolīzijas dalībvalstu starpā,
>
> c) veicinātu tiesu iestāžu un tiesu personāla mācības,
>
> *d) dalībvalstu tiesu iestāžu un līdzvērtīgu iestāžu starpā atvieglotu sadarbību saistībā ar kriminālprocesu un lēmumu izpildi."*

Kā Komisija uzsvēra savā priekšlikumiem pievienotajā ietekmes novērtējumā, "82. panta 1. punktā noteikts, ka tiesu iestāžu sadarbība krimināllietās balstīta uz savstarpējas atzīšanas principu. Šis juridiskais pamats attiektos uz iespējamiem tiesību aktiem par tiešu sadarbību ar pakalpojumu sniedzējiem, kuros izdevēja dalībvalsts tieši vērstos pie struktūras (pakalpojumu sniedzēja) izpildvalstī un pat uzliktu tai saistības. Līdz ar to rastos jauna dimensija abpusējas atzīšanas jomā, kas pārsniegtu tradicionālo tiesisko sadarbību Savienībā, kas līdz šim ir balstīta uz procedūrām, kurās iesaistītas divas tiesu iestādes, viena — izdevējvalstī un otra — izpildvalstī" (izcēlums pievienots).

Ņemot vērā to, ka šī juridiskā pamata izmantošana saistībā ar tiešajiem pieprasījumiem starp valsts iestādēm un privātām pusēm ir jaunums, EDAK pauž nožēlu, ka Komisija nav veikusi papildu analīzi un novērtējumu.

Patiesi, kā darba grupa jau savā iepriekšējā paziņojumā uzsvēra, EDAK joprojām apšauba šā juridiskā pamata piemērotību, ko atbalsta EST analīze un EST ģenerāladvokāta atzinums 1/15. Starp notikumiem saistībā ar 82. panta kā juridisku pamatu spēkā esību PNR nolīgumam starp ES un Kanādu, minams Tiesas atzinums, ka Kanādas kompetentā iestāde "nav nedz tiesu iestāde, nedz arī līdzvērtīga iestāde"[2]. Saistībā ar priekšlikumiem par e-pierādījumiem viens no Komisijas izvirzītajiem galvenajiem mērķiem, šķiet, ir izvairīties no "pārāk liela apgrūtinājuma" tiesiskajā sadarbībā. Līdz ar to priekšlikums ir balstīts uz principu, ka sadarbībai būtu jānotiek starp iestādi un pakalpojumu sniedzēju, nevis starp divām iestādēm. Paredzētā procedūra galvenokārt paredz, ka privātās struktūras pamatā ir saņēmēja puse un atbild uz pieprasījumiem, kurus izdod tiesu iestādes.

EDAK atzīmē, ka elektronisko pierādījumu sniegšanas vai saglabāšanas rīkojumu izpildes process var nozīmēt saņēmējas iestādes iesaistīšanos situācijā, kad saņēmējs pakalpojumu sniedzējs nepilda savas saistības, un tādēļ rodas nepieciešamība pēc rīkojuma *ex post* izpildes panākšanas. Tomēr, tā kā procedūras galvenais mērķis ir neiesaistīt saņēmēju iestādi, EDAK šaubās, vai šī papildprocedūra var attaisnot 82. panta kā vienīgā juridiskā pamata izmantošanu.

[2] Skatīt šajā lietā Atzinuma 1/15 103. punktu un ģenerāladvokāta atzinuma 108. punktu.

Tāpēc EDAK uzskata, ka, lai 82. pantu varētu izmantot kā juridisku pamatu, galvenajiem sadarbības procedūras posmiem jānotiek starp divām tiesu iestādēm, un šāda veida sadarbībai būtu jāizmanto vēl viens juridiskais pamats.

2. E-pierādījumu nepieciešamība salīdzinājumā ar *MLAT* un EIR

EDAK atzīmē, ka Komisija ir apņēmusies pārskatīt šķēršļus kriminālizmeklēšanai, jo īpaši attiecībā uz piekļuvi elektroniskajiem pierādījumiem. Paskaidrojuma rakstā Komisija sniedz priekšlikuma kontekstu un uzsver elektroniskajiem pierādījumiem raksturīgo nepastāvību, to starptautisko dimensiju, kā arī nepieciešamību pielāgot sadarbības mehānismu digitālajam laikmetam. Priekšlikumi regulai un direktīvai par elektronisko pierādījumu nodošanu un piekļuvi tiem nav paredzēti, lai aizstātu iepriekšējos sadarbības instrumentus krimināllietās, piemēram, Budapeštas konvenciju, savstarpējas tiesiskās palīdzības līgumu (*MLAT*) vai Eiropas izmeklēšanas rīkojumu (EIR direktīva). Saskaņā ar Komisijas teikto e-pierādījumu priekšlikumi ir vērsti uz to, lai uzlabotu tiesisko sadarbību krimināllietās starp iestādēm un pakalpojumu sniedzējiem Eiropas Savienībā, kā arī sadarbību ar trešām valstīm, jo īpaši ar Amerikas Savienotajām Valstīm.

Tā kā šie jaunie papildu instrumenti būs īpaši paredzēti piekļuvei elektroniskajiem pierādījumiem un to nodošanai, EDAK novērtēs instrumentu pievienoto vērtību attiecībā uz EIR direktīvu un *MLAT*.

a) E-pierādījumu nepieciešamība, salīdzinot ar aizsardzības pasākumiem saskaņā ar EIR un *MLAT*

Galvenais arguments, ko Komisija izvirzīja par labu priekšlikumiem par e-pierādījumiem, ir elektronisko pierādījumu, kurus glabā un/vai tur citā jurisdikcijā reģistrēti pakalpojumu sniedzēji, nodrošināšanas un iegūšanas procesa paātrinājums.

Tomēr EDAK izsaka nožēlu, ka ietekmes novērtējumā netika parādīta nepieciešamība pēc jauna instrumenta, ar ko organizēt piekļuvi elektroniskajiem pierādījumiem. Patiesībā priekšlikumos trūkst pamatojuma, ka e-pierādījumu priekšlikuma mērķa sasniegšanai nav iespējams izmantot līdzekļus mazāk apgrūtinošiem līdzekļiem, kā arī būtu vēlams apsvērt alternatīvus risinājumus. Piemēram, varēja būt izskatīta iespēja grozīt un uzlabot EIR direktīvu, kas arī atbilstu EIR direktīvā ietvertajai konkrētajai prasībai izvērtēt nepieciešamību grozīt tekstu līdz 2019. gada 21. maijam[3]. Vēl viena iespēja bija paredzēt elektronisko pierādījumu saglabāšanas rīkojumu izmantošanu, lai iesaldētu datus tik ilgi, kamēr tiks izdots oficiāls pieprasījums, pamatojoties uz *MLAT*. Šīs iespējas ļautu saglabāt šajos instrumentos paredzētos aizsardzības pasākumus, vienlaikus nodrošinot, ka pieprasītie personas dati netiek dzēsti.

EDAK atzīmē, ka EIR direktīvā noteiktie termiņi, ir garāki nekā priekšlikumā par e-pierādījumiem. Patiesībā izpildiestādes rīcībā ir 30 dienas, lai pieņemtu lēmumu par pieprasījuma atzīšanu[4], un pēc tam tai rīkojums būtu jāizpilda 90 dienu laikā[5]. EDAK uzskata, ka EIR izpildiestādēm 30 dienu pārdomu perioda nodrošināšana ir būtisks aizsardzības līdzeklis, kas ļauj tām novērtēt, vai izpildes pieprasījums ir pamatots un atbilst visiem EIR izdošanas un nosūtīšanas nosacījumiem[6].

[3] Skatīt EIR direktīvas 37. pantu.
[4] EIR direktīvas 12. panta 3. punkts.
[5] EIR direktīvas 12. panta 4. punkts.
[6] EIR direktīvas 6. pants.

EDAK ir nobažījusies, ka desmit dienu termiņš Eiropas elektronisko pierādījumu sniegšanas rīkojuma sertifikāta (*EPOC*) izpildei, kas norādīts priekšlikumos par e-pierādījumiem, nedodot laiku pārdomām, neļauj pienācīgi novērtēt, vai *EPOC* atbilst visiem kritērijiem un ir pareizi aizpildīts.

Tāpēc EDAK iesaka piešķirt *EPOC* saņēmējam vairāk laika, lai noteiktu, vai rīkojumu vajadzētu vai nevajadzētu izpildīt.

EDAK atzīmē, ka Eiropas elektronisko pierādījumu saglabāšanas rīkojuma (*EPOC-PR*) gadījumā nav garantijas, ka datu saglabāšana tiks veikta tikai elektronisko pierādījumu sniegšanai nepieciešamajā apjomā. Patiesi, datu saglabāšanas ilgums var pārsniegt 60 dienas, jo izdevējiestādei nav piemērots laika ierobežojums, kādā adresāts ir jāinformē par atturēšanos no elektronisko pierādījumu sniegšanas rīkojuma izdošanas vai tā atsaukšanu. Tādēļ EDAK iesaka vismaz noteikt izdevējiestādei termiņu, kādā atturēties no elektronisko pierādījumu sniegšanas rīkojuma izdošanas vai to atsauktu, lai nodrošinātu atbilstību VDAR noteiktajam datu minimizēšanas principam[7].

Visbeidzot, EDAK atzīmē, ka EIR direktīva nosaka izdevējvalstij pienākumu atgriezt pierādījumus izpildiestādei[8]. Tomēr priekšlikumā regulai par E-pierādījumiem šāda iespēja netiek minēta. Nav skaidrs, kas notiek ar elektroniskajiem pierādījumiem pēc tam, kad tie ir nosūtīti izdevējiestādei.

