

Briselē, 2018. gada 18. aprīlī
(OR. en)

8110/18

Starpiestāžu lieta:
2018/0108 (COD)

JAI 323
COPEN 104
CYBER 66
DROIPEN 53
JAIEX 27
ENFOPOL 171
TELECOM 94
DAPIX 106
EJUSTICE 27
MI 269
IA 101
CODEC 577

PRIEKŠLIKUMS

Sūtītājs:	Direktors <i>Jordi AYET PUIGARNAU</i> kungs, Eiropas Komisijas ģenerālsekretāra vārdā
Saņemšanas datums:	2018. gada 18. aprīlis
Saņēmējs:	Eiropas Savienības Padomes ģenerālsekretārs <i>Jeppe TRANHOLM-MIKKELSEN</i> kungs
K-jas dok. Nr.:	COM(2018) 225 final
Temats:	Priekšlikums – EIROPAS PARLAMENTA UN PADOMES REGULA par Eiropas elektronisko pierādījumu sniegšanas un saglabāšanas rīkojumiem elektronisko pierādījumu gūšanai krimināllietās

Pielikumā ir pievienots dokuments COM(2018) 225 *final*.

Pielikumā: COM(2018) 225 *final*

Strasbūrā, 17.4.2018
COM(2018) 225 final

2018/0108 (COD)

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES REGULA

**Par Eiropas elektronisko pierādījumu sniegšanas un saglabāšanas rīkojumiem
elektronisko pierādījumu gūšanai krimināllietās**

{SWD(2018) 118 final} - {SWD(2018) 119 final}

PASKAIDROJUMA RAKSTS

1. PRIEKŠLIKUMA KONTEKSTS

• Priekšlikuma pamatojums un mērķi

Sociālo plašsaziņas līdzekļu, tīmekļa pasta, ziņojumapmaiņas pakalpojumu un lietojumprogrammu ("lietotņu") izmantošana saziņas, darba, socializācijas un informācijas iegūšanas vajadzībām mūsdienās ir kļuvusi par ikdienu daudzās pasaules vietās. Šie pakalpojumi savieno simtiem miljonu lietotāju citu ar citu. Tie dod ievērojamu ieguldījumu lietotāju ekonomiskās un sociālās labklājības nodrošināšanā visā Savienībā un ārpus tās. Tomēr šos pakalpojumus var izmantot arī ļaunprātīgi kā rīkus, lai izdarītu vai sekmētu noziegumus, tostarp smagus noziegumus, piemēram, teroristu uzbrukumus. Kad tas notiek, šie pakalpojumi un lietotnes bieži vien ir vienīgā vieta, kur izmeklētāji var atrast norādes, lai noteiktu, kas ir izdarījis noziegumu, un iegūt pierādījumus, kurus var izmantot tiesā.

Nemot vērā to, ka internets ir bez robežām, šādus pakalpojumus var sniegt no jebkuras vietas pasaulē un tiem ne vienmēr ir nepieciešama fiziska infrastruktūra, korporatīva klātbūtne vai personāls dalībvalstīs, kurās tiek piedāvāti pakalpojumi, vai visā iekšējā tirgū. Tiem arī nav vajadzīgas īpašas datu glabāšanas vietas, kuras pakalpojumu sniedzējs bieži izvēlas, pamatojoties uz likumīgiem apsvērumiem, piemēram, datu drošību, apjoma ietaupījumiem un piekļuves ātrumu. Tā rezultātā arvien vairāk pieaug ar visu veidu noziegumiem saistītu krimināllietu skaits¹, kurās dalībvalstu iestādes pieprasa piekļuvi datiem, kuri varētu kalpot par pierādījumiem un kuri tiek glabāti ārpus attiecīgās valsts un/vai kurus glabā pakalpojumu sniedzēji citās dalībvalstīs vai trešās valstīs.

Attiecībā uz situācijām, kad pierādījumi vai pakalpojumu sniedzējs atrodas citur, valstu sadarbības mehānismi tika izstrādāti pirms vairākiem gadu desmitiem². Neraugoties uz regulāri veiktām reformām, šos sadarbības mehānismus arvien vairāk ietekmē pieaugošā vajadzība pēc savlaicīgas pārrobežu piekļuves pie elektroniskiem pierādījumiem. Reaģējot uz iepriekš minēto, vairākas dalībvalstis un trešās valstis ir ķērušās pie savu valsts instrumentu paplašināšanas. Šādas situācijas izraisītā sadrumstalotība rada juridisku nenoteiktību un pretrunīgus pienākumus, kā arī izvirza jautājumus par pamattiesību un procesuālo tiesību aizsardzību personām, kuras skar šādi pieprasījumi.

2016. gadā Padome aicināja uz konkrētu, kopējas ES pieejas virzītu rīcību, lai uzlabotu savstarpējo tiesisko palīdzību; lai uzlabotu sadarbību starp dalībvalstu iestādēm un pakalpojumu sniedzējiem, kas atrodas trešās valstīs; un lai ierosinātu risinājumus jurisdikcijas noteikšanai un izpildei³ kibertelpā⁴. Eiropas Parlaments līdzīgi uzsvēra problēmas, kādas pašreizējais sadrumstalotais tiesiskais regulējums var radīt pakalpojumu sniedzējiem, kuri vēlas izpildīt tiesībaizsardzības prasības, un aicināja izveidot Eiropas tiesisko regulējumu, tostarp aizsargpasākumus visu iesaistīto personu tiesību un brīvību īstenošana⁵.

¹ Sk. ietekmes novērtējuma 2.1.1. un 2.3. sadaļu.

² Eiropas Savienībā ir savstarpējas atzīšanas mehānismi, kas pašlaik pamatojas uz Eiropas Izmeklēšanas rīkojumu direktīvu; ar trešām valstīm, savstarpējas tiesiskās palīdzības (STP) mehānismi.

³ Šajā dokumentā termins "izpildes jurisdikcija" norāda uz attiecīgo iestāžu kompetenci veikt izmeklēšanas pasākumu.

⁴ [Eiropas Savienības Padomes secinājumi par krimināljustīcijas uzlabošanu kibertelpā, ST9579/16.](#)

⁵ [P8_TA\(2017\)0366.](#)

Šis priekšlikums attiecas uz konkrētu problēmu, ko rada elektroniskajiem pierādījumiem raksturīgā nepastāvība un tās starptautiskā dimensija. Tā mērķis ir pielāgot sadarbības mehānismus digitālajam laikmetam, nodrošinot tiesu iestāžu un tiesībsardzības instrumentus, lai risinātu problēmas, kas saistītas ar noziedznieku mūsdienu sazināšanās veidu un novērstu mūsdienu noziedzības veidus. Šādi instrumenti ir atkarīgi no tā, vai tiem piemēro stingrus pamattiesību aizsardzības mehānismus. Šā priekšlikuma mērķis ir uzlabot juridisko noteiktību iestādēm, pakalpojumu sniedzējiem un iesaistītajām personām, kā arī saglabāt augstus standartus tiesībsardzības pieprasījumiem, tādējādi nodrošinot pamattiesību aizsardzību, pārredzamību un atbildību. Tas arī paātrina procesu, lai nodrošinātu un iegūtu elektroniskus pierādījumus, kurus glabā un/vai tur citā jurisdikcijā esošie pakalpojumu sniedzēji. Šis instruments pastāvēs līdzās spēkā esošajiem tiesiskās sadarbības instrumentiem, kas joprojām ir svarīgi un ko kompetentās iestādes vajadzības gadījumā var izmantot. Vienlaikus Komisija cenšas nostiprināt pastāvošos tiesiskās sadarbības mehānismus ar tādiem pasākumiem kā drošas platformas izveide ātrai pieprasījumu apmaiņai starp tiesu iestādēm ES un ieguldījums 1 miljona EUR apmērā, lai apmācītu praktikantus no visām ES dalībvalstīm savstarpējas juridiskās palīdzības un sadarbības jomā, koncentrējoties uz Amerikas Savienotajām Valstīm kā trešo valsti, kas saņem visvairāk pieprasījumu no ES⁶.

Saskaņā ar šo instrumentu rīkojumu izdošanai un izpildei iestādēm būtu jāpaļaujas uz pakalpojumu sniedzēju norādīto likumīgo pārstāvi. Komisija šodien iesniedz priekšlikumu, lai nodrošinātu, ka šādi juridiskie pārstāvji tiek efektīvi izraudzīti. Tas nodrošina pakalpojumu sniedzējiem vienotu ES mēroga risinājumu juridisko rīkojumu regulēšanai, izmantojot juridisko pārstāvi.

- **Atbilstība spēkā esošajam ES tiesiskajam regulējumam politikas jomā un Eiropas Padomes Budapeštas konvencijai**

Pašreizējo ES tiesisko regulējumu veido Savienības sadarbības instrumenti krimināllietās, piemēram, Direktīva 2014/41/ES par Eiropas izmeklēšanas rīkojumu krimināllietās⁷ (EIR direktīva), Konvencija par Eiropas Savienības dalībvalstu savstarpējo palīdzību krimināllietās⁸, Padomes lēmums 2002/187/TI, ar ko izveido *Eurojust*⁹, Regula (ES) 2016/794 par Eiropu¹⁰, Padomes pamatlēmums 2002/465/TI par kopējām izmeklēšanas grupām¹¹, kā arī divpusējie nolīgumi starp Savienību un trešām valstīm, piemēram, ES un ASV nolīgums par savstarpēju tiesisko palīdzību (STP)¹² un nolīgums par STP starp ES un Jāpānu¹³.

⁶ https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf

⁷ Eiropas Parlamenta un Padomes 2014. gada 3. aprīļa [Direktīva 2014/41/ES](#) par Eiropas izmeklēšanas rīkojumu krimināllietās, OV L 130, 1.5.2014., 1. lpp.

⁸ [Padomes 2000. gada 29. maija Akts](#), ar ko pieņem Konvenciju par Eiropas Savienības dalībvalstu savstarpēju palīdzību krimināllietās saskaņā ar 34. pantu Līgumā par Eiropas Savienību.

⁹ [Padomes lēmums 2002/187/TI](#) (2002. gada 28. februāris), ar ko izveido Eurojust, lai pastiprinātu cīņu pret smagiem noziegumiem. Komisija 2013. gadā pieņēma [priekšlikumu Regulai](#), lai reformētu Eurojust (Priekšlikums Eiropas Parlamenta un Padomes regulai par Eiropas Savienības Aģentūru tiesu iestāžu sadarbībai krimināllietās (*Eurojust*), COM/2013/0535 final).

¹⁰ Eiropas Parlamenta un Padomes 2016. gada 11. maija [Regula \(ES\) 2016/794](#) par Eiropas Savienības Aģentūru tiesībsardzības sadarbībai (Eiropu) un ar kuru aizstāj un atceļ Padomes Lēmumus 2009/371/TI, 2009/934/TI, 2009/935/TI, 2009/936/TI un 2009/968/TI.

¹¹ [Padomes Pamatlēmums 2002/465/TI](#) (2002. gada 13. jūnijs) par kopējām izmeklēšanas grupām.

¹² [Padomes Lēmums 2009/820/KĀDP](#) (2009. gada 23. oktobris) par to, lai Eiropas Savienības vārdā noslēgtu Nolīgumu par izdošanu starp Eiropas Savienību un Amerikas Savienotajām Valstīm un

Ieviešot Eiropas elektronisko pierādījumu sniegšanas rīkojumu (Eiropas e-pierādījumu sniegšanas rīkojums) un Eiropas elektronisko pierādījumu saglabāšanas rīkojumu (Eiropas e-pierādījumu saglabāšanas rīkojums), šis priekšlikums palīdz kriminālprocesa vajadzībām nodrošināt un vākt elektroniskos pierādījumus, ko glabā vai tur pakalpojumu sniedzēji citā jurisdikcijā. EIR direktīva, kas lielā mērā ir aizstājusi Konvenciju par savstarpēju palīdzību krimināllietās, attiecas uz visiem izmeklēšanas pasākumiem¹⁴. Tas ietver piekļuvi elektroniskiem pierādījumiem, taču EIR direktīvā nav īpašu noteikumu attiecībā uz šāda veida pierādījumiem¹⁵. Jaunais instruments neaizstāj EIR, lai iegūtu elektroniskus pierādījumus, bet nodrošina iestādēm papildu rīku. Iespējamās situācijas, kad, piemēram, izpildes dalībvalstī jāveic vairāki izmeklēšanas pasākumi un valsts iestādes dod priekšroku EIR. Jauna instrumenta izveide elektroniskiem pierādījumiem ir labāka alternatīva nekā EIR direktīvas grozījumi, ņemot vērā īpašās problēmas saistībā ar elektronisko pierādījumu iegūšanu, kas neietekmē citus izmeklēšanas pasākumus, uz kuriem attiecas EIR direktīva.

Lai atvieglotu elektronisku pierādījumu pārrobežu vākšanu, jaunais instruments balstīsies uz savstarpējas atzīšanas principiem. Tās valsts iestāde, kurā atrodas rīkojuma adresāts, nebūs tieši jāiesaista rīkojuma izdošanā un izpildē, ja vien netiks konstatēta neatbilstība; šādā gadījumā izpilde būs nepieciešama un tajā iesaistīsies tās valsts kompetentā iestāde, kurā atrodas pārstāvis. Tādēļ šim instrumentam ir vajadzīgi stingri aizsargpasākumi un noteikumi, piemēram, tiesu iestādes apstiprināšana katrā konkrētā lietā. Piemēram, Eiropas e-pierādījumu sniegšanas rīkojumu, lai sniegtu darījuma vai satura datus (pretstatā abonentu un piekļuves datiem), var izdot tikai par noziedzīgiem nodarījumiem, kas sodāmi izdevējvalstī ar brīvības atņemšanas sodu, kura maksimālais ilgums ir vismaz 3 gadi, vai par konkrētiem noziegumiem, kas veikti, izmantojot IKT, vai ko sekmē IKT izmantošana, vai par noziegumiem, kas saistīti ar terorismu, kā minēts priekšlikumā.

Personas dati, uz kuriem attiecas šis priekšlikums, ir aizsargāti, un tos var apstrādāt tikai saskaņā ar Vispārīgo datu aizsardzības regulu (VDAR)¹⁶ un Datu aizsardzības direktīvu policijas un tiesībaizsardzības iestāžu vajadzībām (Datu aizsardzības direktīva tiesībaizsardzības jomā)¹⁷. VDAR stāsies spēkā 2018. gada 25. maijā, savukārt dalībvalstīm Datu aizsardzības direktīva tiesībaizsardzības jomā ir jātransponē līdz 2018. gada 6. maijam.

Eiropas Padomes Budapeštas Konvencija par kibernetiskiem noziegumiem (CETS Nr. 185), kuru ratificēja lielākā daļa ES dalībvalstu, izveido starptautiskus sadarbības mehānismus pret kibernetiskiem noziegumiem¹⁸. Konvencija attiecas uz noziegumiem, kas izdarīti, izmantojot internetu

Nolīgumu par savstarpējo tiesisko palīdzību starp Eiropas Savienību un Amerikas Savienotajām Valstīm.

¹³ [Padomes Lēmums 2010/616/ES](#) (2010. gada 7. oktobris), lai noslēgtu Nolīgumu starp Eiropas Savienību un Japānu par savstarpēju tiesisko palīdzību krimināllietās.

¹⁴ Izņemot kopīgas izmeklēšanas grupas (sk. EIR direktīvas 3. pantu); ne visas dalībvalstis piedalās EIR direktīvā (Īrija, Dānija).

¹⁵ Izņemot atsauci uz tādas personas identificēšanu, kurai ir 10. panta 2. punkta e) apakšpunktā minētā IP adrese un kurai nevar piemērot dubulto sodāmību kā pamatojumu atteikumam atzīt un izpildīt prasību.

¹⁶ Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa [Regula \(ES\) 2016/679](#) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK.

¹⁷ Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa [Direktīva \(ES\) 2016/680](#) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu kriminālsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI.

¹⁸ Eiropas Savienības 2013. gada kibernetiskās drošības stratēģijā Budapeštas konvencija tika atzīta par galveno daudzpusējo sistēmu cīņai pret kibernetiskiem noziegumiem — Komisijas un Eiropas Savienības augstā pārstāvja

un citus datortīklus. Tajā arī ir noteikts, ka līgumslēdzējām pusēm ir jānosaka pilnvaras un procedūras, lai iegūtu elektroniskus pierādījumus un sniegtu savstarpēju juridisko palīdzību, neaprobežojoties tikai ar kibernetiskajiem. Konvencija jo īpaši nosaka, ka līgumslēdzējām pusēm jāizdod e-pierādījumu sniegšanas rīkojumi, lai iegūtu elektroniskos datus no pakalpojumu sniedzējiem viņu teritorijā un abonenta datus no pakalpojumu sniedzējiem, kas piedāvā pakalpojumus viņu teritorijā. Turklāt Konvencija paredz e-pierādījumu saglabāšanas rīkojumu izdošanu tajos gadījumos, kad ir pamats uzskatīt, ka elektroniskie dati ir īpaši neaizsargāti pret zaudējumiem vai izmaiņām. Papildu jautājumus rada valsts e-pierādījumu sniegšanas rīkojumu izdošana un izpildāmība attiecībā uz pakalpojumu sniedzējiem, kas atrodas ārpus Konvencijas līgumslēdzējas puses teritorijas. Šajā sakarā pašlaik tiek apspriesti turpmākie pasākumi, lai uzlabotu pārrobežu piekļuvi elektroniskiem pierādījumiem.¹⁹

• Ierosinātās regulas kopsavilkums

Ar ierosināto regulu tiek ieviesti saistoši Eiropas e-pierādījumu sniegšanas un saglabāšanas rīkojumi. Abi rīkojumi jāizdod vai jāapstiprina dalībvalsts tiesu iestādei. Rīkojumu var izdot, lai panāktu tādu e-pierādījumu saglabāšanu vai sniegšanu, kurus glabā pakalpojumu sniedzējs, kas atrodas citā jurisdikcijā, un kuri ir vajadzīgi kā pierādījums kriminālizmeklēšanā vai kriminālprocesā. Šādus rīkojumus var izdot tikai tad, ja tam pašam noziedzīgajam nodarījumam ir pieejams līdzīgs pasākums salīdzināmā vietējā situācijā izdevējvalstī. Abi rīkojumi var tikt izdoti elektronisko sakaru pakalpojumu sniedzējiem, sociālajiem tīkliem, tiešsaistes tirgiem, citiem mitināšanas pakalpojumu sniedzējiem un interneta infrastruktūras nodrošinātājiem, piemēram, IP adresēm un domēnu nosaukumu reģistriem, vai to juridiskajiem pārstāvjiem, ja tādi ir. Eiropas e-pierādījumu saglabāšanas rīkojums, tāpat kā Eiropas e-pierādījumu sniegšanas rīkojums, ir adresēts juridiskajam pārstāvim ārpus izdevējas dalībvalsts jurisdikcijas, lai saglabātu datus, ņemot vērā turpmāku pieprasījumu sniegt šos datus, piemēram, izmantojot STP kanālus trešo valstu gadījumā vai izmantojot EIR starp iesaistītajām dalībvalstīm. Atšķirībā no uzraudzības pasākumiem vai likumā noteiktajiem datu saglabāšanas pienākumiem, kas nav paredzēti šajā regulā, Eiropas e-pierādījumu saglabāšanas rīkojums ir rīkojums, ko tiesu iestāde izdevusi vai apstiprinājusi konkrētā kriminālprocesā pēc tam, kad ir veikts individuāls proporcionālītātes un nepieciešamības izvērtējums katrā atsevišķā lietā. Tāpat kā Eiropas e-pierādījumu sniegšanas rīkojums, tas attiecas uz konkrētiem zināmiem vai nezināmiem jau notikuša noziedzīgā nodarījuma izdarītājiem. Eiropas e-pierādījumu saglabāšanas rīkojums nozīmē vienīgi atļauju saglabāt datus, kas jau tiek uzglabāti rīkojuma saņemšanas brīdī, nevis piekļuvi datiem nākotnē pēc Eiropas e-pierādījumu saglabāšanas rīkojuma saņemšanas.

Abi rīkojumi var tikt izmantoti tikai kriminālprocesā, sākot ar sākotnējo pirmstiesas izmeklēšanas posmu un beidzot ar procesa slēgšanu ar spriedumu vai citu lēmumu. Rīkojumu par abonentu un piekļuves datu iegūšanu var izdot par jebkuru noziedzīgu nodarījumu, bet rīkojumu par darījumu vai satura datu iegūšanu var izdot tikai par noziedzīgiem nodarījumiem, kas sodāmi izdevējvalstī ar brīvības atņemšanas sodu, kura maksimālais ilgums ir vismaz trīs gadi, vai par konkrētiem noziegumiem, kas minēti priekšlikumā, un ja

ārlietās un drošības politikas jautājumos kopīgais paziņojums par Eiropas Savienības kiberdrošības stratēģiju: Atvērta, droša un uzticama kibertelpa, JOIN (2013) 1 final.

¹⁹ Konvencijas par kibernetiskajiem komiteja (*T-CY*) savā 17. plenārsēdē (2017. gada jūnijā) pieņēma Konvencijas otrā papildprotokola ("Otrais papildprotokols") sagatavošanas darba uzdevumus, kuri *T-CY* jāsagatavo un jāpabeidz līdz 2019. gada decembrim. Mērķis ir atteikties no pieejas, kurā datu glabāšanas vieta tiek uzskatīta par izšķirošu faktoru.

pastāv īpaša saikne ar elektroniskajiem rīkiem un nodarījumiem, uz kuriem attiecas Direktīva par terorisma apkarošanu 2017/541/ES.

Nemot vērā izsekojamajiem datiem piemēroto pasākumu atšķirīgo intensitāti, priekšlikumā ir izklāstīti vairāki nosacījumi un drošības pasākumi. Tie ietver pienākumu saņemt tiesu iestādes rīkojumu iepriekšēju apstiprinājumu. Priekšlikums attiecas tikai uz uzglabātajiem datiem. Šis priekšlikums neattiecas uz reāllaika telesakaru pārtveršanu. Pasākums attiecas tikai uz to, kas ir vajadzīgs un proporcionāls attiecīgo kriminālprocesu vajadzībām. Tas arī ļauj pakalpojumu sniedzējiem attiecīgā gadījumā pieprasīt precizējumus no izdevējiestādēm. Ja šīs problēmas nevar atrisināt un izdevējiestāde nolemj turpināt izpildi, pakalpojumu sniedzēji var izmantot tos pašus iemeslus, lai iebilstu pret izpildi, ko veic to iestādes. Turklāt ir izveidota īpaša procedūra gadījumos, kad pienākums sniegt datus ir pretrunā ar konkurējošu pienākumu, kas izriet no trešās valsts tiesību aktiem.

ES tiesību akti aizsargā aizdomās turēto un apsūdzēto personu tiesības kriminālprocesā, un jau ir izstrādāti noteikumi par personas datu aizsardzību. Tomēr attiecībā uz personām, kuru dati tiek pieprasīti, šie papildu aizsardzības pasākumi priekšlikumā paredz šo personu procesuālās tiesības kriminālprocesā vai ārpus tā. Tas ietver iespēju apstrīdēt rīkojuma likumību, nepieciešamību vai proporcionalitāti, neierobežojot apstrīdēšanas pamatojumu saskaņā ar valsts tiesību aktiem. Tiesības, kas izriet no izpildes valsts tiesību aktiem, tiek pilnībā ievērotas, nodrošinot, ka izdevējvalstī tiek ņemta vērā imunitāte un privilēģijas, kas aizsargā pieprasītos datus pakalpojumu sniedzēja dalībvalstī. Tas jo īpaši attiecas uz gadījumiem, kad tie nodrošina augstāku aizsardzību nekā izdevējvalsts tiesību akti.

Rīkojumi saskaņā ar ierosināto regulu ir izpildāmi tāpat kā salīdzināmi vietējie rīkojumi jurisdikcijā, kurā pakalpojumu sniedzējs saņem rīkojumu. Regula paredz, ka dalībvalstīs jābūt spēkā efektīvām un proporcionālām sankcijām.

2. JURIDISKAIS PAMATS, SUBSIDIARITĀTE UN PROPORCIONALITĀTES PRINCIPS

• Juridiskais pamats

Juridiskais pamats, lai atbalstītu rīcību šajā jomā, ir Līguma par Eiropas Savienības darbību 82. panta 1. punkts. Līguma 82. panta 1. punktā paredzēts, ka saskaņā ar parasto likumdošanas procedūru var pieņemt pasākumus, lai izstrādātu noteikumus un procedūras ar mērķi nodrošināt visu veidu spriedumu un tiesas lēmumu atzīšanu visā Savienībā. Var pieņemt arī pasākumus, lai sekmētu dalībvalstu tiesu vai līdzvērtīgu iestāžu sadarbību tiesvedībā krimināllietās un lēmumu izpildi.

Šis juridiskais pamats attiecas uz mehānismiem, ko reglamentē šī regula. Līguma 82. panta 1. punkts nodrošina tādu tiesas lēmumu savstarpēju atzīšanu, ar kuru izdevējvalsts tiesu iestāde vēršas pret juridisku personu citā dalībvalstī un pat uzliek tai pienākumus bez iepriekšējas attiecīgās dalībvalsts tiesu iestādes iejaukšanās. Eiropas e-pierādījumu sniegšanas vai saglabāšanas rīkojums var izraisīt izpildes valsts tiesu iestādes iejaukšanos, kad nepieciešams izpildīt lēmumu.

• Instrumenta izvēle

LESD 82. panta 1. punkts paredz Savienības likumdevējiem iespēju pieņemt regulas un direktīvas.

Tā kā priekšlikums attiecas uz pārrobežu procedūrām, kur ir vajadzīgi vienoti noteikumi, nav nepieciešamības atstāt dalībvalstīm rīcības brīvību šo noteikumu transponēšanā. Regula ir tieši piemērojama, nodrošina skaidrību un lielāku juridisko noteiktību, kā arī novērš atšķirīgu interpretāciju dalībvalstīs un citas transponēšanas problēmas, kas ir skārušas pamatlēmumus par spriedumu un tiesas lēmumu savstarpēju atzīšanu. Turklāt regula ļauj Savienības teritorijā vienādi piemērot vienu un to pašu pienākumu. Šo iemeslu dēļ vispiemērotākā forma, kas jāizmanto šim savstarpējas atzīšanas instrumentam, tiek uzskatīta par regulu.

- **Subsidiaritāte**

Ņemot vērā problēmu pārrobežu dimensiju, priekšlikumā iekļautie pasākumi ir jāpieņem Savienības līmenī, lai sasniegtu mērķus. Noziegumi, par kuriem ir elektroniski pierādījumi, bieži vien ir saistīti ar situācijām, kad infrastruktūrai, kurā tiek glabāti elektroniskie pierādījumi, un pakalpojumu sniedzējam, kas vada infrastruktūru, ir piemērojams cits valsts tiesiskais regulējums Savienībā vai ārpus tās nekā cietušās personas un noziedzīgā nodarījuma izdarītāja valsts tiesiskais regulējums. Tā rezultātā kompetentajai valstij var rasties ļoti laikietilpīga un izaicinoša problēma, lai efektīvi piekļūtu elektroniskiem pierādījumiem pāri robežām bez vienotiem minimālajiem noteikumiem. Jo īpaši dalībvalstīm, darbojoties atsevišķi, būtu grūti risināt šādus jautājumus:

- Tiesiskā regulējuma sadrumstalotība dalībvalstīs, ko par nopietnu problēmu atzina pakalpojumu sniedzēji, kas centās izpildīt pieprasījumus, pamatojoties uz dažādiem valstu tiesību aktiem;
- Tiesiskās sadarbības efektivitātes uzlabošana, pamatojoties uz spēkā esošajiem Savienības tiesību aktiem, jo īpaši EIR.

Ņemot vērā juridisko pieeju daudzveidību, attiecīgo jomu skaitu (drošība, pamattiesības, tostarp procesuālās tiesības un personas datu aizsardzība, ekonomiskie jautājumi) un ieinteresēto personu plašo loku, Savienības līmeņa tiesību akti ir vispiemērotākais veids, kā risināt konstatētās problēmas.

- **Proporcionalitāte**

Priekšlikumā ir paredzēti noteikumi, saskaņā ar kuriem Savienības kompetentā iestāde var pieprasīt, lai pakalpojumu sniedzējs, kas piedāvā pakalpojumus Savienībā, bet neveic uzņēmējdarbību tajā pašā dalībvalstī, sniegtu vai saglabātu elektroniskos pierādījumus. Priekšlikuma galvenās iezīmes, piemēram, Eiropas e-pierādījumu sniegšanas rīkojuma materiālā piemērošanas joma, nosacījumi, kas nodrošina savstarpēju tiesību atzīšanu, sankciju mehānismu un drošības pasākumus un tiesiskās aizsardzības līdzekļus, ierobežo priekšlikumu, lai tas nepārsniegtu tā galveno mērķu sasniegšanai nepieciešamo mērogu. Jo īpaši priekšlikums attiecas tikai uz uzglabāto datu pieprasījumiem (reāllaika telesakaru pārtveršanas dati nav ietverti) un uz kriminālprocesos izdotiem rīkojumiem par konkrētu izmeklējamu noziedzīgo nodarījumu. Tāpēc tas neietver noziedzīgu nodarījumu novēršanu vai cita veida tiesvedības vai pārkāpumus (piemēram, administratīvās procedūras par tiesību normu pārkāpumiem) un nepieprasa, lai pakalpojumu sniedzēji sistemātiski vāktu vai glabātu vairāk datu, nekā to dara uzņēmējdarbības apsvērumu dēļ vai ievērojot citas juridiskās prasības. Turklāt, lai gan rīkojumus par abonenta un piekļuves datu sniegšanu var izdot par jebkuru noziedzīgu nodarījumu, rīkojumu par darījuma vai satura datu sniegšanu var izdot tikai par noziedzīgiem nodarījumiem, kas sodāmi izdevējvalstī ar brīvības atņemšanas sodu, kura maksimālais ilgums ir vismaz 3 gadi, vai par priekšlikumā minētajiem konkrētiem nodarījumiem, kas veikti, izmantojot IKT, vai ko sekmē IKT izmantošana, vai par noziegumiem, kas saistīti ar terorismu. Visbeidzot, priekšlikums precizē procesuālos

noteikumus un drošības pasākumus, kas piemērojami pārrobežu piekļuvei elektroniskiem pierādījumiem, bet neattiecas uz iekšzemes pasākumu saskaņošanu. Priekšlikums darbojas tikai tiktāl, cik tas ir nepieciešams un proporcionāls tiesībsardzības un tiesu iestāžu vajadzību risināšanai digitālajā laikmetā.

3. PAVEIKTĀ IZVĒRTĒJUMA, APSPRIEŠANĀS AR IEINTERESĒTAJĀM PERSONĀM UN IETEKMES NOVĒRTĒJUMA REZULTĀTI

• Apspriešanās ar ieinteresētajām personām

Vairāk nekā pusotru gadu Komisija apspriedās ar visām attiecīgajām ieinteresētajām pusēm, lai apzinātu problēmas un turpmākās attīstības virzienus. Apspriešanās notika, izmantojot aptaujas, sākot ar atklātu sabiedrisku apspriešanos līdz mērķtiecīgiem apsekojumiem attiecīgajās valsts iestādēs. Ekspertu grupas sanāsmēs un divpusējās tikšanās tika apspriesta ES likumdošanas iespējamā ietekme. Lai apkopotu atsauksmes par iniciatīvu, tika rīkotas arī konferences, kurās apsprieda pārrobežu piekļuvei elektroniskiem pierādījumiem.