Tāpēc EDAK iesaka regulas priekšlikumā paredzēt vairāk informācijas par elektronisko pierādījumu izmantošanu pēc to nodošanas izdevējiestādei, lai nodrošinātu atbilstību VDAR un pārredzamības principam, kā arī *MLAT* noteiktam specifiskuma principam[9].

b) Abpusējas sodāmības principa atmešana

EDAK atzīst, ka savstarpēja atzīšana ir atkarīga no abpusējas sodāmības piemērošanas, kas dalībvalstīm ir savas suverenitātes saglabāšanas veids. Tomēr abpusējas sodāmības principu arvien vairāk uzskata par šķērsli netraucētai tiesu iestāžu sadarbībai. ES dalībvalstis arvien vairāk vēlas sadarboties arī gadījumos, kad izmeklēšanas pasākumi attiecas uz darbībām, kuras saskaņā ar to tiesību aktiem nav uzskatāmas par pārkāpumiem. Tomēr EDAK atgādina, ka abpusējās sodāmības principa mērķis ir sniegt papildu aizsardzības pasākumu, lai nodrošinātu, ka valsts nevar paļauties uz citas valsts palīdzību, piemērojot kriminālsodu, kas nav citas valsts tiesību aktos. Tas, piemēram, liegtu valstij pieprasīt citas valsts palīdzību, lai apcietinātu kādu personu par tās politiskajiem uzskatiem, ja šādi uzskati nav krimināli sodāmi valstī, kurai adresēts pieprasījums, vai uzsākt kriminālvajāšanu pret kādu personu par aborta veikšanu, ja šī persona uzturas citā valstī, kura aborts nav nelegāls. Abpusējās sodāmības principam bieži vien ir arī papildu ierobežojumi vai aizsardzības pasākumi attiecībā uz sankcijām, ja pastāv pārāk lielas atšķirības starp pieprasītāju valsti un izpildvalsti. Galvenais piemērs ir apņemšanās nepiemērot nāves sodu noteiktos MLAT, ja tāds nepastāv vienas vai vairāku pušu tiesību aktos.

EDAK atzīmē, ka priekšlikumā par e-pierādījumiem abpusējās sodāmības princips ir izslēgts. Taču tādējādi tiek svītrotas ne vien parastās savstarpējas atzīšanas formalitātes, bet arī ar pašu abpusējās sodāmības principu saistītie aizsardzības pasākumi.

Patiesi, EDAK atzīmē, ka nav iekļautas norādes uz tās valsts likumiem, kurā reģistrēts pakalpojumu sniedzējs, kuram pieprasījums adresēts, un ka jebkuru datu saglabāšanu, kā arī abonenta vai

[7] VDAR 5. panta 1. punkta c) apakšpunkts.
[8] EIR direktīvas 13. panta 3. un 4. punkts.
[9] VDAR 5. panta 1. punkta a) apakšpunkts.

piekļuves datu sniegšanu, var pieprasīt attiecībā uz jebkādiem noziedzīgiem nodarījumiem[10] neatkarīgi no tā, vai citu dalībvalstu tiesību aktos ir noteikti līdzīgi noziedzīgi nodarījumi.

Tajā pašā laikā elektronisko pierādījumu sniegšanas rīkojumus var izdot un izpildīt tikai tad, ja līdzīgs pasākums ir pieejams attiecībā uz vienu un to pašu noziedzīgo nodarījumu salīdzināmā vietējā situācijā izdevējvalstī[11]. Turklāt, kā paskaidrots Komisija regulas priekšlikuma paskaidrojuma rakstā, tiek noteikts darījuma datu un satura datu specifiskums, jo tie tiek uzskatīti par konfidenciāliem. Patiesi, rīkojumiem par darījumu vai satura datiem tiek piemērots vismaz trīs gadu maksimālā brīvības atņemšanas soda slieksnis, lai nodrošinātu proporcionalitātes principa un skarto personu tiesību ievērošanu[12]. Tomēr EDAK uzsver, ka ES vēl nav notikusi saskaņošana attiecībā uz noziedzīgiem nodarījumiem, par kuriem tiek piemērots sods ar brīvības atņemšanu uz vismaz 3 gadiem.

EDAK iebilst pret atteikšanos no abpusējas sodāmības principa, kura mērķis ir nodrošināt, ka valsts nevar paļauties uz citas valsts palīdzību, lai šī cita valsts, kura izmanto atšķirīgu pieeju, piemērotu pirmās valsts tiesību aktus ārpus šīs valsts teritorijas, jo īpaši ņemot vērā citu svarīgo tradicionālo aizsardzības pasākumu izzušanu krimināltiesību jomā (skatīt turpmāk 3 punktu par vietas identifikācijas kritērijiem un 7. punkta g) apakšpunktu attiecībā uz iespējamiem konfliktiem ar trešo valstu tiesību aktiem).

c) Sekas, kas iestājas, vēršoties tieši pie uzņēmumiem

EDAK atzīst, ka elektroniskie pierādījumi arvien vairāk ir pieejami privātajā infrastruktūrā, un tie var atrasties ārpus izmeklēšanas valsts, pakalpojumu sniedzēja īpašumā.

EDAK atzīmē, ka pēc lēmumiem *Yahoo!*[13] un *Skype*[14] lietā Beļģijā un teroristu uzbrukumu kontekstā ir nepieciešama netraucēta un ātrāka sadarbība starp valsts un privātajām struktūrām. Ietekmes novērtējumā Komisija atsaucas uz trīs veidu procesuālajiem instrumentiem, kas ietver gan valsts iestādes, gan pakalpojumu sniedzējus. Tie ir tiesu iestāžu sadarbība, tiešā sadarbība un tieša piekļuve. Ja pirmais instruments pienākumu par EIR izpildi uzliek nevis pakalpojumu sniedzējam, bet gan izpildiestādei[15], otrs, instruments, tiešā sadarbība, balstās uz pakalpojumu sniedzēja sadarbošanos. Visapgrūtinošākā no pakalpojumu sniedzēja viedokļa ir tieša piekļuve, jo valsts iestādes var piekļūt datiem bez starpnieka palīdzības.

Tādēļ EDAK pauž bažas, ka, vēršoties tieši, pakalpojumu sniedzēji nenodrošinās personas datu aizsardzību tik efektīvi, kā to ir spējīgas izdarīt valsts iestādes, kurām arī ir pienākums to darīt, un uzsver, ka tā rezultātā netiks piemērotas dažas procesuālās garantijas, kas saistībā ar tiesu iestāžu sadarbību paredzētas gan privātpersonām, gan pašiem uzņēmumiem[16]. Piemēram, pakalpojuma sniedzējam, kuram pieprasījums adresēts, būtu jāvēršas citas (dalīb-)valsts tiesā, lai apstrīdētu rīkojumu, savukārt tiesiskās sadarbības kontekstā tam būtu jāstrādā ar savām iestādēm. EDAK iesaka regulas priekšlikumā iekļaut papildu pamatojumu, kas apliecina, ka pakalpojumu sniedzēji aizsargās

[10] Priekšlikuma regulai par e-pierādījumiem 5. panta 3. punkts un 6. panta 2. punkts.
[11] Priekšlikuma regulai par e-pierādījumiem 5. panta 2. punkts.
[12] Priekšlikuma regulai par e-pierādījumiem 5. panta 4. punkta a) apakšpunkts.
[13] *Hof van Cassatie van België, YAHOO!* Inc., No. P.13.2082.N, 2015. gada 1. decembris
[14] *Correctionele Rechtbank van Antwerpen, afdeling Mechelen of Belgium, No. ME20.F1.105151-12*, 2016. gada 27. oktobris. (*Skype* lēmumu ir pārsūdzējis).
[15] 10.-16. pants.
[16] Skatīt arī no starptautiskās datu aizsardzības viedokļa "Darba dokuments par datu aizsardzības un personas privātās dzīves aizsardzības standartiem pārrobežu datu pieprasījumos tiesībaizsardzības nolūkā", Starptautiskā darba grupa datu aizsardzībai telekomunikācijās, 63. sanāksme, 2018. gada 9.-10. aprīlis, Budapešta (Ungārija).

personas pamattiesības, piemēram, uz personas datu aizsardzību, privātās un ģimenes dzīves neaizskaramību, kā arī kompetentās datu aizsardzības iestādes informāciju, lai nodrošinātu kontroles iespējamību.

3. Jaunais jurisdikcijas pamats un tā saucamā vietas identifikācijas kritēriju pazušana

EDAK atzīmē, ka Komisija uzsver, ka viena no galvenajām šo priekšlikumu ierosinātajām izmaiņām, ir atrašanās vietas identifikācijas kritēriju pazušana un iespēja kompetentajām iestādēm pieprasīt datu saglabāšanu un izgatavošanu neatkarīgi no tā, kur šie dati faktiski tiek glabāti.

No datu aizsardzības viedokļa nav nekāds jaunums, ka ES datu aizsardzības likums tiek piemērots neatkarīgi no tā, kur tiek glabāti attiecīgo personu dati. Patiesi, VDAR piemērojamība ir atkarīga vai nu no fakta, ka pārzinis vai apstrādātājs ir reģistrēts ES teritorijā, vai arī no tā, vai tiek apstrādāti ES datu subjekta dati, pat ja pārzinis vai apstrādātājs nav reģistrēts ES teritorijā[17], un tādā gadījumā viņiem arī ir jāieceļ juridiskais pārstāvis ES[18]. No datu aizsardzības viedokļa ir svarīgi atzīmēt, ka paplašinātās teritoriālās darbības mērķis ir nodrošināt pilnīgāku ES datu subjektu aizsardzību, neatkarīgi no tā, kur atrodas uzņēmums, kurš apstrādā viņu datus.