Kopumā respondenti atzina, ka pieaugoša informācijas pakalpojumu izmantošana ir izaicinājums tiesībsardzības jomai, jo attiecīgajām iestādēm bieži vien nav trūkst resursu, lai apstrādātu pierādījumus tiešsaistē. Kā viens no galvenajiem šķēršļiem tiek atzīts arī ilga pierādījumu iegūšanas process. Citi būtiski aspekti, ko uzsvēra valsts iestādes, ir ticamas sadarbības trūkums ar pakalpojumu sniedzējiem, pārredzamības trūkums un juridiskā nenoteiktība saistībā ar izmeklēšanas pasākumu jurisdikciju. Respondentu ieskatā pārrobežu sadarbība starp tiesībsardzības iestādēm un digitālajiem pakalpojumu sniedzējiem sniedz pievienoto vērtību kriminālizmeklēšanā. Pakalpojumu sniedzēji un dažas pilsoniskās sabiedrības organizācijas norādīja uz nepieciešamību nodrošināt juridisko noteiktību, sadarbojoties ar valsts iestādēm un izvairoties no tiesību aktu kolīzijām. Attiecībā uz bažām par to, kā jaunie ES tiesību akti varētu ietekmēt tiesības, ieinteresētās personas uzskatīja, ka ir jāparedz īpašas garantijas, kas ir nepieciešams nosacījums jebkuram pārrobežu instrumentam.

Saskaņā ar sākotnējā ietekmes novērtējumā apkopoto informāciju ieinteresētās personas uzskatīja, ka pašreizējās STP sistēmas nepilnību novēršana padarītu to efektīvāku un uzlabotu juridisko noteiktību. Dažas pilsoniskās sabiedrības organizācijas iebilda pret ES līmeņa tiesību aktiem par tiešo sadarbību. Tās izvēlējās ierobežot ES darbību savstarpējās tiesiskās palīdzības procedūru uzlabošanā. Šī ideja tiks īstenota kā daļa no praktiskajiem pasākumiem, kurus Padome apstiprināja 2016. gada jūnijā.

Mērķtiecīgi apsekojot dalībvalstu valsts iestādes, tika konstatēts arī tas, ka nav vienotas pieejas, kā iegūt pārrobežu piekļuvei elektroniskiem pierādījumiem, jo katrai dalībvalstij ir sava iekšzemes prakse. Pakalpojumu sniedzēji atšķirīgi reaģē uz ārvalstu tiesībsardzības iestāžu pieprasījumiem, un atbildes laiki var atšķirties atkarībā no pieprasījuma iesniedzējas dalībvalsts. Tas rada juridisko nenoteiktību visām ieinteresētajām personām.

Kopumā, apspriežoties ar ieinteresētajām personām, noskaidrojās, ka pašreizējais tiesiskais regulējums ir sadrumstalots un sarežģīts. Tas var izraisīt aizkavēšanos izpildes posmā un neefektīvu izmeklēšanu un kriminālvajāšanu par noziedzumiem, kas saistīti ar pārrobežu piekļuvei elektroniskiem pierādījumiem.

- **Ietekmes novērtējums**

Regulējuma kontroles padome sniedza pozitīvu atzinumu par ietekmes novērtējumu, kas atbalstīja šo priekšlikumu²⁰, un izteica dažādus ieteikumus uzlabojumiem²¹. Pēc šā atzinuma ietekmes novērtējums tika grozīts, lai turpinātu diskusiju par pamattiesību jautājumiem, kas saistīti ar pārrobežu datu apmaiņu, jo īpaši par saikni starp dažādiem pasākumiem, kas ir daļa no vēlāmā risinājuma. Grozījumi novērtējumā tikai veikti arī, lai labāk atspoguļotu, kādi ir ieinteresēto personu un dalībvalstu viedokļi un kā tika ņemti vērā. Turklāt tika pārskatīts politikas konteksts, lai iekļautu papildu atsauces uz dažādiem aspektiem, piemēram, diskusijas ekspertu grupās, kas palīdzēja veidot iniciatīvu. Tika precizēta papildināmība starp dažādiem pasākumiem (jo īpaši EIR direktīva, sarunas par Budapeštas konvencijas papildprotokolu un ES un ASV STP nolīguma kopīga pārskatīšana) darbības jomas, termiņa un dziļuma ziņā, un tika pārskatīts pamata scenārijs, lai labāk atspoguļotu notikumus, kas varētu rasties neatkarīgi no ierosināto pasākumu pieņemšanas. Visbeidzot, tika pievienotas blokshēmas, lai labāk aprakstītu datu apmaiņas darbplūsmas.

Papildus pamata scenārijam tika apsvērti četri galvenie politikas risinājumi (O risinājums): virkne praktisku pasākumu, lai uzlabotu gan tiesiskās sadarbības procedūras, gan tiešu sadarbību starp valsts iestādēm un pakalpojumu sniedzējiem (A risinājums — nelegislatīvs); risinājums, kurā apvienoti A risinājuma praktiskie pasākumi ar starptautiskiem risinājumiem divpusējā vai daudzpusējā līmenī (B risinājums — legislatīvs); risinājums, kurā apvienoti iepriekšējie B risinājumā ietvertie pasākumi ar Eiropas e-pierādījumu sniegšanas rīkojumu un pasākumu, lai uzlabotu piekļuvi datubāzēm, kas nodrošina abonenta informāciju jautājumu veidā, piemēram, Domēna vārds *Whois* (C risinājums — legislatīvs); un risinājums, kurā apvienoti visi iepriekšējie C risinājumā ietvertie pasākumi ar tiesību aktiem par tiešu piekļuvi attālināti uzglabātiem datiem (D risinājums — legislatīvs)²².

Ja netiek veikts neviens pasākums (O risinājums), arvien pieaugošais pieprasījumu skaits pasliktinās situāciju. Visi pārējie risinājumi palīdz sasniegt iniciatīvas mērķus, taču dažādā apmērā. A risinājums varētu uzlabot pašreizējo procesu efektivitāti, piemēram, uzlabojot pieprasījumu kvalitāti, tomēr uzlabošanas iespējas ierobežo pašreizējās sistēmas strukturālās nepilnības.

Ar B risinājumu varētu panākt vairāk uzlabojumu, nodrošinot starptautiski pieņemtus risinājumus, taču šo starptautisko risinājumu iznākums daudzējādā ziņā ir atkarīgs no trešām valstīm. Tādēļ šie risinājumi ir neskaidri un, visticamāk, nav tik efektīvi un nesniegs tik daudz garantiju kā Savienības risinājums.

²⁰ Komisijas dienestu darba dokuments: Ietekmes novērtējums, kas pievienots priekšlikumam regulai par Eiropas elektronisko pierādījumu sniegšanas un saglabāšanas rīkojumiem elektronisko pierādījumu iegūšanai krimināllietās, un priekšlikumam direktīvai, ar ko nosaka saskaņotus noteikumus par juridisko pārstāvju iecelšanu, lai apkopotu pierādījumus kriminālprocesā, SWD (2018) 118.

²¹ Eiropas Komisijas Regulējuma kontroles padome: Atzinums par ietekmes novērtējumu — priekšlikums regulai par Eiropas elektronisko pierādījumu sniegšanas un saglabāšanas rīkojumiem, lai gūtu elektroniskos pierādījumus krimināllietās, un priekšlikums direktīvai, ar ko nosaka saskaņotus noteikumus par juridisko pārstāvju iecelšanu, lai apkopotu pierādījumus kriminālprocesā, SEC (2018) 199.

²² Sīkāku informāciju sk. Komisijas dienestu darba dokumentā: Ietekmes novērtējums, kas pievienots priekšlikumam regulai par Eiropas elektronisko pierādījumu sniegšanas un saglabāšanas rīkojumiem elektronisko pierādījumu nodrošināšanai krimināllietās, un priekšlikumam direktīvai, ar ko nosaka saskaņotus noteikumus par juridisko pārstāvju iecelšanu, lai apkopotu pierādījumus kriminālprocesā, SWD (2018) 118.

C risinājums nepārprotami sniedz pievienoto vērtību salīdzinājumā ar iepriekšējiem risinājumiem, nodrošinot arī ES iekšējo instrumentu tiešai sadarbībai ar pakalpojumu sniedzējiem, kas risinātu lielāko daļu problēmu, kuras konstatētas gadījumos, kad pakalpojumu sniedzējs ir attiecīgo datu turētājs.

D risinājums ir visaptverošākais risinājumu kopums. Papildus iepriekšējiem pasākumiem tas ietver normatīvu aktu par tiešu piekļuvi gadījumos, kad pakalpojumu sniedzēja iesaistīšana nav nepieciešama.

Šī likumdošanas iniciatīva, kuru Komisija ierosina, ir balstīta uz ietekmes novērtējuma atzinumiem. Šo tiesību aktu papildinās praktiskie pasākumi, kas izklāstīti ietekmes novērtējumā, un turpmākais darbs pie Budapeštas konvencijas papildprotokola izstrādes. Pamatojoties uz tiesību akta priekšlikumu, Komisija arī apspriedīsies ar ASV un citām trešām valstīm par turpmāko divpusējo vai daudzpusējo nolīgumu par pārrobežu piekļuvi elektroniskiem pierādījumiem ar papildu garantijām. Attiecībā uz pasākumiem, lai nodrošinātu tiešu piekļuvi un piekļuvi datubāzēm, kas veido daļu no D risinājuma, Komisija pašlaik nav ierosinājusi nevienu tiesību aktu, taču turpinās apsvērt labāko risinājumu šiem diviem jautājumiem.

Paredzams, ka iniciatīva ļaus panākt efektīvāku un iedarbīgāku izmeklēšanu un kriminālvajāšanu, vienlaikus uzlabojot pārredzamību un atbildību, kā arī nodrošinot pamattiesību ievērošanu. Tāpat arī sagaidāms, ka tā veicinās uzticēšanos digitālajam vienotajam tirgum, uzlabojot drošību un mazinot priekšstatu par tādu noziedzīgu nodarījumu nesodāmību, kas izdarīti tīklā savienotās ierīcēs vai ar to starpniecību.

Paredzams, ka valsts sektora iestādēm iniciatīva radīs sākotnējās ieviešanas izmaksas, kuras ilgtermiņā kompensētu kārtējo izmaksu ietaupījumi. Valstu iestādēm būtu nepieciešams pielāgoties jaunajām procedūrām un saņemt apmācību. Tomēr pēc tam šīs iestādes gūtu labumu no racionalizācijas un centralizēšanas, kā arī skaidra tiesiskā regulējuma, kas reglamentē datu piekļuves pieprasījumus, jo šiem pasākumiem būtu jāuzlabo efektivitāte. Turklāt, tā kā vēlamais risinājums mazinātu spiedienu uz tiesiskās sadarbības kanāliem, paredzams, ka valstīm, kas saņem pieprasījumus, samazinātos apstrādājamo pieprasījumu skaits.

Pakalpojumu sniedzējiem būtu jāpielāgojas jaunam tiesiskajam regulējumam, ieviešot (jaunas) procedūras un apmācot savus darbiniekus. No otras puses, saskaņots regulējums varētu samazināt slogu tiem pakalpojumu sniedzējiem, kuri pašlaik atbild uz pieprasījumiem pēc datiem, kas nav saturs un kas tiem ir jānovērtē saskaņā ar dalībvalstu atšķirīgajiem tiesību aktiem. Juridiskā noteiktība un procedūru standartizācija mazinātu administratīvo slogu un veicinātu konkurētspēju, tādējādi pozitīvi ietekmējot arī mazos un vidējos uzņēmumus. Kopumā paredzams, ka šī iniciatīva nesīs arī ietaupījumus.

• **Pamattiesības**

Priekšlikums varētu ietekmēt vairākas pamattiesības:

- tās personas tiesības, kuras dati ir pieejami: tiesību uz personas datu aizsardzību; tiesības uz privātās un ģimenes dzīves neaizskaramību; tiesības uz vārda brīvību; tiesības uz aizstāvību; tiesības uz efektīvu tiesību aizsardzību un taisnīgu tiesu;
- pakalpojumu sniedzēja tiesības: tiesības brīvi veikt uzņēmējdarbību; tiesības uz efektīvu tiesisko aizsardzību;

- visu pilsoņu tiesības: tiesības uz brīvību un drošību.

Ievērojot attiecīgo datu aizsardzības *acquis*, ierosinātajā regulā ir iekļautas pietiekamas un būtiskas garantijas, lai nodrošinātu šo personu tiesību aizsardzību.

Tā kā rīkojumus var izdot tikai kriminālprocesos un tad, ja un salīdzināmās situācijas valsts kontekstā gan pirmstiesas, gan tiesas procesa laikā, piemēro visas krimināltiesību procesuālās garantijas. Tas jo īpaši ietver tiesības uz taisnīgu tiesu, ko paredz ECTK 6. pants un Pamattiesību hartas 47. un 48. pants. Tas ietver arī attiecīgos ES līmeņa tiesību aktus par procesuālajām tiesībām kriminālprocesā: Direktīva 2010/64/ES par tiesībām uz mutisko un rakstisko tulkojumu kriminālprocesā; Direktīva 2012/13/ES par tiesībām uz informāciju par tiesībām un par izvirzītajām apsūdzībām, kā arī par tiesībām piekļūt lietas materiāliem; Direktīva 2013/48/ES par aizturētas un apcietinātas personas tiesībām uz advokāta palīdzību un sazināties ar radniekiem; Direktīva 2016/343 par to, lai nostiprinātu konkrētus nevainīguma prezumpcijas aspektus un tiesības piedalīties klātienē lietas izskatīšanā tiesā kriminālprocesā; Direktīva 2016/800 par procesuālajām garantijām bērniem un Direktīva 2016/1919 par juridisko palīdzību aizdomās turētajiem un apsūdzētajiem kriminālprocesā un pieprasītajām personām Eiropas apcietināšanas ordera procesā.

Konkrētāk, tiesu iestādes iepriekšēja iejaukšanās pirms rīkojuma izdošanas nodrošina, ka ir pārbaudīta pasākuma likumība, kā arī tā nepieciešamība un proporcionālitate attiecīgajā lietā. Tas arī nodrošina, ka rīkojums nevajadzīgi neietekmē pamattiesības, tostarp tādas tiesību principus kā advokāta un klienta saziņas konfidencialitāte. Izdevējiestādei atsevišķā gadījumā ir jānodrošina, lai pasākums ir nepieciešams un proporcionāls, tostarp ņemot vērā izmeklējamā nodarījuma smagumu. Priekšlikumā ir ietverti arī darījumu un satura datu sliekšņi, nodrošinot, ka Eiropas e-pierādījumu sniegšanas rīkojumu attiecībā uz šādiem datiem izmantos tikai smagāku noziegumu gadījumā.

Skaidri tiek aplūkotas arī tiesības uz efektīviem tiesiskās aizsardzības līdzekļiem tām personām, kuru dati tiek pieprasīti. Tiesvedības laikā izdevējvalstī ir jāņem vērā arī dažām profesijām, piemēram, advokātiem, piešķirtā imunitāte un privilēģijas, kā arī valsts drošības vai aizsardzības pamattiesības adresāta valstī. Pārbaude, ko veic tiesu iestāde, kalpo kā papildu garantija.

Tā kā rīkojums ir saistošs pasākums, tas ietekmē arī pakalpojumu sniedzēju tiesības, jo īpaši tiesības brīvi veikt uzņēmējdarbību. Priekšlikumā ir iekļautas pakalpojumu sniedzēja tiesības izvirzīt noteiktas prasības izdevējā dalībvalstī, piemēram, ja tiesu iestāde rīkojumu nav izdevusi vai apstiprinājusi. Ja rīkojums tiek nosūtīts izpildes nodrošināšanai uz izpildes valsti, izpildiestāde pēc apspriešanās ar izdevējiestādi var nolemt neatzīt vai neizpildīt rīkojumu, ja pēc tā saņemšanas ir acīmredzams kāds no ierobežotajiem iebildumu pamatojumiem. Turklāt, ja tiek uzsākta izpildes procedūra, pats adresāts var izteikt iebildumus pret rīkojumu izpildiestādē, pamatojoties uz kādu no šādiem ierobežotiem iemesliem. Tas attiecas, piemēram, uz lietām, kad ir skaidrs, ka rīkojumu nav izdevusi vai apstiprinājusi kompetentā iestāde, vai ja saistību ievērošana acīmredzami pārkāptu Hartu vai būtu acīmredzami ļaunprātīga. Tas neizslēdz adresāta tiesības uz efektīvu tiesiskās aizsardzības līdzekli pret lēmumu par sankciju piemērošanu.