Tādēļ, kaut arī vietas identifikācijas kritēriju izzušana, iespējams, ir jaunums krimināltiesību jomā, tā nav uzskatāma par būtiskām pārmaiņām, raugoties no datu aizsardzības viedokļa. Turklāt EDAK arī norāda, ka saikne ar ES teritoriju joprojām tiek saglabāta, jo priekšlikumi attiecas tikai uz tiem pakalpojumu sniedzējiem, kuri piedāvā pakalpojumus Savienībā, un tas, ka pieprasījumus var adresēt tikai saistībā ar izmeklēšanu krimināllietās norāda uz saikni ar ES (vai nu tāpēc, ka noziegums izdarīts dalībvalsts teritorijā, vai arī tāpēc, ka cietušais vai noziedznieks ir kādas dalībvalsts pilsonis).

Ja vietas identifikācijas kritēriju izzušana tagad būtu jāpiemēro krimināltiesībās, EDAK vislielākās bažas raisa tas, kā nodrošināt, ka šāda attīstība nekaitē datu subjektu un pakalpojumu sniedzēju, kuriem adresēts pieprasījums, datu aizsardzībai un kriminālprocesuālajām tiesībām. Raugoties no šī viedokļa, EDAK atzīst, ka Eiropas Savienībā procesuālās garantijas vismaz daļēji ir saskaņotas un jānodrošina saskaņā ar Eiropas Cilvēktiesību konvenciju. Tādējādi var apgalvot, ka sekas vietas identificēšanas kritēriju izzušanas gadījumos, kad pierādījumi tiks pieprasīti ES iekšienē, iespējams, būtu mazākas, salīdzinot ar pretējo situāciju, kad trešo valstu iestādes pieprasītu datus no uzņēmumiem, kas reģistrēti ES, piemērojot tādus pašus nosacījumus, kādi izklāstīti e-pierādījumu regulas projektā. Patiesi EDAK ir īpaši nobažījusies, ka tā rezultātā varētu rasties problemātiskākas situācijas. Šajā kontekstā iestādes no trešās valsts, kurā krimināltiesību jomā piemēro dažādas un, iespējams, mazākas procesuālas garantijas, varētu piekļūt datiem, kurus ES iekšienē aizsargātu papildu aizsardzības pasākumi. Šajā jautājumā EDAK atgādina paustās bažas par dubultiem standartiem un pamattiesību vājināšanu gadījumos, kad pakalpojumu sniedzēji un datu subjekti nevar izmantot ES tiesību aktos paredzētās procesuālās garantijas, ja pieprasījumu iesniedz trešās valsts iestāde.

Turklāt, tā kā šis jaunais jurisdikcijas pamats "neatkarīgi no datu atrašanās vietas" tiek saistīts ar procedūru, kas galvenokārt balstās uz tiešiem kompetento iestāžu pieprasījumiem, kas adresēti pakalpojumu sniedzējiem, EDAK ir bažas, ka privāti uzņēmumi, kuri saņem pieprasījumus un kuriem

[17] Skatīt 3. pantu, jo īpaši 2. punktu.
[18] Skatīt 27. pantu.

nav saistošs kāds juridisks instruments, piemēram, *MLAT*, ar ko tradicionāli regulē datu apmaiņu starp tiesu iestādēm un aizsardzības pasākumu noteikšanu, var nepiemērot datu aizsardzības pasākumus. Jo īpaši *MLAT* kontekstā minimālie datu aizsardzības pasākumi nozīmē, piemēram, konfidencialitātes pienākumus un specifiskuma principu, kas nozīmē, ka dati netiks apstrādāti citam nolūkam.

Tādējādi EDAK vismaz atgādina, ka Direktīvā 2016/680 paredzētie aizsardzības pasākumi būtu jāpiemēro arī attiecībā uz datu nosūtīšanu un jo īpaši 39. pantu, ja pakalpojumu sniedzējs ir reģistrēts trešā valstī, attiecībā uz kuru nav pieņemts lēmums par atbilstību šajā jomā. Konkrētāk, EDAK uzsver, ka šī norma jo īpaši paredz rīkojuma(-u) izdevējiestādes dalībvalsts kompetentās datu aizsardzības iestādes informēšanu un nosūtīšanas dokumentēšanu arī attiecībā uz pamatojumu par to, ka nosūtīšana trešās valsts kompetentajai iestādei ir neefektīva vai nepiemērota.

4. Jēdziens "pakalpojumu sniedzēji" būtu jāierobežo vai jāpapildina ar papildu aizsardzības pasākumiem datu subjektu tiesībām

Attiecībā uz pakalpojumu sniedzējiem EDAK atzinīgi vērtē plašo definīciju, kas ļauj iekļaut gan sakaru pakalpojumus, gan *"over-the-top" (OTT)* pakalpojumus, jo visi šie pakalpojumi ir funkcionāli līdzvērtīgi, un tādēļ paredzētie pasākumi varētu līdzīgi ietekmēt tiesības uz privātumu un komunikāciju noslēpumu, kā tas uzsvērts DG29 deklarācijā un iepriekš Atzinumā 01/2017 par e-privātuma regulas priekšlikumu. Patiešām, regulas par elektroniskajiem pierādījumiem priekšlikums attiecas uz pakalpojumu sniedzējiem, kas sniedz vai nu elektronisko sakaru pakalpojumus, kas definēti 2. panta 4. punktā direktīvā, ar ko izveido Eiropas Elektronisko sakaru kodeksu, informācijas sabiedrības pakalpojumiem, kas definēti Direktīvas (ES) 2015/1535 1. panta 1. punkta b) apakšpunktā, "attiecībā uz kuriem datu glabāšana nav lietotājiem sniegtā pakalpojuma pamatelements, tie ietver sociālos tīklus, tiešsaistes tirgus, kas sekmē darījumus starp to lietotājiem, un citus mitināšanas pakalpojumu sniedzējus", un interneta domēna nosaukumu un IP numerācijas pakalpojumiem, "piemēram, IP adreses sniedzēji, domēna nosaukumu reģistri, domēna nosaukumu reģistratori un saistītie privātuma un starpnieku pakalpojumi"[19].

Tomēr pakalpojuma sniedzējs regulas projekta izpratnē ir "jebkura fiziska vai juridiska persona, kas sniedz vienu vai vairākus šādu kategoriju pakalpojumus", un EDAK ir bažas, ka šis instruments varētu attiekties gan uz pārziņiem, gan uz apstrādātājiem VDAR izpratnē. Patiesi, tā kā regulas priekšlikuma 2. panta 4. punktā definētā "pakalpojumu piedāvāšana" ir iespēja juridiskām vai fiziskām personām vienā vai vairākās dalībvalstīs izmantot uzskaitītos pakalpojumus, un būtisku saikni ar attiecīgo(-ajām) dalībvalsti(-īm), šīs darbības ietver darbus, ko apstrādātājs veic pārziņa labā, piemēram, datu glabāšanu.

Tādējādi EDAK pauž bažas, ka bez noteiktiem ierobežojumiem pakalpojumu sniedzējiem, kas darbojas kā pārziņi VDAR izpratnē, un bez īpaša pienākuma apstrādātājam informēt datu pārzini, ja pie tā vēršas ar elektronisko pierādījumu sniegšanas vai saglabāšanas rīkojumu, datu subjektu tiesības varētu tikt apietas. Tas jo īpaši tāpēc, ka saistībā ar iespējamām pretrunīgiem pienākumiem, kas adresātam liedz izpildīt saņemtos rīkojumus, regulas projektā tiesu iestādes tiek mudinātas vērsties pie vispiemērotākā dalībnieka neatkarīgi no piemērojamiem datu aizsardzības noteikumiem,

[19] Priekšlikuma regulai par e-pierādījumiem 2. panta 3. punkta c) apakšpunkts.

jo īpaši ņemot vērā, ka varētu tikt pieprasīti jebkādi dati, ne tikai personas dati, uz kuriem attiecas VDAR[20].

Saskaņā ar VDAR apstrādātājs rīkojas tikai saskaņā ar pārziņa sniegtajiem norādījumiem. Tāpēc pārziņa pienākums ir nodrošināt datu subjektu tiesību ievērošanu un sniegt viņiem būtisko informāciju, tostarp attiecībā uz viņu datu saņēmējiem, piemēram, saistībā ar datu subjektu piekļuves tiesību īstenošanu. Apstrādātājs nesaņems šos pieprasījumus no datu subjektiem un nespēs atbildēt, ja vien pārzinis to nav īpaši pieprasījis.

Līdz ar to, ja vien viņu tiesības, piemērojot VDAR, nav ierobežotas, EDAK uzsver, ka datu subjekti, kas gūst labumu no VDAR piemērošanas, var nespēt efektīvi īstenot savas tiesības, ja pārzinis nespēj sniegt pilnīgu informāciju. EDAK arī norāda, ka iespēja, ka trūks informācijas, ir vēl lielāka, ja uzņēmējam nav noteikts īpašs pienākums informēt pārzini gadījumos, kad pieprasītie dati skar datu subjektus, kuriem neattiecas VDAR piešķirtā aizsardzība. Patiesi, šajā gadījumā tiesu iestādēm, kuras pieprasa datus, nebūs obligāti jāinformē datu subjekti par pašu veiktu turpmāko apstrādi. Tādēļ EDAK aicina ierobežot piemērošanas jomu līdz pārziņiem VDAR izpratnē, vai arī ieviest noteikumu, kurā precizēts, ka gadījumā, kad pakalpojuma sniedzējs, pie kura vēršas, nav datu pārzinis, viņš par to informē pārzini.

5. Jēdzieni "uzņēmējdarbības veikšana" un "juridiskais pārstāvis" saistībā ar šiem priekšlikumiem būtu skaidri jānošķir no šiem jēdzieniem VDAR kontekstā

Ņemot vērā vietas identifikācijas kritēriju nepiemērojamību attiecībā uz datiem, elektronisko pierādījumu sniegšanas un saglabāšanas rīkojumu adresāti ierosinātās regulas piemērošanas jomas ietvaros ir tikai pakalpojumu sniedzēji, kas piedāvā pakalpojumus Savienībā neatkarīgi no tā, vai tie ir reģistrēti ES vai ne, ar pienākumu nozīmēt juridisko pārstāvi saskaņā ar direktīvas projektā ierosinātajiem noteikumiem. Tādēļ "uzņēmējdarbības veikšanas" un "juridiskā pārstāvja" jēdzieni ir definēti dokumentu projektos.

EDAK atzīmē, ka šie jēdzieni parādās arī saistībā ar citiem ES tiesību instrumentiem, jo īpaši VDAR. Tādēļ būtu jāiesniedz precizējumi attiecībā uz šo jēdzienu definīcijām un to nodalīšanu saistībā ar priekšlikumu projektiem un VDAR kontekstā.

a) Uzņēmējdarbības veikšana

EDAK arī atgādina, ka jēdzienu "uzņēmējdarbības veikšana" regulas projekta kontekstā nedrīkst sajaukt ar jēdzienu "uzņēmējdarbības veikšanas vieta" saistībā ar VDAR. Tiešām regulas projekta nolūkiem uzņēmējdarbības veikšanas jēdziens, kas definēts 2. panta 5. punktā, ir plašāks nekā VDAR, jo tas ir "faktiska saimnieciskās darbības veikšana uz nenoteiktu laiku, izmantojot stabilu infrastruktūru, no kuras faktiski tiek veikta pakalpojumu sniegšanas darbība, vai stabila infrastruktūra, no kuras tiek pārvaldīta darījumdarbība", neatkarīgi no tā, vai šīs uzņēmējdarbības veikšanas ietvaros tiek apstrādāti personas dati. Tādējādi, ja "uzņēmējdarbības veikšanas vietas" definīcija VDAR izpratnē neapšaubāmi būtu jāiekļauj regulas projekta "uzņēmējdarbības veikšanas" definīcijā, otrādi tas varētu nebūt obligāti.

[20] Skatīt 7. panta 3. un 4. punktu.

Tāpēc EDAK brīdina, ka pakalpojumu sniedzēju uzņēmējdarbības veikšana regulas projekta izpratnē var nenozīmēt, ka ir izpildīti nosacījumi VDAR piemērošanai saskaņā ar 3. panta 1. punktu. Šajā sakarā pārziņi un apstrādātāji tiek aicināti pārbaudīt, vai VDAR piemērojamība neizriet no 3. panta 2. punkta, kas nozīmētu juridiskā pārstāvja Eiropas Savienībā nozīmēšanu un vienas pieturas aģentūras mehānisma neesību.

b) Juridiskais pārstāvis

Savā paziņojumā DG29 uzsvēra, ka būtu jāizvairās sajaukt pienākumu nozīmēt pārstāvi saskaņā ar VDAR 27. pantu un juridisko pārstāvi, kas paredzēts regulas par e-pierādījumiem projektā.

Saistībā ar priekšlikuma projektu EDAK vēlētos atgādināt šos ieteikumus un jo īpaši uzsvērt, ka tā izpratnē juridiskais pārstāvis direktīvas projekta par juridiskā pārstāvja iecelšanu saistībā ar priekšlikumiem par e-pierādījumiem ir jānozīmē jebkurā gadījumā, tam ir jāuztic īpašas funkcijas neatkarīgi no pakalpojumu sniedzēja piešķirtajām pilnvarām, tam ir jābūt pilnvarotam atbildēt uz pieprasījumiem un rīkoties pakalpojuma sniedzēja vārdā, kā arī jābūt lielākai atbildībai nekā pārstāvim VDAR izpratnē.

Turklāt EDAK uzsver, ka pienākums iecelt juridisko pārstāvi jebkurā gadījumā atbilstīgi e-pierādījumu projektu priekšlikumiem, neatkarīgi no tā, vai pakalpojumu sniedzējs ir reģistrēts ES, iespēja nozīmēt pat vairākus juridiskos pārstāvjus vienam un tam pašam pakalpojumu sniedzējam saskaņā ar direktīvas par e-pierādījumiem projektu un pienākums informēt dalībvalstu iestādes par juridiskā pārstāvja nozīmēšanu atšķiras no VDAR, kas neparedz šādu pienākumu informēt par nozīmēto juridisko pārstāvi, izņēmumus nozīmēšanai un ierobežotu juridiskā pārstāvja atbildību.

Tāpēc, ņemot vērā nozīmīgās atšķirības attiecībā uz lomu, atbildību un attiecībām ar citu pakalpojumu sniedzēja uzņēmējdarbību vienā gadījumā un pārzini vai apstrādātāju otrā, EDAK iesaka, ka gadījumos, kad pakalpojumu sniedzējs nav reģistrēts ES, bet uz to attiecas gan VDAR saskaņā ar 3. panta 2. punktu, gan e-pierādījumu regula, būtu jānozīmē divi atsevišķi juridiskie pārstāvji, katrs ar savām skaidri noteiktām atšķirīgām funkcijām saskaņā ar instrumentu, uz kā pamata tas ir nozīmēts.

6. Jaunas datu kategorijas

Regulas priekšlikumā definētas dažādas datu kategorijas atbilstīgi 2. pantam: abonenta dati, piekļuves dati, darījumu dati un satura dati. Komisijas priekšlikuma 20. apsvērumā tālāk precizēts, ka *"Datu kategorijas, uz kurām attiecas šī regula, ietver abonenta datus, piekļuves datus, darījumu datus (šīs trīs kategorijas dēvē par "datiem, kas nav saturs") un satura datus. Šis dalījums, izņemot piekļuves datus, pastāv daudzu dalībvalstu tiesību aktos, kā arī pašreizējā ASV tiesiskajā regulējumā, un tas ļauj pakalpojumu sniedzējiem brīvprātīgi apmainīties ar ārvalstu tiesībaizsardzības iestādēm ar datiem, kas nav saturs."*

Šajā sakarā EDAK vispirms uzsver, ka visas četras iepriekš minēto datu kategorijas ir jāuzskata par personas datiem saskaņā ar ES datu aizsardzības tiesību aktiem, jo tās satur informāciju, kas attiecas uz identificētu vai identificējamu fizisku personu, neatkarīgi no tā, vai datu subjekts regulas priekšlikumā dēvēts par "abonentu" vai "lietotāju". Tāpat jāatzīmē, ka Komisijas priekšlikuma 2. panta 6. punktā definētie "elektroniskie pierādījumi" ietver visas četras datu kategorijas un tādēļ attiecas uz personas datiem. Tāpēc regulas priekšlikumā nevis paredz noteikumus par piekļuvi pierādījumiem, kurus definē un kvalificē saskaņā ar valsts tiesību aktiem un tiesu procedūrām, bet arī paredz jaunus materiālās un procesuālās normas attiecībā uz piekļuvi personas datiem.

Lai gan regulas priekšlikumā ir noteiktas jaunas personas datu apakškategorijas, kurām piemēro atšķirīgas procesuālās piekļuves normas, EDAK atgādina, ka saskaņā ar attiecīgo EST judikatūru, lai konstatētu iejaukšanos pamattiesībās uz privāto dzīvi, nav svarīgi, vai attiecīgā informācija par privāto dzīvi ir jutīga, kā arī vai attiecīgajām personām ir sagādātas jebkādas neērtības.

Turklāt EDAK atgādina, ka attiecībā uz "datiem, kas nav saturs", kuri ietver abonenta datus, piekļuves datus un darījumu datus atbilstīgi Komisijas priekšlikumam, Eiropas Savienības Tiesa ir pieņēmusi spriedumu apvienotajās lietās C-203/15 un C-698/15 *Tele2 Sverige AB*, ka metadati, piemēram, datplūsmas dati un vietas identifikācijas dati, ir līdzeklis attiecīgo personu profila izveidei, informācija, kas ir ne mazāk jutīga, ņemot vērā tiesības uz privāto dzīvi, kā faktiskais komunikācijas saturs[21].

Kā jau minēts DG29 2017. gada 29. novembra paziņojumā par datu aizsardzību un privātuma aspektiem saistībā ar pārrobežu piekļuvi elektroniskiem pierādījumiem, tādēļ EDAK atkārtoti pauž bažas par pašreizējo robežu starp "datiem, kas nav saturs" un satura datiem, kā arī četrām personas datu kategorijām, kas noteiktas regulas priekšlikumā. Patiesi, četras piedāvātās kategorijas, šķiet, nav skaidri nodalītas, un "piekļuves datu" definīcija joprojām ir neskaidra salīdzinājumā ar citām kategorijām. Tādēļ EDAK pauž nožēlu, ka Komisijas ietekmes novērtējumā un priekšlikumā nav norādīts detalizētāks pamatojums šo jauno personas datu apakškategoriju izveidei un pauž bažas par dažādajiem garantiju līmeņiem, kas saistīti ar materiālajām un procesuālajām piekļuves normām personas datu kategorijām, jo īpaši ņemot vērā praktiskās grūtības novērtēt, kādai datu kategorijai dažos gadījumos pieprasītie dati piederēs. Piemēram, IP adreses varētu tikt klasificētas gan kā darījumu dati, gan kā abonenta dati.