Potenciāla problēma attiecībā uz ES pasākumiem šajā jomā ir iespēja, ka trešās valstis varētu ieviest savstarpējus pienākumus ES pakalpojumu sniedzējiem, kas neatbilst ES pamattiesību nosacījumiem, tostarp augstam datu aizsardzības līmenim, ko nodrošina ES *acquis*. Priekšlikumā šī situācija tiek risināta divos veidos: pirmkārt, nodrošinot pasākumu, kurā ir stingras garantijas un skaidras norādes uz nosacījumiem un aizsardzības pasākumiem, ko jau

paredz ES *acquis*, tādējādi kalpojot par paraugu ārvalstu tiesību aktiem; un, otrkārt, iekļaujot īpašu klauzulu “pienākumu kolīzija”, kas pakalpojumu sniedzējiem ļauj identificēt un rosināt izskatīt pretrunīgus pienākumus, ar kuriem tie saskaras, panākot to pārskatīšanu tiesā. Šī klauzula ir paredzēta, lai nodrošinātu atbilstību gan vispārējiem bloķējošiem nolikumiem, piemēram, ASV Elektroniskās saziņas privātuma likumam (*Electronic Communications Privacy Act — ECPA*), kas aizliedz atklāt informāciju par satura datiem tās ģeogrāfiskajā apgabalā, izņemot īpašos apstākļos, gan tiesību aktiem, kas parasti neaizliedz informācijas izpaušanu, izņemot atsevišķus gadījumus. Attiecībā uz lietām, kas saistītas ar *ECPA*, konkrētās situācijās pašreiz ir iespējams novērst piekļuvi satura datiem, tādēļ STP būtu jāpaliek par galveno instrumentu, kas nodrošina piekļuvi šādiem datiem. Tomēr, ņemot vērā izmaiņas, kas radušās saistībā ar ASV Aktu par datu likumīgu izmantojumu ārzemēs (*Clarifying Lawful Overseas Use of Data — CLOUD* ²³), bloķējošo nolikumu varētu atcelt, ja ES noslēgtu nolīgumu ar ASV. Papildu starptautiskie nolīgumi ar citiem galvenajiem partneriem var vēl vairāk samazināt tiesību normu kolīziju situācijas.

Ņemot vērā iepriekš minēto, šajā priekšlikumā minētie pasākumi ir saderīgi ar pamattiesībām.

4. IETEKME UZ BUDŽETU

Tiesību akta priekšlikums regulai neietekmē Savienības budžetu.

5. CITI ELEMENTI

- Īstenošanas plāni un uzraudzības, izvērtēšanas un ziņošanas kārtība**

Regula ir tieši piemērojama Savienībā. To tieši piemēros speciālisti, bez vajadzības grozīt iekšējās tiesību sistēmas.

Regula tiks izvērtēta, un Komisija iesniegs ziņojumu Eiropas Parlamentam un Padomei ne vēlāk kā piecus gadus pēc tās stāšanās spēkā. Balstoties uz ziņojumā izklāstītajiem secinājumiem, jo īpaši par to, vai regulā nav konstatētas jebkādas praksē būtiskas nepilnības, un ņemot vērā tehnoloģiju attīstību, Komisija izvērtēs nepieciešamību paplašināt regulas darbības jomu. Vajadzības gadījumā Komisija iesniegs priekšlikumus par šīs regulas pielāgošanu. Dalībvalstis sniegs Komisijai informāciju, kas nepieciešama ziņojuma sagatavošanai. Dalībvalstis vāc datus, kas nepieciešami regulas ikgadējai uzraudzībai.

Vajadzības gadījumā Komisija sniegs norādījumus pakalpojumu sniedzējiem par regulas prasību ievērošanu.

- Sīkāks konkrētu priekšlikuma noteikumu skaidrojums**

	REGULA	
	Pants	Preambula
I. Priekšmets,	1. Priekšmets	1–15

²³ 2018. gada 23. martā Amerikas Savienotajās Valstīs tika pieņemts Akts par datu likumīgu izmantojumu ārzemēs (*Clarifying Lawful Overseas Use of Data — CLOUD*). *CLOUD* akts ir pieejams [šeit](#)

darbības joma un definīcijas	2. Definīcijas	16–23
	3. Darbības joma	24–27
II. Eiropas elektronisko pierādījumu sniegšanas rīkojums, Eiropas elektronisko pierādījumu saglabāšanas rīkojums un sertifikāti, juridiskais pārstāvis	4. Izdevējiestāde	30
	5. Eiropas elektronisko pierādījumu sniegšanas rīkojuma izdošanas nosacījumi	28–29, 31–35
	6. Eiropas elektronisko pierādījumu saglabāšanas rīkojuma izdošanas nosacījumi	36
	7. Eiropas elektronisko pierādījumu sniegšanas rīkojuma un Eiropas elektronisko pierādījumu saglabāšanas rīkojuma adresāts	37
	8. Eiropas elektronisko pierādījumu sniegšanas rīkojuma sertifikāts un Eiropas elektronisko pierādījumu saglabāšanas rīkojuma sertifikāts	38–39
	9. <i>EPOC</i> izpilde	40–41
	10. <i>EPOC-PR</i> izpilde	42
	11. Konfidencialitāte un lietotāja informācija	43
	12. Izmaksu atlīdzināšana	Nav
III. Sankcijas un to piemērošana	13. Sankcijas	Nav
	14. Izpildes procedūra	44–45, 55
IV. Tiesiskās aizsardzības līdzekļi	15. un 16. Pārskatīšanas procedūra pretrunīgu pienākumu gadījumā, kas izriet no trešās valsts tiesību aktiem	47–53
	17. Efektīvi tiesiskās aizsardzības līdzekļi	54
	18. Privilēģiju un imunitātes nodrošināšana saskaņā ar izpildes valsts tiesību aktiem	35
V. Nobeiguma noteikumi	19. Uzraudzība un ziņošana	58
	20. Grozījumi sertifikātos un veidlapās	59–60
	21. Deleģēšanas īstenošana	60
	22. Paziņojumi	Nav
	23. Saistība ar Eiropas izmeklēšanas rīkojumiem	61

	24. Izvērtējums	62
	25. Stāšanās spēkā	Nav

1. nodaļa. Priekšmets, definīcijas un darbības joma

1. pants. Priekšmets

Šis pants nosaka priekšlikuma vispārējo darbības jomu un mērķi, proti, paredzēt noteikumus, saskaņā ar kuriem kompetentā tiesu iestāde Eiropas Savienībā var pieprasīt pakalpojumu sniedzējam, kas piedāvā pakalpojumus Savienībā, sniegt vai saglabāt elektroniskos pierādījumus, pamatojoties uz Eiropas elektronisko pierādījumu sniegšanas vai saglabāšanas rīkojumu. Šos instrumentus var izmantot tikai pārrobežu situācijās, proti, situācijās, kad pakalpojumu sniedzējs veic uzņēmējdarbību vai ir pārstāvēts citā dalībvalstī.

Šī regula nodrošina izmeklēšanas iestādēm papildu līdzekļus, lai iegūtu elektroniskos pierādījumus, neierobežojot pilnvaras, kas jau noteiktas valsts tiesību aktos, lai uzliktu saistības pakalpojumu sniedzējiem, kuri veic uzņēmējdarbību vai ir pārstāvēti to teritorijā. Ja pakalpojumu sniedzējs veic uzņēmējdarbību vai ir pārstāvēts vienā un tajā pašā dalībvalstī, šīs dalībvalsts iestādes izmanto valsts pasākumus, lai uzliktu saistības pakalpojumu sniedzējam.

Dati, kas pieprasīti ar Eiropas e-pierādījumu sniegšanas rīkojumu, jāiesniedz iestādēm tieši, neiesaistot tās dalībvalsts iestādes, kurā pakalpojumu sniedzējs veic uzņēmējdarbību vai ir pārstāvēts. Tāpat regula norobežojas no datu atrašanās vietas kā noteicošā sasaistes faktora, jo datu glabāšana parasti nenozīmē, ka tos jebkādā veidā kontrolē valsts, kuras teritorijā dati tiek glabāti. Vairākumā gadījumu šādu glabāšanu nosaka tikai pakalpojumu sniedzējs, pamatojoties uz uzņēmējdarbības apsvērumiem²⁴.

Turklāt regula ir piemērojama arī tad, ja pakalpojumu sniedzēji Savienībā neveic uzņēmējdarbību vai nav pārstāvēti, bet piedāvā pakalpojumus Savienībā. To atspoguļo 3. panta 1. punkts.

Ja priekšlikums attiecas uz pakalpojumu sniedzēju, kas veic uzņēmējdarbību vai ir pārstāvēts dalībvalstī ar iecelta juridiskā pārstāvja palīdzību, šāda juridiskā pārstāvja iecelšana nenozīmē pakalpojumu sniedzēja uzņēmējdarbības reģistrāciju šīs regulas izpratnē.

1. panta 2. punkts atgādina, ka ar šo regulu netiek grozīts pienākums ievērot pamattiesības un tiesību principus, kas noteikti Līguma par Eiropas Savienību 6. pantā.

2. pants. Definīcijas

Šis pants nosaka definīcijas, kas ir piemērojamas visā instrumentā.

Šīs regulas darbības jomā ietilpst šādi pakalpojumu sniedzēju veidi: elektronisko sakaru pakalpojumu sniedzēji; informācijas sabiedrības pakalpojumu sniedzēji, kuriem datu glabāšana ir lietotājam sniegtā pakalpojuma pamatelements, tostarp sociālie tīkli, ciktāl tie nav uzskatāmi par elektronisko sakaru pakalpojumiem; tiešsaistes tirgi, kas veicina darījumus

²⁴ Ietekmes novērtējumā ir sniegti papildu skaidrojumi.

starp to lietotājiem (piemēram, patērētājiem vai uzņēmumiem) un citi mitināšanas pakalpojumu sniedzēji, kā arī interneta domēnu nosaukumu un numerācijas pakalpojumu sniedzēji.

Regulas darbības joma attiecas uz elektronisko sakaru pakalpojumu sniedzējiem, kā noteikts [Direktīvā, ar ko izveido Eiropas Elektronisko sakaru kodeksu]. Tradicionālie telesakaru pakalpojumi, patērētāji un uzņēmumi arvien vairāk paļaujas uz jauniem interneta pakalpojumiem, kas ļauj izmantot starppersonu saziņu, piemēram, IP balss pārraidi, tūlītējo ziņapmaiņu un e-pasta pakalpojumus tradicionālo sakaru pakalpojumu vietā. Tādējādi šajā priekšlikumā būtu jāietver šie pakalpojumi, kā arī sociālie tīkli, piemēram, *Twitter* un *Facebook*, kas lietotājiem ļauj koplietot saturu.

Daudzos gadījumos dati vairs netiek glabāti lietotāja ierīcē, bet ir pieejami mākoņa infrastruktūrā, kas principā ļauj piekļūt datiem no jebkuras vietas. Pakalpojumu sniedzējiem nav jāveic uzņēmējdarbība vai jāizvieto serveri katrā jurisdikcijā; tā vietā datu glabāšanai un pakalpojumu sniegšanai tiek izmantota centralizēta administrācija un decentralizētas sistēmas. Tādējādi tiek uzlabota līdzsvarošana un samazināta kavēšanās, atbildot uz lietotāju datu pieprasījumiem. Satura piegādes tīkli (SPT) parasti tiek izmantoti, lai paātrinātu satura piegādi, kopējot saturu vairākos visā pasaulē izplatītos serveros. Tas ļauj uzņēmumiem apkalpot saturu no servera, kas atrodas vistuvāk lietotājam vai kas var maršrutēt saziņu pa mazāk pārslogotu tīklu. Lai ņemtu vērā šo attīstību, definīcija aptver mākoņa un citus mitināšanas pakalpojumus, kas nodrošina dažādus datošanas resursus, piemēram, tīklus, serverus vai citu infrastruktūru, krātuvi, lietotnes un pakalpojumus, kas ļauj glabāt datus dažādiem mērķiem. Instruments attiecas arī uz digitālajiem tirgiem, kas patērētājiem un/vai uzņēmumiem ļauj veikt darījumus, izmantojot tiešsaistes pārdošanas vai pakalpojumu līgumus. Šādi darījumi tiek veikti vai nu tiešsaistes tirgus vietnē, vai arī tirgotāju vietnē, kurā tiek izmantoti tiešsaistes tirgus piedāvātie datošanas pakalpojumi. Tādēļ tieši šajā tirgū ir pieejami elektroniskie pierādījumi, kas varētu būt vajadzīgi kriminālprocesa gaitā.

Priekšlikums neattiecas uz pakalpojumiem, kuriem datu glabāšana nav noteicošais elements. Lai gan vairākums pakalpojumu sniedzēju piedāvāto pakalpojumu ietver noteiktu datu glabāšanu, jo īpaši, ja tie tiek piegādāti tiešsaistē no attāluma, tomēr ir iespējams izdalīt pakalpojumus, kuriem datu saglabāšana nav galvenā, bet gan tikai papildu pazīme, tostarp juridiskus, arhitektūras, inženiertehniskos un grāmatvedības pakalpojumus, kas tiek sniegti tiešsaistē no attāluma.

Interneta infrastruktūras pakalpojumu sniedzēju rīcībā esošie dati, piemēram, domēna nosaukumu reģistratori un reģistri un privātuma un starppakalpojumu pakalpojumu sniedzēji vai reģionālie interneta reģistri interneta protokolu adresēm, var būt nozīmīgi kriminālprocesos, jo tie var sniegt pavedienus, kas ļauj identificēt noziedzīgā darbībā iesaistīto personu vai uzņēmumu.

To datu kategorijas, kuras kompetentās iestādes var iegūt ar Eiropas e-pierādījumu sniegšanas rīkojumu, ietver abonenta datus, piekļuves datus, darījumu datus (šīs trīs kategorijas kopā minētas kā “dati, kas nav saturs”) un uzglabātos satura datus. Šis dalījums, izņemot piekļuves datus, pastāv daudzu dalībvalstu tiesību aktos un arī trešo valstu tiesiskajos regulējumos.

Visās kategorijās ir ietverti personas dati, un tādējādi uz tiem attiecas aizsardzības pasākumi saskaņā ar ES datu aizsardzības *acquis*. Šiem datiem ir atšķirīga ietekmes intensitāte uz pamattiesībām, jo īpaši tas attiecas uz abonenta datiem, no vienas puses, un uz darījumu un satura datiem, no otras puses. Ir svarīgi nodrošināt, lai šis instruments būtu piemērojams

visām šīm kategorijām: abonenta un piekļuves dati bieži vien ir sākumpunkts, lai izmeklēšanā iegūtu norādes par aizdomās turētās personas identitāti. Tomēr darījumu un satura datiem var būt īpaši nozīmīgi kā pierādījuma materiāls. Ņemot vērā atšķirīgo ietekmi uz pamattiesībām, ir pamatoti pievienot atšķirīgus nosacījumus abonenta datiem, no vienas puses, un darījumu un satura datiem, no otras puses, kā to paredz vairāki regulas noteikumi.

Ir lietderīgi nošķirt piekļuves datus kā īpašu datu kategoriju, ko izmanto šajā regulā. Piekļuves dati, kā definēts šeit, ir paredzēti tādām pašām mērķim kā abonenta dati, t. i., lai identificētu lietotāju, un to ietekmes līmenis uz pamattiesībām ir līdzīgs. Tādēļ tiem jāpiemēro tādi paši nosacījumi kā abonenta datiem. Tādējādi ar šo priekšlikumu tiek ieviesta jauna datu kategorija, kurai piemērojami tādi paši nosacījumi kā abonenta datiem, ja abu datu izvirzītais mērķis ir vienāds.

Regulas 2. pantā ir noteiktas dalībvalstis un iestādes, kuras varētu tikt iesaistītas procedūrā. Izdevējiestādes definīcija ir iekļauta 4. pantā.

Ārkārtas gadījumi ir izņēmuma gadījumi, kad pakalpojumu sniedzējiem ir nepieciešams regulāri savlaicīgi reaģēt, un tiem tiks piemēroti īpaši nosacījumi. Tādēļ tie šajā pantā ir definēti atsevišķi.

3. pants. Darbības joma

Šis pants nosaka priekšlikuma darbības jomu. Regula attiecas uz visiem pakalpojumu sniedzējiem, kas piedāvā pakalpojumus Savienībā, tostarp uz pakalpojumu sniedzējiem, kuri neveic uzņēmējdarbību Savienībā. Pakalpojumu aktīva piedāvāšana Savienībā ar visām no tā izrietošajām priekšrocībām pamato to, kādēļ regula ir piemērojama arī šiem pakalpojumu sniedzējiem, radot līdzvērtīgus konkurences apstākļus starp dalībniekiem vienā un tajā pašā tirgū. Turklāt, neattiecinot regulu uz šiem pakalpojumu sniedzējiem, tiktu radītas nepilnības regulējumā, kas ļautu noziedzniekiem apiet regulas darbības jomu.

Lai noskaidrotu, vai tiek piedāvāti pakalpojumi, iestādēm ir jānovērtē, vai pakalpojumu sniedzējs ļauj juridiskām vai fiziskām personām vienā vai vairākās dalībvalstīs izmantot savus pakalpojumus. Tomēr pakalpojuma pieejamība (kas varētu izrietēt arī no pakalpojumu sniedzēja vai starpnieka tīmekļa vietnes vai e-pasta adreses un citas kontaktinformācijas pieejamības) vien nebūtu pietiekams nosacījums šīs regulas piemērošanai. Tādēļ ir nepieciešama būtiska saikne ar šīm dalībvalstīm, lai pārliecinātos par pietiekamu saistību starp pakalpojumu sniedzēju un teritoriju, kurā tas piedāvā savus pakalpojumus. Šāda būtiska saistība pastāv, ja pakalpojumu sniedzējam ir uzņēmums vienā vai vairākās dalībvalstīs. Ja uzņēmums Savienībā neveic uzņēmējdarbību, kritērijs par būtisku saistību ar Savienību būtu jāizvērtē, pamatojoties uz ievērojamu lietotāju skaitu vienā vai vairākās dalībvalstīs vai arī darbību vēršanu uz vienu vai vairākām dalībvalstīm. Darbību vēršanu uz vienu vai vairākām dalībvalstīm var noteikt, pamatojoties uz visiem būtiskajiem apstākļiem, tostarp tādiem faktoriem kā valoda vai valūta, ko parasti izmanto dalībvalstī. Darbību vēršanu uz kādu dalībvalsti tāpat var noteikt, ņemot vērā lietotnes pieejamību attiecīgās valsts lietotņu veikalā, vietējo reklāmas pakalpojumu sniegšanu vai reklāmas, kas sniegtas attiecīgajā dalībvalstī izmantotajā valodā, informācijas izmantošanu, kas iegūta no personām, kuras veic darbību attiecīgajā dalībvalstī, vai attiecības ar klientiem, piemēram, nodrošinot klientu apkalpošanas dienstu valodā, ko parasti izmanto attiecīgajā dalībvalstī. Tāpat tiek pieņemts, ka pastāv būtiska saistība, ja pakalpojumu sniedzējs vērš savas darbības uz vienu vai vairākām dalībvalstīm, kā noteikts 17. panta 1. punkta c) apakšpunktā Regulā 1215/2012 par jurisdikciju un spriedumu atzīšanu un izpildi civillietās un komercietās.

Eiropas e-pierādījumu sniegšanas rīkojums un Eiropas e-pierādījumu saglabāšanas rīkojums ir izmeklēšanas pasākumi, kurus var izdot tikai kriminālizmeklēšanā vai krimināllietās par konkrētiem noziedzīgiem nodarījumiem. Saikne ar konkrētu izmeklēšanu atšķir tos no tiesību aktos paredzētajiem preventīvajiem pasākumiem vai datu saglabāšanas pienākumiem un nodrošina procesuālo tiesību piemērošanu kriminālprocesos. Tādēļ kompetence uzsākt izmeklēšanu attiecībā uz konkrētu nodarījumu ir priekšnoteikums regulas izmantošanai.

Papildu prasība attiecas uz pieprasītajiem datiem, proti, tiem jābūt saistītiem ar pakalpojumiem, ko piedāvā pakalpojumu sniedzējs Savienībā.

2. nodaļa. Eiropas e-pierādījumu sniegšanas rīkojums, Eiropas e-pierādījumu saglabāšanas rīkojums un sertifikāti

4. pants. Izdevējiestāde

Tiesu iestādei, kas izdod Eiropas e-pierādījumu sniegšanas vai e-pierādījumu saglabāšanas rīkojumu, vienmēr ir jābūt iesaistītai vai nu kā izdevējiestādei, vai kā apstiprinātajai iestādei. Rīkojumus par darījumu un satura datu sniegšanu izdod tiesnesis vai tiesa. Attiecībā uz abonenta vai piekļuves datiem tos var izdot arī prokurors.

5. pants. Eiropas elektronisko pierādījumu sniegšanas rīkojuma izdošanas nosacījumi

Regulas 5. pantā izklāstīti nosacījumi Eiropas e-pierādījumu sniegšanas rīkojuma izdošanai. Tie ir jāizvērtē izdevējai tiesu iestādei.

Eiropas e-pierādījumu sniegšanas rīkojumu drīkst izdot tikai tad, ja tas ir nepieciešams un proporcionāls konkrētajā lietā. Turklāt e-pierādījumu sniegšanas rīkojums būtu jāizdod tikai tad, ja izdevējvalstī līdzīgā vietējā situācijā būtu pieejams līdzīgs pasākums.

Abonenta datu un piekļuves datu sniegšanas rīkojumus var izdot par jebkuru noziedzīgu nodarījumu. Salīdzinot ar abonenta un piekļuves datiem, darījumu datiem un satura datiem būtu jāpiemēro stingrākas prasības, lai atspoguļotu šādu datu sensitivitāti un attiecīgi lielāku tiesību aizskārumu, ko rada rīkojumi par šādiem datiem. Tādējādi rīkojumus var izdot tikai par nodarījumiem, kuros maksimālais brīvības atņemšanas sods ir vismaz trīs gadi. Sliekšņa noteikšana, pamatojoties uz maksimālo brīvības atņemšanas sodu, ļauj piemērot proporcionālāku pieeju kopā ar vairākiem citiem *ex ante* un *ex post* nosacījumiem un drošības pasākumiem, lai nodrošinātu proporcionalitātes principa un iesaistīto personu tiesību ievērošanu.

Tajā pašā laikā sliekšnis nedrīkst mazināt instrumenta efektivitāti un tā praktisku izmantošanu. Dalībvalstis piemēro dažādus maksimālos soda apmērus spriedumos, kas attiecas uz to valsts sistēmu. Valstu kriminālkodeksi ir atšķirīgi un nav saskaņoti. Tas attiecas uz noziedzīgiem nodarījumiem un tiem piemērojamām sankcijām. Valstu procesuālie kodeksi atšķiras arī attiecībā uz darījumu vai satura datu iegūšanas sliekšņiem: dažas dalībvalstis nenosaka konkrētu sliekšni; citās ir izveidoti noziedzīgu nodarījumu saraksti. Trīs gadu sliekšnis ierobežo instrumenta darbības jomu attiecībā uz smagākiem noziegumiem, pārmērīgi neierobežojot to praktisku izmantošanu. Šis sliekšnis no darbības jomas izslēdz daudzus noziegumus atkarībā no dalībvalsts kriminālkodeksa (piemēram, dažās dalībvalstīs pārrobežu datu e-pierādījumu sniegšanas rīkojumu par vairāk sensitīviem datiem var uzskatīt par neproporcionālu attiecībā uz dalību organizētās noziedzības grupā un nolaupīšanu, kā arī tādiem noziedzīgiem nodarījumiem kā sīkas zādzības, krāpšana un uzbrukums). No otras puses, trīs gadu sliekšnis ietver noziedzīgus nodarījumus, kuru apkarošanai nepieciešama

efektīvāka pieeja; tie ir, piemēram, dalība noziedzīgā organizācijā, teroristu grupu finansēšana, noziedzīgas organizācijas atbalstīšana vai reklamēšana, apmācība teroristu nodarījumu izdarīšanai, konkrēti teroristiski nodarījumi un gatavošanās teroristiska nodarījuma izdarīšanai vai gatavošanās kīlnieku sagrābšanai, kas pretējā gadījumā tiktu izslēgti, ja atkarībā no dalībvalsts tiktu piemērots augstāks sliekšnis. Šis sliekšnis ir izvēlēts, lai visām dalībvalstīm nodrošinātu līdzsvaru starp kriminālizmeklēšanas efektivitāti un tiesību aizsardzību un proporcionalitāti. Sliekšņa piemērošanai ir arī priekšrocība, proti, tas ir vienkārši piemērojams praksē.

Turklāt rīkojumus par darījumu vai satura datu sniegšanu var izdot arī attiecībā uz uzskaitītajiem konkrētiem saskaņotiem nodarījumiem, par kuriem pierādījumi parasti ir pieejami tikai elektroniskā formā. Tas pamato regulas piemērošanu arī lietās, kad maksimālais brīvības atņemšanas sods ir mazāks par iepriekšminēto sliekšni; pretējā gadījumā šos noziedzīgos nodarījumus nevarētu pienācīgi izmeklēt, kā rezultātā nodarījuma izdarītājs varētu palikt nesodīts. *Nodarījumi ir minēti šādu tiesību aktu īpašajos noteikumos:* i) Padomes Pamatlēmums 2001/413/TI par krāpšanas un viltošanas apkarošanu attiecībā uz bezskaidras naudas maksāšanas līdzekļiem, ii) Direktīva 2011/93/ES par seksuālas vardarbības pret bērniem, bērnu seksuālas izmantošanas un bērnu pornogrāfijas apkarošanu un ar ko aizstāj Padomes Pamatlēmumu 2004/68/TI un iii) Direktīva 2013/40/ES par uzbrukumiem informācijas sistēmām un ar ko aizstāj Padomes Pamatlēmumu 2005/222/TI. Rīkojumus var izdot arī par nodarījumiem, kas uzskaitīti Direktīvā 2017/541/ES par terorisma apkarošanu un ar ko aizstāj Padomes Pamatlēmumu 2002/475/TI un groza Padomes Lēmumu 2005/671/TI. Dažiem no šiem nodarījumiem minimālais maksimālais sliekšnis ir vismaz 1 gads, citiem – 2 gadi, bet neviena nav zemāks par maksimālo 1 gada sliekšni.

Šajā pantā noteikta arī obligātā informācija, kura ir jāietver Eiropas e-pierādījumu sniegšanas rīkojumā, lai pakalpojumu sniedzējs varētu identificēt un sniegt pieprasītos datus. Tāpat Eiropas e-pierādījumu sniegšanas rīkojumā ir jāiekļauj pasākuma nepieciešamības un proporcionalitātes pamatojums, norādot pasākuma

Eiropas e-pierādījumu sniegšanas rīkojumu īsteno, izsniedzot Eiropas e-pierādījumu sniegšanas rīkojuma sertifikātu (*EPOC*) (sk. 8. pantu), kas tiek iztulkots un nosūtīts pakalpojumu sniedzējam. *EPOC* ir norādīta tā pati obligātā informācija kā rīkojumā, izņemot norādi par pasākuma nepieciešamību un proporcionalitāti vai sīkāku informāciju par attiecīgo lietu.

Situācijās, kad pieprasītie dati tiek glabāti vai apstrādāti kā daļa no infrastruktūras, ko pakalpojumu sniedzējs nodrošina uzņēmumam — parasti mitināšanas vai programmatūras pakalpojumu gadījumā —, pašam uzņēmumam jābūt galvenajam izmeklēšanas iestāžu pieprasījuma adresātam. Gadījumos, kad uzņēmums nav pakalpojumu sniedzējs, uz kuru attiecas šīs regulas darbības joma, šim nolūkam var būt nepieciešama EIR vai STP procedūra. Eiropas e-pierādījumu sniegšanas rīkojumu var adresēt pakalpojumu sniedzējam tikai tad, ja pieprasījumu nebūtu pareizi adresēt uzņēmumam, jo īpaši, ja tas radītu izmeklēšanas apdraudējuma risku, piemēram, ja ir uzsākta izmeklēšana par pašu uzņēmumu.

Pirms Eiropas e-pierādījumu sniegšanas rīkojuma izdošanas izdevējiestādei arī jāņem vērā iespējamā imunitāte un privilēģijas saskaņā ar pakalpojumu sniedzēja dalībvalsts tiesību aktiem vai ietekmi uz šīs dalībvalsts pamatinteresēm, piemēram, valsts drošību un aizsardzību. Šā noteikuma mērķis ir nodrošināt, lai izdevējvalstī tiek ņemta vērā imunitāte un privilēģijas, kas aizsargā pakalpojumu sniedzēja reģistrācijas dalībvalstī pieprasītos datus, jo īpaši, ja tie nodrošina augstāku aizsardzību nekā izdevējvalsts tiesību akti.

6. pants. Eiropas elektronisko pierādījumu saglabāšanas rīkojuma izdošanas nosacījumi

Eiropas e-pierādījumu saglabāšanas rīkojumam piemērojami līdzīgi nosacījumi kā Eiropas e-pierādījumu sniegšanas rīkojumam. To var izdot par jebkuru noziedzīgu nodarījumu saskaņā ar 6. pantā izklāstītajiem nosacījumiem. Tā mērķis ir novērst attiecīgo datu izņemšanu, dzēšanu vai grozīšanu situācijās, kad šo datu sniegšanai var būt nepieciešams ilgāks laiks, piemēram, tāpēc, ka tiks izmantoti tiesiskās sadarbības kanāli. Piemēram, ņemot vērā to, ka EIR kopumā var izdot par jebkuru pārkāpumu, neierobežojot to ar sliekšņiem, arī Eiropas e-pierādījumu saglabāšanas rīkojums netiks ierobežots. Pretējā gadījumā šis instruments nebūtu efektīvs. Lai izmeklēšanas iestādes varētu ātri rīkoties un, ņemot vērā to, ka attiecīgais datu sniegšanas pieprasījums būs nākamais pieprasījums, kad atkal tiks pārbaudīti visi nosacījumi, prokurors var izdot vai apstiprināt arī Eiropas e-pierādījumu saglabāšanas rīkojumus.

7. pants. Eiropas e-pierādījumu sniegšanas rīkojuma vai Eiropas e-pierādījumu saglabāšanas rīkojuma adresāts

Eiropas e-pierādījumu sniegšanas rīkojumi un Eiropas e-pierādījumu saglabāšanas rīkojumi jāadresē juridiskajam pārstāvim, ko pakalpojumu sniedzējs ir izraudzījis pierādījumu vākšanai kriminālprocesos saskaņā ar direktīvu, ar ko nosaka saskaņotus noteikumus par juridisko pārstāvju iecelšanu pierādījumu vākšanai kriminālprocesos. Nosūtīšanai izmantos Eiropas e-pierādījumu sniegšanas sertifikātu ("EPOC") vai Eiropas e-pierādījumu saglabāšanas rīkojuma sertifikātu ("EPOC-PR"), kā minēts 8. pantā. Minētais juridiskais pārstāvis būs atbildīgs par sertifikātu saņemšanu un savlaicīgu un pilnīgu izpildi. Tādējādi pakalpojumu sniedzēji varēs izvēlēties, kā organizēt dalībvalsts iestāžu prasīto datu sagatavošanu.

Ja juridiskais pārstāvis nav izraudzīts, rīkojumus var adresēt jebkuram pakalpojumu sniedzēja uzņēmumam Savienībā. Šis atkāpšanās risinājums nodrošina sistēmas efektivitāti gadījumā, ja pakalpojumu sniedzējs (vēl) nav izraudzījis īpašu pārstāvi, piemēram, ja nav pienākuma iecelt juridisko pārstāvi saskaņā ar direktīvu, jo pakalpojumu sniedzēji veic uzņēmējdarbību un aktīvi darbojas tikai vienā dalībvalstī, vai gadījumos, kad pienākums iecelt juridisko pārstāvi vēl nav stājies spēkā pirms direktīvas transponēšanas termiņa beigām.

Ja juridiskais pārstāvis nepilda prasības, pastāv divas situācijas, kad izdevējiestāde var vērsties pie jebkura pakalpojumu sniedzēja uzņēmuma Savienībā: ārkārtas gadījumos, kā noteikts 9. panta 2. punktā, un gadījumos, kad juridiskais pārstāvis nepilda 9. un 10. pantā noteiktos pienākumus, un ja izdevējiestāde uzskata, ka pastāv nepārprotams datu zuduma risks.