Šajā sakarā EDAK arī atgādina, ka tās regulas priekšlikuma 14. apsvērumā par tiesību uz privāto dzīvi ievērošanu un personas datu aizsardzību elektroniskajos paziņojumos (e-privātums) Komisija uzskata, ka "elektronisko sakaru dati ir jādefinē pietiekami plaši un tehnoloģiju ziņā neitrāli tā, lai aptvertu visu informāciju, kas attiecas uz pārraidīto vai apmaiņā nosūtīto saturu (elektronisko sakaru saturu), un informāciju par elektronisko sakaru pakalpojumu galalietotāju, kas apstrādāta nolūkā to pārraidīt, izplatīt vai nodrošināt iespēju veikt elektronisko sakaru satura apmaiņu; tas attiecas arī uz datiem, ko izmanto, lai izsekotu un identificētu paziņojuma avotu un galamērķi, ģeogrāfisko atrašanās vietu, kā arī saziņas datumu, laiku, ilgumu un veidu". Tā kā pašreizējo un nākotnes e-privātuma sistēmu, kā arī ar to saistītos privātās dzīves tiesību ierobežojumus piemēros noteikumiem, kas reglamentē tiesībaizsardzības iestāžu piekļuvi elektroniskajiem pierādījumiem, EDAK iesaka regulas priekšlikumā iekļaut plašāku elektronisko sakaru datu definīciju, lai nodrošinātu, ka izveidotie atbilstošie aizsardzības pasākumi un piekļuves nosacījumi konsekventi attiecas gan uz "datiem, kas nav saturs", gan uz "satura datiem".

7. Eiropas elektronisko pierādījumu sniegšanas un saglabāšanas rīkojumu procedūru analīze

Vispārīgi runājot, elektronisko pierādījumu sniegšanas vai saglabāšanas rīkojuma izdošanas procedūra ir šāda.

- Kompetentā tiesu iestāde — izdevējiestāde, atkarībā no pieprasītā datu veida un rīkojuma veida izdod rīkojumu saskaņā ar 5. un 6. pantā minētajiem (ierobežotajiem) nosacījumiem, to

[21] EST 2016. gada 21. decembra spriedums, 99. punkts.

nosūta, izmantojot saskaņoto sertifikātu, pakalpojumu sniedzēja juridiskajam pārstāvim vai jebkuram tā uzņēmumam ES teritorijā — adresātam.

- Saņemot sertifikātu, adresāts izpilda rīkojumu — tas nozīmē, ka ārkārtas situācijā datus pārsūta desmit dienu vai sešu stundu laikā vai saglabā tos līdz 60 dienām, izņemot gadījumus, kad tas nav iespējams, jo sertifikāts ir nepilnīgs vai nepārvaramas varas apstākļu rezultātā, vai tādēļ, ka tas adresātam nav faktiski iespējams, vai arī tāpēc, ka adresāts atsakās, pamatojoties uz pretrunīgiem pienākumiem attiecībā uz trešās valsts pamattiesībām vai pamatinteresēm, vai citu iemeslu dēļ.
- Gadījumā, kad adresāts nav izpildījis saņemto rīkojumu, nenorādot iemeslus, kādi ir izdevējiestādei ir pieņemami, ir paredzētas procedūras, lai kompetentā iestāde dalībvalstī, kurā pakalpojuma sniedzējam ir pārstāvis vai kurā tas ir reģistrēts, panāktu rīkojumu izpildi, izņemot gadījumus, kad piemērojami ierobežotu atteikuma iemesli un izpildes iestāde iebilst pret rīkojuma atzīšanu vai izpildi.
- Gadījumā, kad adresāts izteicis pamatotu iebildumu pret rīkojumu, balstoties uz pretrunīgiem pienākumiem, izdevējiestāde nodod lietu dalībvalsts kompetentajai tiesai, kura pēc tam atbild par iespējamā konflikta izvērtēšanu un par rīkojuma izpildes nodrošināšanu attiecīgajā dalībvalstī, ja konflikts nepastāv. Konflikta gadījumā kompetentā tiesa ar savas valsts centrālās iestādes starpniecību vēršas trešās valsts centrālajās iestādēs, norādot 15 dienu termiņu atbildes sniegšanai, kuru var pagarināt par 30 dienām pēc pamatota pieprasījuma, ja pastāv pretrunīgi pienākumi attiecībā uz trešās valsts pamattiesībām vai pamatinteresēm, vai pati lemt, vai rīkojumu atstāt spēkā vai atsaukt, balstoties uz citiem atteikuma iemesliem, uz kuriem atsaucas adresāts.
- Neskarot aizsardzības līdzekļus, kas pieejami saskaņā ar VDAR un tiesībaizsardzības direktīvu, personām, kuru dati iegūti, izmantojot elektronisko pierādījumu sniegšanas rīkojumu, ir arī tiesības uz efektīviem tiesiskās aizsardzības līdzekļiem pret šādu rīkojumu.

EDAK novērtēja regulas projektā paredzētās procedūras un aizsardzības pasākumus, aptverot dažādus etapus un visus šeit izklāstītos aspektus, un iesaka šādus aizsardzības pasākumus un grozījumus.

a) Rīkojumu izdošanas sliekšņi būtu jāpaaugstina, un rīkojumus izdod vai apstiprina tiesas

Attiecībā uz rīkojumu izdošanas nosacījumiem EDAK atzinīgi vērtē principu par stingrākiem aizsardzības pasākumiem piekļuvei darījumu vai satura datiem. Tomēr tā atzīmē, ka, ņemot vērā to, ka starp dalībvalstīm nav pilnībā saskaņoti krimināLsodi, atsauce uz "noziedzīgiem nodarījumiem, kas sodāmi izdevējvalstī ar brīvības atņemšanas sodu, kura maksimālais ilgums ir vismaz 3 gadi"[22] joprojām nozīmē atšķirīgus sliekšņus un neatbilstības ES datu subjektu datu aizsardzības jomā.

Turklāt EDAK uzsver, ka, jo īpaši ņemot vērā abonentu datu plašo definīciju, attiecībā uz elektronisko pierādījumu saglabāšanas rīkojumiem un elektronisko pierādījumu sniegšanas rīkojumiem, kas skar abonenta vai piekļuves datus, slieksnis šķiet samērā zems, jo principā šādu rīkojumu izdošanu var pamatot ar jebkādiem noziedzīgajiem nodarījumiem. Tāpat iestādēm, kurām ir atļauts izdot šādus rīkojumus, ir vairāk ierobežojumu saistībā ar elektronisko pierādījumu sniegšanas rīkojumiem, kas

[22] Skatīt 5. panta 3. punkta a) apakšpunktu.

attiecas uz darījumu vai satura datiem, nekā ar elektronisko pierādījumu saglabāšanas rīkojumu vai elektronisko pierādījumu rīkojumu izdošanu, pieprasot sniegt abonenta vai piekļuves datus, jo prokurori var izdot vai atļaut tikai pēdējā veida rīkojumus, savukārt tiesnesis, tiesa vai izmeklēšanas tiesnesis var izdot vai atļaut jebkuru rīkojumu.

Jo īpaši EDAK pauž nožēlu, ka zemākais slieksnis, kas paredz iespēju tiesībaizsardzības iestādēm pieprasīt piekļuvi abonentam un datiem par jebkuru noziedzīgu nodarījumu, pamatojas uz Eiropas Savienības Tiesas judikatūras *"a contrario"* interpretāciju (kur galvenā uzmanība ir pievērsta citiem datiem), lai nodalītu aizsardzības pasākumus, kuri jānodrošina. EST patiešām uzsvēra, ka attiecībā uz datplūsmas un vietas identifikācijas datiem kompetento iestāžu piekļuve skar tikai smagu noziegumu apkarošanu[23]. EDAK noprot, ka priekšlikums paredz iespēju pieprasīt piekļuvi pamatinformācijai, kas tikai ļautu identificēt personu, neizpaužot nekādus komunikācijas datus bez iepriekšējas tiesas atļaujas. Tomēr tā pauž nožēlu par Komisijas plašo šī lēmuma "*a contrario*" interpretāciju un aicina ieviest stingrākus aizsardzības pasākumus, lai ierobežotu piekļuvi citiem abonentu datiem un datu piekļuvei. EDAK ierosina ierobežot piekļuvi šiem datiem vai nu tikai attiecībā uz regulas projektā ietvertajā sarakstā minētajiem noziegumiem, vai vismaz "smagiem noziedzīgiem nodarījumiem", jo īpaši ņemot vērā zemāko, šādiem datiem paredzētu iepriekšējas atļaujas slieksni.

Turklāt EDAK uzsver, ka šī *"a contrario"* interpretācija arī noved pie tā, ka priekšlikums paver prokuroriem iespēju izdot vai atļaut rīkojumu izdošanu. EDAK uzskata, ka, izņemot pieprasījumus attiecībā uz pamatinformāciju, kas tikai ļauj identificēt personu, neizpaužot nekādus komunikāciju datus, tas ir solis atpakaļ, salīdzinot ar EST judikatūru attiecībā uz piekļuvi komunikāciju datiem. Patiešām, judikatūrā, kas attiecas uz piekļuvi komunikāciju datiem tiesībaizsardzības nolūkos, EST ir ierobežojusi iespēju nodrošināt šādu piekļuvi, arī balstoties uz citiem kritērijiem, un "izņemot atbilstoši pamatotus steidzamības gadījumus"[24], pakļaujot "iepriekšējai tiesas vai neatkarīgas valsts iestādes kontrolei", "pēc šo iestāžu pamatota lūguma, kas iesniegts ar [noziedzīgu nodarījumu] novēršanu, atklāšanu vai kriminālvajāšanu saistītu procedūru ietvaros". [25]

EDAK atgādina, ka jēdziens "tiesa" ir autonoms ES tiesību jēdziens, un EST pastāvīgi ir uzsvērusi un atgādinājusi kritērijus, kas jāizpilda, lai kvalificētos par tiesu, ieskaitot neatkarības kritērijus[26], kas, šķiet, nav attiecināms uz prokuroriem, un to arī atgādina Eiropas Cilvēktiesību tiesa savā judikatūrā[27].

Tādējādi 4. panta 1. punkta a) un b) apakšpunktā un 3. punkta a) un b) apakšpunktā ir paredzētas procedūras, kurās abonentam un piekļuves datiem piemēro ievērojami mazāku aizsardzību, jo viens pats prokurors varēs pieprasīt datus bez jebkādas turpmākas kontroles no tās valsts iestādes, kurā atrodas pieprasītie dati, vai no tās, kurā atrodas uzņēmuma, kuram adresēts pieprasījums, juridiskais pārstāvis, kā arī bez neatkarīgas administratīvās iestādes kontroles.

Turklāt EDAK atzīmē 5. panta 2. punktā paredzēto tā saucamo papildu aizsardzības pasākumu, kas ierobežo iespēju izdot elektronisko pierādījumu sniegšanas rīkojumu, ja attiecībā uz vienu un to pašu noziedzīgu nodarījumu salīdzināmā iekšzemes situācijā ir pieejams līdzīgs pasākums. Tomēr tā brīdina par šādas normas nelabvēlīgo ietekmi: tā vietā, lai radītu papildu aizsardzību, tā mudina dalībvalstis paplašināt savas iespējas pieprasīt abonenta vai piekļuves datu sniegšanu, lai nodrošinātu elektronisko pierādījumu sniegšanas rīkojumu izdošanu saskaņā ar šo regulu.

[23] Skatīt lietu 203/15, 125. punktu.
[24] Skatīt lietu 203/15, 120. punktu.
[25] Skatīt apvienotās lietas C-293/12 un C-594/12, 62. punktu.
[26] Skatīt, piemēram, lietu C-203/14.
[27] Skatīt, piemēram, *Moulin*/Francija 23/11/2010.

b) Datu sniegšanas termiņiem vajadzētu būt pamatotiem

EDAK atzīmē, ka uz Eiropas elektronisko pierādījumu sniegšanas rīkojumiem atbilde ir jāsniedz ne vēlāk kā desmit dienu laikā no sertifikāta saņemšanas, ja vien izdevējiestāde nav norādījusi agrākas izpaušanas iemeslus, un ne vēlāk kā sešu stundu laikā ārkārtas gadījumos, kā paredzēts 9. panta 1. un 2. punktā.

Tomēr EDAK nav manījusi nekādus kritērijus, ar ko iestādēm tiek uzlikts pienākums pierādīt ārkārtas situāciju datu sagatavošanai, pat *ex post,* lai nodrošinātu šīs ļoti ātras procedūras izmantošanas kontroles iespēju, savukārt sešu stundu termiņš var nozīmēt ļoti vāju kontroli pirms datu sniegšanas vai pat nekādu kontroli no pakalpojuma sniedzēja puses. Patiesi, ietekmes novērtējumā uzsvērta nepieciešamība kompetentajām iestādēm nodrošināt savlaicīgu piekļuvi datiem. Tomēr ietekmes novērtējumā sniegtie piemēri attiecas uz pierādījumiem, kas nepieciešami nopietnu noziegumu izdarīšanas gadījumā (terorisma situācijas ar ķīlniekiem, notiekoši bērnu seksuālās izmantošanas gadījumi), taču pierādījumu nepastāvībā balstīts pamatojums nešķiet pareizs gadījumos, kad nav īpašas steidzamības, izņemot šo potenciālo datu mainīgumu. Turklāt datu mainīgums nenodrošina nekādu papildu pamatojumu attiecībā uz samērīguma principu piekļuvei datiem ar mazāku aizsardzību situācijās, kad nav nekādas citas steidzamības, izņemot datu mainīgumu.

Papildus tam EDAK šaubās par nepieciešamību noteikt sešu stundu termiņu, vienlaikus paredzot, ka šis termiņš netiks piemērots, kamēr izdevējiestāde neiesniedz papildu paskaidrojumus "piecu dienu laikā", ja pakalpojumu sniedzējs nevar izpildīt savu pienākumu.

Tāpēc EDAK aicina ietekmes novērtējumā iekļaut papildu elementus, lai pamatotu šo termiņu nepieciešamību gadījumos, kad izdarītais noziedzīgais nodarījums vai noziedzīgais nodarījums, par kuru sauc pie atbildības, nav smagi, un, ja šādi detalizēti elementi netiek sniegti, precīzi formulētus kritērijus ārkārtas situāciju pamatošanai, ja ir izdots *EPOC*. Piemēram, varētu paredzēt tādu pašu modeli kā EIR direktīvā. EIR direktīvā paredzēts īsāks termiņš, ja to pamato ar "procesuālo termiņu, nodarījuma smaguma vai citu īpaši steidzamu apstākļu dēļ " (skatīt 12. panta 2. punktu), vai 24 stundu termiņš, lai lemtu par pagaidu pasākumiem (skatīt 32. panta 2. punktu). Patiesi, regulas projekta ietekmes novērtējumā nav paredzēti sīki izstrādāti elementi, kas pamato to, kāpēc šie termiņi nav efektīvi, un uzsvērt tikai, ka nosūtīto pieprasījumu skaita rezultātā saņēmējas tiesu iestādes ir pārslogotas un nespēj ievērot termiņus.

c) Eiropas elektronisko pierādījumu sniegšanas un saglabāšanas rīkojumus neizmanto, lai pieprasītu citas dalībvalsts datu subjekta datus, vismaz neinformējot attiecīgās dalībvalsts kompetentās iestādes, jo īpaši attiecībā uz satura datiem

EDAK atgādina, ka esošajos instrumentos tiek nodrošināta tiesiskā sadarbība un tādējādi papildu aizsardzības pasākumi, jo īpaši, lai kontrolētu pieprasījumu nepieciešamību un samērīgumu, un uzsver, ka šie aizsardzības pasākumi ir īpaši pamatoti gadījumos, kad pieprasītie dati ir satura dati, kas ietver vairāk ierobežojumu datu subjektu tiesībām aizsargāt savus personas datus un privātumu. Šajā sakarā EDAK atgādina, ka EIR direktīva arī paredz telekomunikāciju pārtveršanas iespēju, izmantojot citas dalībvalsts tehnisko palīdzību (skatīt 30. pantu), kā arī pienākumu informēt citas dalībvalsts kompetento iestādi par datu pārtveršanu gadījumos, kad palīdzība nav nepieciešama, ja attiecīgais datu subjekts atrodas vai atradīsies šīs dalībvalsts teritorijā (skatīt 31. pantu).

EDAK nesaskata pamatojumu procedūrai, kas paredzēta e-pierādījumu regulas projektā, lai dotu iespēju iegūt satura datus, neiesaistot vismaz tās dalībvalsts kompetentās iestādes, kurā atrodas datu subjekts.

d) Eiropas elektronisko pierādījumu saglabāšanas rīkojumus neizmanto, lai apietu pakalpojumu sniedzēju datu saglabāšanas pienākumus

EDAK atzīmē, ka galvenais Eiropas elektronisko pierādījumu saglabāšanas rīkojumu mērķis ir novērst datu dzēšanu.

Kaut arī EDAK atzīst, ka dažos gadījumos tas var būt nepieciešami un samērīgi, tā pauž nožēlu, ka trūkst aizsardzības pasākumu saistībā ar šādu rīkojumu izdošanu. Jo īpaši EDAK iesaka, ka gadījumos, kad elektronisko pierādījumu saglabāšanas rīkojumi tiek adresēti tikai attiecībā uz konkrētiem datiem, kur projektā, šķiet, atļauti plaša mēroga pieprasījumi, un gadījumos, kad šie rīkojumi tiek izdoti attiecībā uz datiem, kurus plānots dzēst atbilstīgi datu saglabāšanas principam, rīkojums nekad nedrīkst kalpot par pamatu pakalpojumu sniedzējam turpināt datu apstrādi pēc sākotnējā dzēšanas datuma. Citiem vārdiem sakot, datus vajadzētu "iesaldēt".

Turklāt jānostiprina saikne starp elektronisko pierādījumu saglabāšanas rīkojumu un tam sekojošo elektronisko pierādījumu sniegšanas pieprasījumu, izmantojot Eiropas elektronisko pierādījumu sniegšanas rīkojumu, EIR pieprasījumu vai savstarpējas tiesiskās palīdzības lūgumu, lai nodrošinātu, ka Eiropas elektronisko pierādījumu saglabāšanas rīkojumi tiek izdoti tikai tad, ja ir skaidrība par otru pieprasījumu (nevis tikai tiek uzskatīts par iespējamu), un, ja otru lūgumu noraida, arī saglabāšanas rīkojums zaudē spēku, negaidot 60 dienu termiņu[28], ja tam sekojošais pieprasījums tiek noraidīts agrāk.

e) Konfidencialitāte un lietotāja informācija

EDAK atzīmē, ka regulas projektā ir iekļauts īpašs pants[29] attiecībā uz adresēto rīkojumu konfidencialitāti. Lai izvairītos no neskaidrībām un pārpratumiem saistībā ar tiesībām uz datu aizsardzību, EDAK atgādina, ka, lai gan VDAR noteikts, ka datu subjektu tiesību ierobežojumi, lai nodrošinātu noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu un saukšanu pie atbildības par tiem, būtu jāparedz likumā un tāpēc tiem jābūt publiski pieejamiem[30], un ka šie likumdošanas pasākumi ietver konkrētas normas attiecībā uz datu subjektu tiesībām tikt informētam par ierobežojumu, izņemot gadījumus, kad tas var kaitēt ierobežojuma nolūkam[31], tas neparedz pienākumu atsevišķi informēt datu subjektus par katru piekļuves pieprasījumu, ko iesniedz tiesībaizsardzības iestādes.