8. pants. Eiropas e-pierādījumu sniegšanas un e-pierādījumu saglabāšanas rīkojuma sertifikāts

EPOC un EPOC-PR ir paredzēti rīkojumu nosūtīšanai adresātam, kā definēts 7. pantā. Abu sertifikātu veidlapas ir iekļautas regulas I un II pielikumā; tās ir jāiztulko vienā no tās dalībvalsts oficiālajām valodām, kurā atrodas adresāts. Pakalpojumu sniedzējs var paziņot, ka rīkojumi tiks pieņemti arī citās Savienības oficiālajās valodās. Sertifikātu mērķis ir nodrošināt visu nepieciešamo informāciju, kas jānosūta adresātam standartizētā formātā, minimizējot kļūdu avotus, ļaujot viegli identificēt datus un pēc iespējas izvairoties no brīvā teksta, tādējādi samazinot tulkošanas izmaksas. Pilns pamatojums, kā arī iemesli nepieciešamības un proporcionālītātes principa ievērošanai vai sīkāka informācija par lietu netiek iekļauta

sertifikātā, lai neapdraudētu izmeklēšanu. Tādēļ tas ir nepieciešams tikai kā daļa no paša rīkojuma, lai vēlāk ļautu aizdomās turētajai personai apstrīdēt to kriminālprocesa laikā.

Daži pakalpojumu sniedzēji jau ir izveidojuši platformas tiesībaizsardzības iestāžu pieprasījumu iesniegšanai. Ar šo regulu netiek novērsta šo platformu izmantošana, jo tās piedāvā daudzas priekšrocības, tostarp vienkāršu autentifikācijas iespēju un datu drošu nosūtīšanu. Tomēr šīm platformām jāļauj iesniegt *EPOC* un *EPOC-PR* formātā, kas paredzēts I un II pielikumā, nepieprasot iesniegt papildu datus, kas attiecas uz rīkojumu.

Tāpat dalībvalstu vai Savienības struktūru izveidotās platformas var nodrošināt drošus nosūtīšanas veidus un atvieglot rīkojumu autentificēšanu un statistikas vākšanu. Būtu jāapsver iespēja paplašināt *eCodex* un *SIRIUS* platformas, iekļaujot drošu savienojumu ar pakalpojumu sniedzējiem, lai nosūtītu *EPOC* un *EPOC-PR*, kā arī — ja nepieciešams — atbildes no pakalpojumu sniedzējiem.

9. pants. EPOC izpilde

9. pants uzliek adresātiem pienākumu atbildēt uz *EPOC* un ievieš obligātus termiņus. Parastais termiņš ir 10 dienas, tomēr iestādes var noteikt īsāku termiņu, ja tas ir pamatoti. Turklāt ārkārtas gadījumos, kas definēti kā situācija, kad ir apdraudēta personas dzīvība vai fiziska neaizskaramība, vai kritiskā infrastruktūra, termiņš ir 6 stundas.

Turklāt šis noteikums nodrošina dialoga iespēju starp adresātu un izdevējiestādi. Ja *EPOC* ir nepilnīgs, acīmredzami nepareizs vai tajā nav pietiekamas informācijas, lai pakalpojumu sniedzējs varētu izpildīt *EPOC*, adresāts sazinās ar izdevējiestādi un lūdz precizējumu, izmantojot III pielikumā iekļauto veidlapu. Tāpat pakalpojumu sniedzējs informē izdevējiestādi gadījumos, kad tas nevar sniegt datus nepārvaramas varas apstākļu dēļ vai tādēļ, ka tas faktiski nav iespējams. Tas būtu attiecināms uz gadījumu, ja, piemēram, persona, kuras dati tiek pieprasīti, nav šā pakalpojuma klients vai — piemēram, atbilstīgi citām privātuma prasībām — pakalpojumu sniedzējs ir likumīgi izdzēsis datus, pirms viņš vai tā juridiskais pārstāvis saņēma rīkojumu. Izdevējiestādei būtu jābūt informētai par šiem apstākļiem, lai tā varētu ātri reaģēt un, iespējams, vākt elektroniskos pierādījumus no cita pakalpojumu sniedzēja, tādējādi novēršot, ka izdevējiestāde uzsāk izpildes procedūru gadījumā, kad tas nebūtu lietderīgi.

Ja adresāts vispār nesniedz informāciju vai nenodrošina izsmeļošu vai savlaicīgu informāciju citu iemeslu dēļ, kas nav minēti iepriekš, viņam ir jāinformē izdevējiestāde par šiem iemesliem, izmantojot III pielikumā iekļauto veidlapu. Tādēļ adresāti var lūgt izdevējiestādei precizējumu par jebkuru jautājumu, kas saistīts ar *EPOC* izpildi. Tas ļauj izdevējiestādei izlabot vai pārskatīt *EPOC* sākuma stadijā pirms izpildes posma.

Ja dati netiek sniegti nekavējoties, jo īpaši, ja starp adresātu un izdevējiestādi ir uzsākts dialogs, kas nozīmē, ka 9. panta 1. punktā norādītie termiņi netiks ievēroti, pakalpojumu sniedzējam ir pienākums saglabāt datus, lai novērstu to zudumu pēc *EPOC* saņemšanas ar noteikumu, ka datus ir iespējams identificēt. Saglabāšana var attiekties uz precizēto *EPOC* vai vēlāku STP vai EIR pieprasījumu, kas tiks nosūtīts sākotnējā *EPOC* vietā.

10. pants. EPOC-PR izpilde

Lai izpildītu *EPOC-PR*, jā saglabā rīkojuma saņemšanas brīdī pieejamie dati. Pakalpojumu sniedzējiem jā saglabā dati, ciktāl tas nepieciešams, lai sniegtu datus pēc pieprasījuma, ar nosacījumu, ka izdevējiestāde 60 dienu laikā pēc rīkojuma izdošanas apstiprina, ka tā ir

izdevusi nākamo pieprasījumu sniegt datus. Šim nolūkam ir jāveic vismaz daži oficiāli pasākumi, piemēram, savstarpējas tiesiskās palīdzības pieprasījuma nosūtīšana tulkošanai.

No otras puses, datu saglabāšanas pieprasījumus vajadzētu veikt vai datus saglabāt tikai tik ilgi, cik tas ir nepieciešams, lai varētu iesniegt vēlāku pieprasījumu šo datu sniegšanai. Lai novērstu datu nevajadzīgu vai pārmērīgi ilgu saglabāšanu, iestāde, kas izdevusi Eiropas e-pierādījumu saglabāšanas rīkojumu, informē adresātu, tiklīdz ir pieņemts lēmums neizdot vai anulēt datu sniegšanas rīkojumu vai tiesiskās sadarbības lūgumu.

Šis noteikums arī nodrošina adresāta un izdevējiestādes dialoga iespēju līdzīgi 9. panta noteikumiem. Ja *EPOC-PR* ir nepilnīgs, acīmredzami nepareizs vai tajā nav pietiekamas informācijas, lai pakalpojumu sniedzējs varētu izpildīt *EPOC-PR*, adresāts sazinās ar izdevējiestādi un lūdz precizējumu, izmantojot III pielikumā iekļauto veidlapu. Tāpat pakalpojumu sniedzējs informē izdevējiestādi gadījumos, kad tas nevar sniegt datus nepārvaramas varas apstākļu dēļ vai tādēļ, ka tas faktiski nav iespējams.

11. pants. Konfidencialitāte un lietotāja informācija

Jānodrošina konfidencialitāte attiecībā uz notiekošu izmeklēšanu, tostarp faktu, ka ir izdots rīkojums par attiecīgo datu sniegšanu. Šis pants pamatojas uz EIR direktīvas 19. pantu. Tas paredz pienākumu adresātam un pakalpojumu sniedzējam, ja tās ir dažādas personas, saglabāt *EPOC* vai *EPOC-PR* konfidencialitāti, proti, neinformēt personu, kuras dati tiek pieprasīti, ja to pieprasa izdevējiestāde, lai aizsargātu noziedzīgu nodarījumu izmeklēšanu saskaņā ar VDAR 23. pantu.

No otras puses, ir svarīgi, tostarp tiesiskās aizsardzības līdzekļu izmantošanas nolūkā, lai persona, kuras dati tika pieprasīti, būtu par to informēta. Ja pakalpojumu sniedzējs to nedara pēc izdevējiestādes pieprasījuma, izdevējiestāde saskaņā ar Tiesībaizsardzības direktīvas 13. pantu informē personu, tiklīdz vairs nepastāv izmeklēšanas apdraudējuma risks, un ietver informāciju par pieejamajiem tiesiskās aizsardzības līdzekļiem. Šāda informācija tiek sniegta tikai attiecībā uz Eiropas e-pierādījumu sniegšanas rīkojumiem, jo šādā gadījumā būs mazāks tiesību ierobežojums, bet netiek sniegta Eiropas e-pierādījumu saglabāšanas rīkojuma gadījumā.

12. pants. Izmaksu atlīdzināšana

Ja to paredz izdevējvalsts tiesību akti par iekšzemes rīkojumiem līdzīgās iekšējās lietās, pakalpojumu sniedzēji var arī pieprasīt izdevumu atlīdzināšanu no izdevējvalsts saskaņā ar izdevējvalsts tiesību aktiem. Tas nodrošina vienlīdzīgu attieksmi pret tiem pakalpojumu sniedzējiem, uz kuriem attiecas iekšzemes rīkojums un tās pašas dalībvalsts adresēts *EPOC*, ja šī dalībvalsts ir izvēlējusies atlīdzināt izdevumus konkrētiem pakalpojumu sniedzējiem. No otras puses, ierosinātā regula nesaskaņo izdevumu atlīdzināšanu, jo dalībvalstis šajā ziņā ir izvēlējušās atšķirīgu izvēli.

Izdevumu atlīdzināšanu var pieprasīt tieši pakalpojumu sniedzējs vai tā juridiskais pārstāvis. Izdevumus var atlīdzināt tikai vienu reizi.

3. nodaļa. Sankcijas un to izpilde

13. pants. Sankcijas

Dalībvalstis nodrošina iedarbīgu, samērīgu un atturošu naudas sodu piemērošanu, ja pakalpojumu sniedzēji nepilda savas saistības saskaņā ar 9., 10. vai 11. pantu. Tas neskar valstu tiesību aktus, kas paredz kriminālsodu piemērošanu šādās situācijās.

14. pants. Izpildes procedūra

Regulas 14. pants paredz procedūru rīkojumu izpildei prasību neievērošanas gadījumā, izmantojot dalībvalsts palīdzību, kurā atrodas nosūtītā sertifikāta adresāts. Atkarībā no sākotnējā adresāta tā ir vai nu pakalpojumu sniedzēja, vai juridiskā pārstāvja dalībvalsts. Izdevējiestāde pilnībā nosūta rīkojumu, tostarp nepieciešamības un proporcionalitātes pamatojumu, kam pievienots sertifikāts, izpildes valsts kompetentajai iestādei, kura to izpilda saskaņā ar savas valsts tiesību aktiem, vajadzības gadījumā piemērojot 13. panta minētās sankcijas. Ja rīkojums ir nosūtīts izpildes nodrošināšanai uz izpildes valsti, izpildes iestāde pēc apspriešanās ar izdevējiestādi var nolemt neatzīt un neizpildīt rīkojumu, ja, saņemot rīkojumu, tā uzskata, ka ir piemērojams kāds no ierobežotajiem iebildumu pamatojumiem. Turklāt, ja tiek uzsākta piespiedu izpildes procedūra, adresāts pats varēs iebilst pret rīkojumu izpildes iestādē. Adresāts to var darīt, balstoties uz jebkuru no šādiem pamatojumiem, izņemot imunitāti un privilēģijas, kā arī gadījumus, kad ir skaidrs, ka rīkojumu nav izdevusi vai nav apstiprinājusi kompetentā iestāde vai arī ka šāda prasību izpilde būtu vērtējama kā Eiropas Savienības Pamattiesību hartas acīmredzams pārkāpums vai acīmredzama ļaunprātība. Piemēram, rīkojums par tādu satura datu sniegšanu, kas attiecas uz nenoteiktu cilvēku grupu kādā ģeogrāfiskajā apgabalā vai kam nav norādīta saikne ar konkrētu kriminālprocesu, acīmredzami ignorētu šajā regulā noteiktos Eiropas e-pierādījumu sniegšanas rīkojuma izdošanas nosacījumus, un tas izrietētu jau no paša sertifikāta satura. Citus pamatojumus var norādīt tikai tā persona, kuras dati tiek pieprasīti, saskaņā ar tās tiesiskās aizsardzības līdzekļiem izdevējā valstī (sk. turpmāk 17. pantu). Turklāt pakalpojumu sniedzējiem ir pieejams tiesiskās aizsardzības līdzeklis pret izpildes iestādes lēmumu par soda piemērošanu.

Lai novērstu turpmākus kavējumus šīs procedūras laikā, izpildes procedūrā ir paredzēti vairāki termiņi izpildes iestādei un izdevējiestādei.

4. nodaļa. Tiesiskās aizsardzības līdzekļi

Regulas 15. un 16. pants. Pārskatīšanas procedūra pretrunīgu pienākumu gadījumā, kuri izriet no trešās valsts tiesību aktiem

Regulas 15. un 16. pants paredz pārskatīšanas procedūru gadījumos, kad pakalpojumu sniedzējiem, kuru galvenā mītne atrodas trešās valstīs, saskaras ar pretrunīgiem pienākumiem. Turklāt šie noteikumi ir ļoti svarīgi, lai nodrošinātu indivīdu un starptautiskās sabiedrības tiesības. Nosakot augstu standartu, to mērķis ir mudināt trešās valstis nodrošināt līdzīgu aizsardzības līmeni. Pretējā gadījumā, ja trešās valsts iestādes cenšas iegūt ES pilsoņa datus no ES pakalpojumu sniedzēja, Savienības vai dalībvalstu tiesību akti, kas aizsargā pamattiesības, piemēram, datu aizsardzības *acquis*, var līdzīgā veidā novērst informācijas izpaušanu. Eiropas Savienība sagaida, ka trešās valstis ievēros šādus aizliegumus, kā to paredz šis priekšlikums.

Adresāts var uzsākt 15. pantā paredzēto procedūru, ja Eiropas e-pierādījumu sniegšanas rīkojuma izpildes rezultātā tiktu pārkāpts(-i) trešās valsts tiesību akts(-i), kas aizliedz datu izpaušanu, pamatojoties uz nepieciešamību aizsargāt attiecīgo personu pamattiesības vai trešās valsts pamatintereses, kuras saistītas ar valsts drošību vai aizsardzību. Adresātam ir jāinformē izdevējiestāde par savu secinājumu, ka pastāv pretrunīgi pienākumi, un jāiesniedz pamatoti iebildumi. Šādu pamatotu iebildumu nevar pamatot tikai ar faktu, ka trešās valsts tiesību aktos nav līdzīgu noteikumu, vai arī tikai ar apstākli, ka dati tiek glabāti trešā valstī. Pamatotu iebildumu izvirza saskaņā ar 9. panta 5. punktā noteikto procedūru paziņojumam par nodomu neievērot prasības, izmantojot III pielikumā paredzēto veidlapu.

Pamatojoties uz šo pamatoto iebildumu, izdevējiestāde pārskata savu rīkojumu. Ja izdevējiestāde nolemj atcelt rīkojumu, procedūra tiek izbeigta. Ja izdevējiestāde vēlas apstiprināt rīkojumu, lietu nodod tās dalībvalsts kompetentajai tiesai. Tad tiesa, pamatojoties uz pamatoto iebildumu un ņemot vērā visus būtiskos lietas faktus, izvērtē, vai konkrētā gadījumā ir piemērojami trešās valsts tiesību akti un — ja tas tā ir — vai konkrētajā gadījumā pastāv konflikts. Veicot šo novērtējumu, tiesai būtu jāņem vērā, vai trešās valsts tiesību akti tā vietā, lai aizsargātu pamattiesības vai trešās valsts pamatintereses, kas saistītas ar valsts drošību vai aizsardzību, acīmredzami cenšas aizsargāt citas intereses vai arī ir vērsti uz to, lai kriminālizmeklēšanas ietvaros aizsargātu nelikumīgas darbības no tiesībaizsardzības iestāžu pieprasījumiem.