Tikmēr EDAK atgādina, ka Datu aizsardzības direktīvā ir paredzētas šīs datu subjektu tiesības saņemt informāciju no pašām kompetentajām iestādēm, ja vien uz šīm tiesībām nav attiecināms ierobežojums, un šīs tiesības ir jebkuram datu subjektam, ne tikai datu subjektiem, kuri dzīvo ES teritorijā.

f) Rīkojuma izpildes panākšanas kārtība, ja pakalpojumu sniedzējs atsakās to izpildīt

[28] Skatīt 10. panta 1. punktu.
[29] Skatīt 11. pantu.
[30] Skatīt 23. panta 1. punkta d) apakšpunktu.
[31] Skatīt 23. panta 2. punkta h) apakšpunktu.

EDAK atzīmē, ka regulas projekta 14. pantā ir paredzēta procedūra rīkojuma izpildes nodrošināšanai gadījumos, kad adresāts to nepilda, balstoties uz tiesu iestāžu sadarbību starp izdevējiestādi un izpildes valsts kompetento iestādi.

Tomēr šķiet, ka šī procedūra neļauj izpildes iestādei atteikties izpildīt rīkojumu, kas pārsūtīts, balstoties uz citiem, ne tīri procesuāliem iemesliem (tāpat kā adresātam, galvenokārt saistībā ar sniegtās informācijas trūkumu vai faktisko neiespējamību sniegt datus), jo attiecīgos datus saskaņā ar valsts tiesību aktiem aizsargātā imunitāte vai privilēģijas, vai arī tādēļ, ka to izpaušana var ietekmēt pamatintereses, piemēram, valsts drošību un aizsardzību[32].

Tāpēc EDAK atkārtoti pauž bažas par to, ka tiek izslēgta saņēmējas kompetentās iestādes pārsūtīto rīkojumu dubultā pārbaude, salīdzinot ar citiem instrumentiem. Pat pamatojums atteikties izpildīt rīkojumu, balstoties uz to, ka tas pārkāpj Hartu, šķiet, pārsniedz standarta slieksni, kas saistīts ar attiecīgās personas pamattiesību pārkāpumu. Tādējādi, ievērojot Eiropas apcietināšanas ordera piemērus, kurā paredz gan obligātus, gan fakultatīvus atteikuma pamatojumus, vai vismaz EIR direktīvu, kurā kopumā paredzēts pieņēmums, saskaņā ar kuru "brīvības, drošības un tiesiskuma telpa ir izveidota, pamatojoties uz savstarpēju uzticību un pieņēmumu, ka citas dalībvalstis ievēros Savienības tiesības un it īpaši pamattiesības", ir atspēkojams[33], regulas projektā vismaz būtu jāparedz minimālā klasiskā atkāpe, kas, ja ir būtiska pamats uzskatīt, ka rīkojuma izpilde varētu izraisīt attiecīgās personas pamattiesību pārkāpumu un ka izpildvalsts tādā gadījumā nepildītu savus pienākumus attiecībā uz Hartā atzīto pamattiesību aizsardzību, rīkojuma izpilde būtu jānoraida.

g) Rīkojuma izpildes panākšana un pretrunīgi pienākumi atbilstīgi trešo valstu likumiem (15.-16. pants)

EDAK atzinīgi vērtē regulas projektā paredzēto iespēju adresātiem noraidīt rīkojumu, pamatojoties uz to, ka tas būtu pretrunā ar pamattiesībām, jo tā mērķis ir nodrošināt aizsardzības pasākumus pretrunīgu juridisku pienākumu gadījumā. Tā arī uzskata, ka ir būtiski, lai priekšlikumā paredzēts apspriesties ar trešo valstu iestādēm, vismaz gadījumā, kad rodas konflikts, kā arī pienākums atsaukt rīkojumu, ja trešās valsts iestāde izvirza iebildumus.

Tādēļ būtu ievērojami jāuzlabo paredzētā procedūra, kādā atteikties izpildīt rīkojumu, pamatojoties uz pretrunīgiem pienākumiem atbilstīgi trešo valstu tiesību aktiem.

Pirmkārt, EDAK atzīmē, ka regulas projekts uztic privātam uzņēmumam kā elektronisko pierādījumu sniegšanas rīkojuma adresātam novērtēt, vai šis rīkojums būtu pretrunā ar trešās valsts piemērojamajiem tiesību aktiem, kas aizliedz pieprasīto datu izpaušanu. Uzņēmumam ir jāsniedz pamatots iebildums, kurā ietver visu būtisko informāciju par trešās valsts tiesību aktiem, to piemērojamību attiecīgajā lietā, kā arī pretrunīgā pienākuma raksturojums.

Vislielākās bažas EDAK ir pat to, ka, izvirzot šādu iebildumu, izdevējiestādes dalībvalsts kompetentā tiesa vienpersoniski novērtē, vai pastāv konflikts, jo tiesa sazinās ar trešo valstu iestādēm tikai tad, kad tā ir konstatējusi konfliktu. Tāpēc kompetentajai ES tiesai ir piešķirta kompetence šajā kontekstā galīgi interpretēt trešās valsts tiesību aktus, taču pēc būtības tā nav īpaši liels speciālists šajā jomā. EDAK uzskata, ka pienākums apspriesties ar trešās valsts kompetentajām iestādēm šajā priekšlikumā ir pārāk ierobežots. Datu aizsardzības jomā EDAK vērš likumdevēja uzmanību uz to, ka gadījumā, ja trešās valsts kompetentā tiesa interpretētu VDAR, lai novērtētu, vai tā ir pretrunā ar tās prasībām, ES datu aizsardzības iestādes un kompetentās tiesas joprojām būtu kompetentas novērtēt nosūtīšanas

[32] Skatīt 14. panta 2. punktu.
[33] Skatīt EIR direktīvas 19. pantu.

likumību, pamatojoties uz tiesas nolēmumu vai trešās valsts administratīvās iestādes lēmumu, kas pieprasa nodot vai izpaust personas datus VDAR piemērošanas jomā[34].

Turklāt EDAK uzsver, ka trešās valsts tiesību aktu novērtējumam, ko veic ES pieprasījuma iesniedzējas valsts kompetentā tiesa, jābalstās uz objektīviem elementiem, un bažījās par kritērijiem, kādi kompetentajai tiesai jāņem vērā, novērtējot trešās valsts tiesību aktus saskaņā ar regulas projekta 15. panta 4. punktu un 16. panta 5. punkta a) apakšpunktu. Patiešām, Tiesai būtu jāizvērtē fakts, ka "tā vietā, lai aizsargātu pamattiesības vai trešās valsts pamatintereses, kas saistītas ar valsts drošību vai aizsardzību," trešās valsts tiesību akti "acīmredzami cenšas aizsargāt citas intereses vai arī ir vērsti uz to, lai kriminālizmeklēšanas ietvaros aizsargātu nelikumīgas darbības no tiesībaizsardzības iestāžu pieprasījumiem" vai "intereses, ko aizsargā trešās valsts tiesību akti, tostarp trešās valsts intereses nepieļaut datu izpaušanu". Piemēram, lai gan principā šim novērtējumam vajadzīgs uz pierādījumiem balstīts novērtējums, ņemot vērā visu pieejamo informāciju un šāda lēmuma iespējamo ietekmi, vismaz formulējums ("ir vērsti uz") šķiet neskaidrs un būtu jākoriģē ("kuru mērķis/nolūks ir").

EDAK pauž nožēlu, ka vienīgais gadījums, kurā apspriedīsies ar trešās valsts iestādēm un varētu izvirzīt iebildumus pret elektronisko pierādījumu sniegšanas rīkojuma izpildi, būtu situācija, kad šī kompetentā ES tiesa uzskatītu, ka pastāv attiecīgs konflikts, nosūtītu visus elementus attiecīgās trešās valsts centrālajām iestādēm, un šīs trešās valsts centrālā iestāde celt iebildumus, ievērojot īsos termiņus, kas nepārsniedz 50 dienas (15 dienas, kas, iespējams, pagarinātas līdz 30 dienām un pēc pēdējā iespējamā atgādinājuma sniegtas 5 papildu dienas). Visos citos gadījumos kompetentā tiesa varētu atstāt spēkā elektronisko pierādījumu sniegšanas rīkojumu un piemērot naudas sodu pakalpojumu sniedzējam, kurš atsakās rīkojumu izpildīt. Līdz ar to EDAK ir bažas par to, ka kompetentajām ES tiesām nebūs plašāka pienākuma apspriesties ar attiecīgo trešo valstu kompetentajām iestādēm, lai pārliecinātos, ka procedūra sistemātiskāk nodrošinās, ka tiks ņemti vērā abu pušu argumenti un izrādītu vēl lielāku cieņu pret trešo valstu likumiem.

Kā jau uzsvērts DG29 paziņojumā un iepriekš tekstā, EDAK atgādina, ka īpaša uzmanība būtu jāpievērš tam, ka trešās valstis varētu pieņemt līdzīgus instrumentus, kuri potenciāli varētu ietekmēt datu subjektu tiesības un viņu tiesības uz privāto dzīvi Eiropas Savienībā, jo īpaši tādu līdzīgu instrumentu risks, kas tieši nonāks pretrunā ar ES datu aizsardzības tiesību aktiem.