Ja tiesa konstatē, ka šajā gadījumā pastāv faktiska pretruna ar pienākumiem, kas izriet no tiesību aktiem, kuri aizsargā personu pamattiesības vai trešās valsts pamatintereses saistībā ar valsts drošību vai aizsardzību, tiesai ar trešās valsts centrālo iestāžu starpniecību jāpieprasa attiecīgās trešās valsts atzinums. Ja trešā valsts, ar kuru notikusi apspriešanās, apstiprina konflikta pastāvēšanu un iebilst pret rīkojuma izpildi, tiesai ir jāatsauc rīkojums.

Ja konflikts rodas, pamatojoties uz citiem trešo valstu tiesību aktiem, kas nav paredzēti, lai aizsargātu personas pamattiesības vai trešās valsts pamatintereses saistībā ar valsts drošību vai aizsardzību, tiesa pieņem lēmumu, līdzsvarojot intereses par labu rīkojumam un pret rīkojuma apstiprināšanu..

Regulas 9. pantā norādītie nosacījumi, jo īpaši 9. panta 6. punktā izklāstītie e-pierādījumu pienākumi, ir piemērojami arī gadījumos, kad rodas pretrunīgi pienākumi, kas izriet no trešās valsts tiesību aktiem. Ja tiesa konstatē, ka rīkojums ir jāapstiprina, izdevējiestāde un pakalpojumu sniedzējs tiek informēti, lai turpinātu rīkojuma izpildi. Ja rīkojums tiek atcelts, var izdot atsevišķu Eiropas e-pierādījumu saglabāšanas rīkojumu, lai nodrošinātu datu pieejamību, ja tos var iegūt, pamatojoties uz savstarpējas tiesiskās palīdzības pieprasījumu.

Ņemot vērā to, ka Eiropas e-pierādījumu saglabāšanas rīkojums pats par sevi nav datu izpaušana un līdz ar to nerada līdzīgas bažas, pārskatīšanas procedūra attiecas tikai uz Eiropas e-pierādījumu sniegšanas rīkojumu.

17. pants. Efektīvi tiesiskās aizsardzības līdzekļi

Šis noteikums nodrošina efektīvu tiesiskās aizsardzības līdzekļu pieejamību personām, uz kurām attiecas Eiropas e-pierādījumu sniegšanas rīkojums. Šos tiesiskās aizsardzības līdzekļus izmanto izdevējvalstī saskaņā ar valsts tiesību aktiem. Aizdomās turētajām un apsūdzētajām personām tiesiskās aizsardzības līdzekļi parasti tiek nodrošināti kriminālprocesa laikā. Eiropas e-pierādījumu saglabāšanas rīkojumam, kas pats par sevi nepieļauj datu izpaušanu, nav pieejami īpaši aizsardzības līdzekļi, izņemot gadījumus, kad pēc šā rīkojuma tiek izdots Eiropas e-pierādījumu sniegšanas rīkojums vai cits instruments, kā rezultātā tiek izpausta informācija, kas liek nodrošināt īpašus tiesiskās aizsardzības līdzekļus.

Personām, kuru dati tika lūgti, lai gan tās nav aizdomās turētās vai apsūdzētās personas kriminālprocesā, arī ir tiesības izmantot tiesiskās aizsardzības līdzekli izdevējvalstī. Visas šīs tiesības neierobežo nekādus tiesiskās aizsardzības līdzekļus, kas pieejami saskaņā ar Tiesību aizsardzības un VDAR.

Pretstatā pakalpojumu sniedzējiem regula neierobežo visu visu šo personu iespējamo pamatojumu, lai apstrīdētu rīkojuma likumību. Šie pamatojumi ietver rīkojuma nepieciešamību un proporcionalitāti.

Tiesiskās aizsardzības līdzekļu izmantošana izdevējvalstī nerada nesamērīgu apgrūtinājumu iesaistītajām personām. Līdzīgi kā ar rīkojumiem, kurus izpilda, izmantojot citas tiesu iestāžu sadarbības formas, izdevējvalsts tiesām ir vislabākās iespējas pārskatīt to iestāžu izdotu Eiropas e-pierādījumu sniegšanas rīkojumu likumību un novērtēt saderību ar to valsts tiesību aktiem. Turklāt izpildes posmā adresāti var atsevišķi iebilst pret *EPOC* vai *EPOC-PR* izpildi savā uzņēmējvalstī, pamatojoties uz regulā uzskaitīto pamatojumu sarakstu (sk. iepriekš 14. pantu).

18. pants. Privilēģiju un imunitātes nodrošināšana saskaņā ar uzņēmējvalsts tiesību aktiem

Šis noteikums paredzēts tādām pašām mērķim kā 5. panta 7. punkts — nodrošināt, lai izdevējvalstī tiktu ņemta vērā imunitāte un privilēģijas, kas aizsargā pakalpojumu sniedzēja dalībvalstī pieprasītos datus, jo īpaši, ja starp šīm dalībvalstīm pastāv atšķirības, kā arī šīs dalībvalsts pamatintereses, piemēram, valsts drošību un aizsardzību. Regulas 18. pants nosaka, ka izdevējvalsts tiesai tās ir jāņem vērā tādā pašā mērā kā tad, ja to paredzētu šīs valsts tiesību akti. Ņemot vērā atšķirības starp dalībvalstīm attiecībā uz pierādījumu atbilstības un pieļaujamības izvērtēšanu, noteikums sniedz tiesai zināmu rīcības brīvību attiecībā uz to, kā tās ņemt vērā.

5. nodaļa. Nobeiguma noteikumi

19. pants. Uzraudzība un ziņošana

Šis pants nosaka, ka dalībvalstīm jāiesniedz īpaša informācija par regulas piemērošanu, lai palīdzētu Komisijai pildīt savus pienākumus saskaņā ar 24. pantu. Komisija izveido sīki izstrādātu programmu šīs regulas iznākumu, rezultātu un ietekmes uzraudzībai.

20. pants. Grozījumi sertifikātos un veidlapās

Šā priekšlikuma I, II un III pielikumā ietvertie sertifikāti un veidlapas atvieglos *EPOC* un *EPOC-PR* izpildi. Tādēļ ir nepieciešams, lai nākotnē būtu iespēja vērst uzmanību uz iespējamo nepieciešamību pēc iespējas ātrāk uzlabot sertifikāta un veidlapas saturu. Grozījumi trīs pielikumos ar parastās likumdošanas procedūras palīdzību neatbilst šai prasībai, un tie ir nebūtiski normatīvo aktu elementi, savukārt galvenie elementi ir definēti 8. pantā. Tādēļ 20. pantā ir paredzēta ātrāka un elastīgāka procedūra grozījumu veikšanai, izmantojot deleģētos aktus.

21. pants. Deleģēšanas izpilde

Šis pants nosaka nosacījumus, saskaņā ar kuriem Komisijai ir tiesības pieņemt deleģētos aktus, lai nodrošinātu nepieciešamos grozījumus sertifikātā un priekšlikumam pievienotajās veidlapās. Tas paredz standarta procedūru šādu deleģēto aktu pieņemšanai.

22. pants. Paziņojumi

Dalībvalstīm ir jāpaziņo Komisijai, kuras ir kompetentās izdevējiestādes un izpildes iestādes un kuras tiesas ir tiesīgas izskatīt pakalpojumu sniedzēju pamatotos iebildumus tiesību normu kolīziju gadījumā.

23. pants. Saistība ar Eiropas e-pierādījumu sniegšanas rīkojumiem

Šis noteikums precizē, ka regula neliedz dalībvalstu iestādēm izdot Eiropas izmeklēšanas rīkojumus saskaņā ar Direktīvu 2014/41/ES, lai iegūtu elektroniskos pierādījumus.

24. pants. Izvērtējums

Šis noteikums nosaka, ka Komisija veic šīs regulas izvērtējumu saskaņā ar Komisijas labāka regulējuma pamatnostādņēm un saskaņā ar 2016. gada 13. aprīļa Iestāžu nolīguma 22. punktu²⁵. Piecus gadus pēc ierosinātās regulas stāšanās spēkā Komisija ziņos Eiropas Parlamentam un Padomei par izvērtējuma rezultātiem, kā arī izvērtēs vajadzību paplašināt tās darbības jomu uz pakalpojumiem, kas vēl nav ietverti, taču var kļūt nozīmīgāki izmeklēšanā.

25. pants. Stāšanās spēkā

Ierosinātā regula stāsies spēkā divdesmitajā dienā pēc tās publicēšanas Oficiālajā Vēstnesī. Pēc tam regula būs piemērojama 6 mēnešus pēc tās stāšanās spēkā.

²⁵ Iestāžu 2016. gada 13. aprīļa nolīgums starp Eiropas Parlamentu, Eiropas Savienības Padomi un Eiropas Komisiju par labāku likumdošanas procesu; OV L 123, 12.5.2016. 1.–14. lpp.

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES REGULA

**Par Eiropas elektronisko pierādījumu sniegšanas un saglabāšanas rīkojumiem
elektronisko pierādījumu gūšanai krimināllietās**

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību (LESD) un jo īpaši tā 82. panta 1. punktu,
ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu²⁶,

saskaņā ar parasto likumdošanas procedūru,

Tā kā:

- 1) Savienība ir izvirzījusi mērķi saglabāt un attīstīt brīvības, drošības un tiesiskuma telpu. Lai pakāpeniski izveidotu šādu telpu, Savienība pieņem pasākumus attiecībā uz tiesu iestāžu sadarbību krimināllietās, pamatojoties uz spriedumu un tiesas lēmumu savstarpējas atzīšanas principu, ko parasti dēvē par stūrakmeni tiesu iestāžu sadarbībai krimināllietās Eiropas Savienībā kopš Eiropadomes Tampere sanāksmes 1999. gada 15. un 16. oktobrī.
- 2) Pasākumi elektronisko pierādījumu iegūšanai un saglabāšanai kļūst arvien nozīmīgāki, lai nodrošinātu kriminālizmeklēšanu un kriminālvajāšanu visā Savienībā. Efektīvi mehānismi elektronisko pierādījumu iegūšanai ir būtiski noziedzības apkarošanai, vienlaikus ievērojot nosacījumus, lai nodrošinātu pilnīgu atbilstību pamattiesībām un principiem, kas atzīti Līgumos ietvertajā Eiropas Savienības Pamattiesību hartā, jo īpaši nepieciešamības un proporcionālītātes principi, pienācīgs process, datu aizsardzība, sarakstes noslēpums un privātums.
- 3) Tieslietu un iekšlietu ministru un Savienības iestāžu pārstāvju kopīgajā 2016. gada 22. marta paziņojumā par teroristu uzbrukumiem Briselē tika uzsvērts, ka prioritārā kārtā nepieciešams atrast veidus, kā ātrāk un efektīvāk nodrošināt un iegūt elektroniskos pierādījumus un noteikt konkrētus pasākumus šā jautājuma risināšanai.
- 4) Padomes 2016. gada 9. jūnija secinājumos uzsvērts, ka arvien lielāka nozīme ir elektroniskiem pierādījumiem kriminālprocesos un ekonomikas un sabiedrības labā kibertelpas aizsardzībai pret ļaunprātīgu izmantošanu un noziedzīgām darbībām, tādēļ tiesībaizsardzības un tiesu iestādēm ir vajadzīgi efektīvi līdzekļi, lai veiktu izmeklēšanu un sauktu pie atbildības par noziedzīgiem nodarījumiem, kas saistīti ar kibertelpu.
- 5) Komisija 2017. gada 13. septembra Kopīgajā paziņojumā "Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību"²⁷ uzsvēra, ka efektīva

²⁶ OV C , , lpp.

kibernoziegumu izmeklēšana un kriminālvajāšana ir galvenais faktors, kas attur no kibernoziegumu veikšanas, un ka pašreizējo procesuālo regulējumu nepieciešams labāk pielāgot interneta laikmetam. Spēkā esošās procedūras reizēm nespēja atbilstoši ātri reaģēt uz kiberuzbrukumiem, tādēļ ir īpaši nepieciešama ātra pārrobežu sadarbība.

- 6) Savā 2017. gada 3. oktobra Rezolūcijā par cīņu pret kibernoziegumiem²⁸ Eiropas Parlaments pievienojās šīm bažām, uzsverot problēmas, kādas šobrīd sadrumstalotais tiesiskais regulējums var radīt pakalpojumu sniedzējiem, kuri vēlas izpildīt tiesībsardzības prasības, un aicināja Komisiju nākt klajā ar Savienības elektronisko pierādījumu tiesisko regulējumu, nodrošinot pietiekamus aizsardzības līdzekļus visu iesaistīto personu tiesībām un brīvībām.
- 7) Tīkla pakalpojumus var nodrošināt no jebkuras vietas, un tiem nav vajadzīga fiziskā infrastruktūra, telpas vai personāls attiecīgajā valstī. Tāpēc attiecīgos pierādījumus bieži glabā ārpus izmeklēšanas valsts vai to dara pakalpojumu sniedzējs, kas veic uzņēmējdarbību ārpus šīs valsts. Bieži vien nav nekādas citas saiknes starp izmeklējamu lietu attiecīgajā valstī un valsti, kurā pakalpojumu sniedzējs glabā datus vai atrodas tā galvenā uzņēmējdarbības vieta.
- 8) Šīs saiknes neesības dēļ tiesiskās sadarbības lūgumi bieži tiek adresēti valstīm, kurās ir liels pakalpojumu sniedzēju skaits, taču nav citas saistības ar attiecīgo lietu. Turklāt pieprasījumu skaits ir palielinājies, ņemot vērā to, ka arvien vairāk tiek izmantoti tīklu pakalpojumi, kuriem pēc būtības nav robežu. Tādēļ elektronisko pierādījumu iegūšanai, izmantojot tiesiskās sadarbības kanālus, bieži vien ir vajadzīgs ilgs laiks — ilgāks, nekā sekojošās norādes varētu būt pieejamas. Turklāt nav skaidra regulējuma sadarbībai ar pakalpojumu sniedzējiem, vienlaikus daži trešo valstu pakalpojumu sniedzēji pieņem tiešus pieprasījumus pēc datiem, kas nav saturs, kā to ļauj šo valstu piemērojamie tiesību akti. Tādēļ visas dalībvalstis paļaujas uz pieejamajiem sadarbības kanāliem ar pakalpojumu sniedzējiem, izmantojot dažādus valstu instrumentus, nosacījumus un procedūras. Turklāt attiecībā uz satura datiem dažas dalībvalstis ir piemērojušas vienpusējus pasākumus, savukārt citas turpina paļauties uz tiesisko sadarbību.
- 9) Sadrumstalotais tiesiskais regulējums rada problēmas pakalpojumu sniedzējiem, kuri vēlas izpildīt tiesībsardzības prasības. Tādēļ ir nepieciešams izstrādāt Eiropas tiesisko regulējumu attiecībā uz elektroniskiem pierādījumiem, lai uzliktu pienākumu tiem pakalpojumu sniedzējiem, uz kuriem attiecas instrumenta darbības joma, bez tiesu iestādes iesaistīšanas pakalpojumu sniedzēja dalībvalstī sniegt atbildi tieši iestādēm.
- 10) Rīkojumi saskaņā ar šo regulu būtu jāadresē šīm mērķim izraudzītajiem pakalpojumu sniedzēju juridiskajiem pārstāvjiem. Ja pakalpojumu sniedzējs, kas veic uzņēmējdarbību Savienībā, nav izraudzījies juridisko pārstāvi, rīkojumus var adresēt jebkuram šā pakalpojumu sniedzēja uzņēmumam Savienībā. Šī atkāpšanās iespēja palīdz nodrošināt sistēmas efektivitāti, ja pakalpojumu sniedzējs (vēl) nav iecēlis īpašu pārstāvi.
- 11) Eiropas e-pierādījumu sniegšanas rīkojums un Eiropas e-pierādījumu saglabāšanas rīkojums elektronisko pierādījumu iegūšanai krimināllietās var darboties, tikai

²⁷ JOIN(2017) 450 final.

²⁸ 2017/2068(INI).

pamatojoties uz augstu savstarpējās uzticēšanās līmeni starp dalībvalstīm, kas ir būtisks priekšnoteikums šā instrumenta pareizai darbībai.