Turklāt EDAK uzsver, ka izdevējiestādes dalībvalsts kompetentā tiesa nevar būt tā kompetentā tiesa, kura panāk rīkojuma izpildi, kā paredzēts regulas projekta 14. pantā, kas pat palielinātu pretrunīgu procedūru risku un pretpārbaužu neesību situācijā, kad pastāv pretrunīgi likumi. Tas izriet no fakta, ka dažos gadījumos varētu būt iesaistītas trīs valstis: rīkojuma izdevējiestādes valsts, pakalpojumu sniedzēja trešā valsts un dalībvalsts, kurā ir pakalpojumu sniedzēja likumīgais pārstāvis ES, un kur rīkojums būtu izpildāms. Līdz ar to, ievērojot šobrīd paredzēto procedūru, pieprasījuma iesniedzējas iestādes tiesa dalībvalstī A var pati interpretēt pakalpojumu sniedzēja trešās valsts B tiesību aktus, nepieprasot šīs trešās valsts iestāžu atzinumu (lai gan tās ir iebildušas pret rīkojumu), un lūgt citas ES dalībvalsts C tiesu izpildīt savu lēmumu bez iespējas celt iebildumus.

Turklāt EDAK arī atzinīgi vērtē konkrētu tiesiskās aizsardzības līdzekļu ieviešanu pret elektronisko pierādījumu sniegšanas rīkojumiem papildus VDAR un tiesībaizsardzības direktīvā paredzētajiem aizsardzības līdzekļiem. Savā iepriekšējā paziņojumā DG29 jau aicināja ieviest šādus aizsardzības pasākumus. Tomēr EDAK pauž nožēlu, ka šādi aizsardzības līdzekļi nav paredzēti arī attiecībā uz saglabāšanas rīkojumiem, jo šie rīkojumi arī var radīt to personu pamatbrīvību ierobežojumus, kuru dati tiek saglabāti. Patiešām, elektronisko pierādījumu saglabāšanas rīkojumu rezultātā datus var saglabāt ilgāk, nekā tas tiktu darīts saskaņā ar datu aizsardzības noteikumiem. Tāpēc elektronisko

[34] Skatīt VDAR 48. pantu.

pierādījumu saglabāšanas rīkojums pats par sevi ierobežo attiecīgā datu subjekta pamattiesības, un tā pamatojums ir jāpārskata un jāparedz konkrēti tiesiskās aizsardzības līdzekļi, jo īpaši gadījumos, kad elektronisko pierādījumu saglabāšanas rīkojums tiks izdots kopā ar pierādījumu sniegšanas rīkojumu nolūkā iegūt datus. Kā DG29 ieteikusi savos paziņojumos, būtu jāparedz tiesiskās aizsardzības līdzekļi, kas ir vismaz līdzvērtīgi tiem, kas pieejami iekšzemes situācijā.

h) Datu nosūtīšanas drošība, atbildot uz rīkojumu

EDAK atzīmē, ka regulas projektā ir paredzēts, ka rīkojumi adresējami tikai saņēmējiem Eiropas Savienībā, un tādēļ nav paredzēts īpašs kanāls datu nosūtīšanai starp adresātiem un pakalpojumu sniedzējiem, kuri atrodas ārpus Eiropas Savienības.

Kaut arī EDAK atzinīgi vērtē to, ka nav paredzētas papildu atkāpes no ES vispārējās sistēmas attiecībā uz datu aizsardzību, tā atgādina, ka jebkuram rīkojumam, kas nosūtīts adresātam un nozīmētu nosūtīšanu ārpus ES, jāievēro VDAR paredzētais tiesiskais regulējums. Patiesi, tiesiskās sadarbības tiesiskā regulējuma, kas paredz datu aizsardzības pasākumu ievērošanu, apiešanas rezultātā elektronisko pierādījumu sniegšanas vai saglabāšanas rīkojumu adresāti nolūkā izpildīt šādus rīkojumus nedrīkstētu apiet arī datu nosūtīšanas prasības.

Turklāt, lai gan EDAK atzinīgi vērtē to, ka nav normas, ar kuru uzliek pienākumu atšifrēt šifrētos datus[35], bažas raisa fakts, ka priekšlikumu projektos nav paredzētas nekādas konkrētas prasības adresātiem novērtēt iesniegto datu autentiskumu, un EDAK uzsver, ka šis novērtējums veido arī tradicionālo instrumentu, kuri ir tiesiskās sadarbības pamatā, pievienoto vērtību, un brīdina par paaugstināto risku attiecīgajiem datu subjektiem, ja šāds novērtējums netiek veikts.

Secinājumi

Balstoties uz šo novērtējumu, EDAK vēlas likumdevējiem sniegt turpmāk norādītos ieteikumus.

1) Regulas juridiskajam pamatam nevajadzētu būt LESD 82. panta 1. punktam.
2) Būtu labāk jāparāda jauna instrumenta nepieciešamība, salīdzinot ar pašreizējo EIR direktīvu vai *MLAT*, tostarp sīki analizējot pamattiesības mazāk ierobežojošus līdzekļus, piemēram, grozot šos spēkā esošos instrumentus vai ierobežojot šā instrumenta piemērošanas jomu līdz elektronisko pierādījumu saglabāšanas rīkojumiem kopā ar citām pastāvošajām procedūrām attiecībā uz pieprasījumiem piekļūt datiem.
3) Regulā būtu jāparedz ilgāks termiņš, lai izpildes pakalpojuma sniedzējs varētu nodrošināt aizsardzības pasākumus attiecībā uz pamattiesību aizsardzības ievērošanu.
4) Abpusējās sodāmības princips būtu jāsaglabā, jo īpaši, ja dati par vietas identificēšanas kritērijiem tiek atcelti, lai saglabātu pienākumu ņemt vērā aizsardzības pasākumus, kādi nodrošināti abās iesaistītajās valstīs (pieprasījuma iesniedzējas iestādes valsts un valsts, kurā atrodas pakalpojumu sniedzējs).
5) Regulas piemērošanas jomu būtu jāierobežo līdz pārziņiem VDAR izpratnē vai arī būtu jāievieš noteikums, ka gadījumā, kad pakalpojuma sniedzējs, pie kura vēršas, nav datu pārzinis, bet gan apstrādātājs, viņam ir pienākums informēt pārzini.
6) Regulā būtu jāiekļauj aizsardzības pasākumi attiecībā uz datu nosūtīšanu gadījumos, ja pakalpojumu sniedzējs ir reģistrēts trešā valstī, attiecībā uz kuru nav pieņemts atbilstības

[35] Skatīt ietekmes novērtējuma 19. apsvērumu un 240. lappusi.

lēmums šajā jomā, vai iekļaut atsauci uz Direktīvu 2016/680, jo būs piemērojami šie aizsardzības pasākumi.

7) Tā kā obligātā juridiskā pārstāvja nozīmēšana atšķiras no VDAR paredzētās, regulā būtu precīzi jānorāda, ka juridiskajam pārstāvim, kas nozīmēts saskaņā ar regulu par e-pierādījumiem, jāatšķiras no pārstāvja, kas nozīmēts saskaņā ar VDAR 3. panta 2. punktu.
8) Regulā būtu jāietver plašāka elektronisko sakaru datu definīcija, lai nodrošinātu, ka attiecīgie aizsardzības pasākumi un nosacījumi piekļuves nodrošināšanai ietvertu gan datus, kas nav saturs, gan satura datus.
9) Regulā būtu jāpaaugstina sliekšņi rīkojumu izdošanai, un lēmumi jāizdod vai jāapstiprina tiesā, izņemot abonentu datus, ja šīs kategorijas datu definīcija tiek krasi sašaurināta līdz pamatinformācijai, kas tikai ļauj identificēt personu, bez piekļuves jebkādiem komunikācijas datiem.
10) Regulai būtu jāierobežo piekļuve abonentu un piekļuves datiem līdz striktā noziedzīgo nodarījumu sarakstā iekļautiem gadījumiem vai vismaz "smagiem noziedzīgiem nodarījumiem".
11) Regulā būtu labāk jāpamato datu sniegšanas termiņš, jo īpaši ārkārtas situācijā, un iespējā izmantot ātro sešu stundu procedūru jāietver prasība iestādēm, kas izsniegušas pieprasījumu, pierādīt šīs steidzamības esību šādas procedūras izmantošanai, pat pēc tam, lai būtu iespēja kontrolēt šādu ārkārtas pilnvaru izmantošanu.
12) Būtu jāatsakās no procedūras, kas ļauj sniegt satura datus bez tās dalībvalsts kompetentās iestādes iesaistes, kurā atrodas datu subjekts.
13) Regulā būtu jāuzlabo aizsardzības pasākumi, kas saistīti ar Eiropas elektronisko pierādījumu saglabāšanas rīkojumu izdošanu.
14) Regulā vismaz būtu jāiekļauj minimālā klasiskā atkāpe, nosakot, ka gadījumos, kad pastāv būtisks pamats uzskatīt, ka rīkojuma izpilde varētu izraisīt attiecīgās personas pamattiesību pārkāpumu, kā rezultātā izpildvalsts neievērotu savas saistības attiecībā uz Hartā atzīto pamattiesību aizsardzību, rīkojuma izpilde ir jānoraida.
15) Regulā būtu jāparedz plašāks pienākums konsultēties ar tās trešās valsts kompetentajām iestādēm, kurās atrodas pakalpojumu sniedzējs, kam pieprasīts sniegt datus, kolīzijas normu gadījumā, lai izvairītos no vienas tiesas veiktas subjektīvas interpretācijas.
16) elektronisko pierādījumu saglabāšanas rīkojumu spēkā esībai un ilgumam vajadzētu būt vairāk sasaistītiem ar tiem sekojošajiem elektronisko pierādījumu sniegšanas rīkojumiem.
17) Būtu jānodrošina labāka datu nosūtīšanas drošība.
18) Būtu jāparedz datu autentiskuma pārbaude, jo īpaši gadījumos, kad var tikt sniegti šifrēti dati.

Eiropas Datu aizsardzības kolēģijas vārdā

Priekšsēdētāja

(Andrea Jelinek)