- 12) Šajā regulā ir ievērotas pamattiesības un principi, kas ir jo īpaši atzīti Eiropas Savienības Pamattiesību hartā. Tie ietver tiesības uz brīvību un drošību, privātās un ģimenes dzīves neaizskaramību, personas datu aizsardzību, darījumdarbības brīvību, tiesības uz īpašumu, tiesības uz efektīvu tiesību aizsardzību un taisnīgu tiesu, nevainīguma prezumpciju un tiesības uz aizstāvību, likumības un proporcionalitātes principus, kā arī tiesības netikt divreiz tiesātam vai sodītam krimināllietā par to pašu noziedzīgo nodarījumu. Ja izdevējai dalībvalstij ir norādes par paralēla kriminālprocesa iespējamu norisi citā dalībvalstī, tā apspriežas ar šīs dalībvalsts iestādēm saskaņā ar Padomes Pamatlēmumu 2009/948/TI²⁹.
- 13) Lai garantētu pamattiesību pilnīgu ievērošanu, šajā regulā ir skaidri norādīti nepieciešamie standarti attiecībā uz jebkādu personas datu iegūšanu, šādu datu apstrādi, pārskatīšanu tiesā attiecībā uz šajā instrumentā paredzētā izmeklēšanas pasākuma izmantošanu un pieejamie tiesiskās aizsardzības līdzekļi.
- 14) Šī regula būtu jāpiemēro, neskarot procesuālās tiesības kriminālprocesā, kas noteiktas Eiropas Parlamenta un Padomes Direktīvās 2010/64/ES³⁰, 2012/13/ES³¹, 2013/48/ES³², 2016/343³³, 2016/800³⁴ un 2016/1919³⁵.
- 15) Šajā instrumentā ir paredzēti noteikumi, saskaņā ar kuriem kompetentā tiesu iestāde Eiropas Savienībā, izdodot Eiropas e-pierādījumu sniegšanas vai saglabāšanas rīkojumu, var pieprasīt pakalpojumu sniedzējam, kas Savienībā piedāvā pakalpojumus, sniegt vai saglabāt elektroniskos pierādījumus. Šī regula ir piemērojama visos gadījumos, kad pakalpojumu sniedzējs veic uzņēmējdarbību vai ir pārstāvēts citā dalībvalstī. Attiecībā uz iekšzemes situācijām, kad šajā regulā paredzētos instrumentus nevar izmantot, regulai nevajadzētu ierobežot valsts kompetento iestāžu pilnvaras, kas jau ir noteiktas valsts tiesību aktos, uzlikt pienākumus pakalpojumu sniedzējiem, kuri veic uzņēmējdarbību vai ir pārstāvēti to teritorijā.
- 16) Kriminālprocesā vissvarīgākie pakalpojumu sniedzēji ir elektronisko sakaru pakalpojumu sniedzēji un konkrēti informācijas sabiedrības pakalpojumu sniedzēji,

²⁹ [Padomes Pamatlēmums 2009/948/TI](#) (2009. gada 30. novembris) par jurisdikcijas īstenošanas konfliktu novēršanu un atrisināšanu kriminālprocesā (OV L 328, 15.12.2009., 42. lpp.).

³⁰ Eiropas Parlamenta un Padomes [Direktīva 2010/64/ES](#) (2010. gada 20. oktobris) par tiesībām uz mutisko un rakstisko tulkojumu kriminālprocesā (OV L 280, 26.10.2010., 1. lpp.).

³¹ Eiropas Parlamenta un Padomes [Direktīva 2012/13/ES](#) (2012. gada 22. maijs) par tiesībām uz informāciju kriminālprocesā (OV L 142, 1.6.2012., 1. lpp.).

³² Eiropas Parlamenta un Padomes [Direktīva 2013/48/ES](#) (2013. gada 22. oktobris) par tiesībām uz advokāta palīdzību kriminālprocesā un Eiropas apcietināšanas ordera procesā, par tiesībām uz to, ka pēc brīvības atņemšanas informē trešo personu, un par tiesībām, kamēr atņemta brīvība, sazināties ar trešām personām un konsulārajām iestādēm (OV L 294, 6.11.2013., 1. lpp.).

³³ Eiropas Parlamenta un Padomes [Direktīva \(ES\) 2016/343](#) (2016. gada 9. marts) par to, lai nostiprinātu konkrētus nevainīguma prezumpcijas aspektus un tiesības piedalīties klātienē lietas izskatīšanā tiesā kriminālprocesā (OV L 65, 11.3.2016., 1. lpp.).

³⁴ Eiropas Parlamenta un Padomes [Direktīva \(ES\) 2016/800](#) (2016. gada 11. maijs) par procesuālajām garantijām bērniem, kuri ir aizdomās turētie vai apsūdzētie kriminālprocesā (OV L 132, 21.5.2016., 1. lpp.).

³⁵ Eiropas Parlamenta un Padomes [Direktīva \(ES\) 2016/1919](#) (2016. gada 26. oktobris) par juridisko palīdzību aizdomās turētajiem un apsūdzētajiem kriminālprocesā un pieprasītajām personām Eiropas apcietināšanas ordera procesā (OV L 297, 4.11.2016., 1. lpp.).

kas veicina mijiedarbību starp lietotājiem. Tādējādi šai regulai vajadzētu attiekties uz abām grupām. Elektronisko sakaru pakalpojumu sniedzēji ir definēti priekšlikumā direktīvai, ar ko izveido Eiropas Elektronisko sakaru kodeksu. Tie ietver starppersonu saziņu, piemēram, IP balss pārraidi, tūlītējās ziņapmaiņas un e-pasta pakalpojumus. Šeit ietvertie informācijas sabiedrības pakalpojumu veidi ir tie, attiecībā uz kuriem datu glabāšana ir lietotājam sniegtā pakalpojuma pamatelements, un jo īpaši attiecas uz sociālajiem tīkliem, ciktāl tie nav elektronisko sakaru pakalpojumi, uz tiešsaistes tirgiem, kas sekmē darījumus starp to lietotājiem (piemēram, patērētājiem vai uzņēmumiem) un citiem mitināšanas pakalpojumiem, tostarp, ja pakalpojumu sniedz, izmantojot mākoņdatošanu. Informācijas sabiedrības pakalpojumi, attiecībā uz kuriem datu glabāšana nav lietotājam sniegtā pakalpojuma pamatelements un kuriem ir tikai palīgraksturs, piemēram, juridiskie, arhitektūras, inženiertehniskie un grāmatvedības pakalpojumi, kas tiek sniegti tiešsaistē no attāluma, būtu jāizslēdz no šīs regulas darbības jomas pat tad, ja tie varētu atbilst informācijas sabiedrības pakalpojumu definīcijai saskaņā ar Direktīvu (ES) 2015/1535.

- 17) Daudzos gadījumos dati lietotāja ierīcē vairs netiek glabāti vai apstrādāti, bet ir pieejami mākoņa infrastruktūrā piekļuvei no jebkuras vietas. Lai sniegtu minētos pakalpojumus, pakalpojumu sniedzējiem nav nepieciešams veikt uzņēmējdarbību vai izvietot serverus konkrētā jurisdikcijā. Tādējādi šīs regulas piemērošanai nevajadzētu būt atkarīgai no pakalpojumu sniedzēja uzņēmuma vai datu apstrādes vai glabāšanas ierīces faktiskās atrašanās vietas.
- 18) Īpaši svarīgi attiecībā personu, kuras atbildīgas par ļaunprātīgām vai apdraudētām tīmekļa vietnēm, identificēšanu ir tādu interneta infrastruktūras pakalpojumu sniedzēji, kas saistīti ar vārdu un numuru piešķiršanu, piemēram, domēnu vārdu reģistratori un reģistri, privātuma un starpniekservera pakalpojumu sniedzēji vai reģionālie interneta reģistri interneta protokola ("IP") adresēm. Viņu rīcībā ir dati, kas ir īpaši nozīmīgi kriminālprocesā, jo tie ļauj identificēt personu vai struktūru, kas atbildīgas par kriminālnoziedzīgumā izmantoto tīmekļa vietni, vai noziedzīgo darbību rezultāta cietušas personas, ja apdraudētu tīmekļa vietni ir uzlauzuši noziedznieki.
- 19) Šī regula regulē tikai uzglabāto datu vākšanu, proti, tie ir pakalpojumu sniedzēja rīcībā esošie dati brīdī, kad viņš saņem Eiropas e-pierādījumu sniegšanas vai saglabāšanas rīkojuma sertifikātu. Regulā nav noteikts vispārējs datu saglabāšanas pienākums, kā arī netiek atļauts pārtvert vai iegūt uzglabātos datus nākotnē pēc datu sniegšanas vai saglabāšanas rīkojuma sertifikāta saņemšanas. Dati būtu jāsniedz neatkarīgi no tā, vai tie ir šifrēti vai ne.
- 20) Datu kategorijas, uz kurām attiecas šī regula, ietver abonenta datus, piekļuves datus, darījumu datus (šīs trīs kategorijas dēvē par "datiem, kas nav saturs") un saturs 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.
- 21) Ir lietderīgi nošķirt piekļuves datus kā īpašu datu kategoriju, ko izmanto šajā regulā. Piekļuves dati tiek vākti ar tādu pašu mērķi kā abonenta dati, proti, lai identificētu ar tiem saistīto lietotāju, un pamattiesību aizskārums līmenis ir līdzīgs kā abonenta datu gadījumā. Piekļuves dati parasti tiek reģistrēti kā notikumu ieraksta daļa (citiem vārdiem sakot, servera žurnālā), lai norādītu lietotāja piekļuves pakalpojumam sesijas sākumu un beigas. Bieži vien tā ir atsevišķa IP adrese (statiska vai dinamiska) vai cits identifikators, kas nošķir piekļuves sesijas laikā izmantoto tīkla saskarni. Ja lietotājs

nav zināms, bieži vien vispirms ir identifikatora dati, un tikai pēc tam var pieprasīt, lai pakalpojumu sniedzējs iesniedz ar šo identifikatoru saistītos abonenta datus.

- 22) No otras puses, darījumu dati parasti tiek prasīti ar mērķi iegūt informāciju par lietotāja kontaktiem un atrašanās vietu, un tos var sniegt, lai izveidotu attiecīgās personas profilu. Tas nozīmē, ka piekļuves dati paši par sevi nevar kalpot līdzīgam mērķim, piemēram, tie neatklāj nekādu informāciju par sarunu partneriem, kas saistīti ar lietotāju. Tādējādi ar šo priekšlikumu tiek ieviesta jauna datu kategorija, kas ir uzskatāma par abonenta datiem, ja šo datu iegūšanas mērķis ir līdzīgs.
- 23) Visas datu kategorijas ietver personas datus, un tādējādi uz tiem attiecas aizsardzības pasākumi saskaņā ar Savienības datu aizsardzības *acquis*, taču atšķirīga ir ietekmes intensitāte uz pamattiesībām, jo īpaši tas attiecas uz abonenta datiem un piekļuves datiem, no vienas puses, un uz darījumu datiem un satura datiem no otras puses. Lai gan abonenta dati un piekļuves dati ir noderīgi, lai izmeklēšanā gūtu pirmās norādes par aizdomās turētās personas identitāti, darījumu un satura dati ir vissvarīgākie kā pierādījumu materiāls. Tādēļ ir būtiski, lai šis instruments aptvertu visas šīs datu kategorijas. Ņemot vērā atšķirīgo pamattiesību aizskāruma līmeni, tiek piemēroti dažādi nosacījumi abonentu un piekļuves datu iegūšanai, no vienas puses, un darījumu un satura datu iegūšanai, no otras puses.
- 24) Eiropas e-pierādījumu sniegšanas rīkojums un Eiropas e-pierādījumu saglabāšanas rīkojums ir izmeklēšanas pasākumi, kas būtu jāizdod tikai saistībā ar konkrētiem kriminālprocesiem pret konkrētiem zināmiem vai vēl nezināmiem konkrētiem, jau izdarīta noziedzīgā nodarījuma izpildītājiem, pirms tam katrā atsevišķā lietā izvērtējot proporcionalitāti un nepieciešamību.
- 25) Šī regula neskar iestāžu izmeklēšanas pilnvaras civillietās vai administratīvos procesos, tostarp gadījumos, kad to rezultātā var tikt piemērotas sankcijas.
- 26) Šī regula būtu jāpiemēro pakalpojumu sniedzējiem, kas piedāvā pakalpojumus Savienībā, un šajā regulā paredzētos rīkojumus var izdot tikai attiecībā uz datiem, kas attiecas uz Savienībā piedāvātiem pakalpojumiem. Pakalpojumi, kas tiek piedāvāti tikai ārpus Savienības, neietilpst šīs regulas darbības jomā, pat ja pakalpojumu sniedzējs veic uzņēmējdarbību Savienībā.
- 27) Lai noteiktu, vai pakalpojumu sniedzējs piedāvā pakalpojumus Savienībā, nepieciešams izvērtēt, vai pakalpojumu sniedzējs ļauj juridiskām vai fiziskām personām vienā vai vairākās dalībvalstīs izmantot savus pakalpojumus. Tomēr tiešsaistes saskarnes pieejamība vien, piemēram, pakalpojumu sniedzēja vai starpnieka tīmekļa vietnes vai e-pasta adreses un citas kontaktinformācijas pieejamība vienā vai vairākās dalībvalstīs, aplūkojot atsevišķi, nebūtu pietiekams nosacījums šīs regulas piemērošanai.
- 28) Nosakot šīs regulas piemērošanas jomu, par nozīmīgu faktoru būtu uzskatāma arī būtiska saistība ar Savienību. Būtu jāuzskata, ka šāda būtiska saistība ar Savienību pastāv, ja pakalpojumu sniedzējs veic uzņēmējdarbību Savienībā. Ja viņš neveic šādu uzņēmējdarbību, kritērijs par būtisku saistību būtu jāizvērtē, pamatojoties uz ievērojamu lietotāju skaitu vienā vai vairākās dalībvalstīs vai darbību vēršanu uz vienu vai vairākām dalībvalstīm. Darbību vēršanu uz vienu vai vairākām dalībvalstīm var noteikt, pamatojoties uz visiem būtiskajiem apstākļiem, tostarp tādiem faktoriem kā minētajā dalībvalstī parasti lietotā valoda vai valūta, vai iespēja pasūtīt preces vai pakalpojumus. Par darbību vēršanu uz kādu dalībvalsti norāda arī lietojumprogrammas ("lietotnes") pieejamība attiecīgās valsts lietotņu veikalā, vietējo reklāmas

pakalpojumu sniegšana vai reklāmas sniegšana attiecīgajā dalībvalstī izmantotajā valodā, vai attiecības ar klientiem, piemēram, nodrošinot klientu apkalpošanas dienestu valodā, ko parasti izmanto attiecīgajā dalībvalstī. Tāpat tiek pieņemts, ka pastāv būtiska saistība, ja pakalpojumu sniedzējs vērš savu darbību uz vienu vai vairākām dalībvalstīm, kā noteikts 17. panta 1. punkta c) apakšpunktā Regulā 1215/2012 par jurisdikciju un spriedumu atzīšanu un izpildi civillietās un komerclietās³⁶. No otras puses, pakalpojuma sniegšanu tikai nolūkā nodrošināt atbilstību Regulā (ES) 2018/302³⁷ noteiktajam diskriminācijas aizliegumam tikai šā viena iemesla dēļ nevar uzskatīt par darbību virzīšanu vai vēršanu uz konkrētu teritoriju Savienībā.

- 29) Eiropas e-pierādījumu sniegšanas rīkojums būtu jāizdod tikai tad, ja tas ir nepieciešams un proporcionāls. Novērtējumā būtu jāņem vērā, vai rīkojums nepārsniedz leģitīmā mērķa sasniegšanai nepieciešamo, proti, iegūt attiecīgos un nepieciešamos datus, kas kalpotu kā pierādījums tikai konkrētajā lietā.
- 30) Ja tiek izdots Eiropas e-pierādījumu sniegšanas vai saglabāšanas rīkojums, tā izdošanas vai apstiprināšanas procesā vienmēr būtu jāiesaista tiesu iestāde. Ņemot vērā darījumu un satura datu sensitīvo būtību, Eiropas e-pierādījumu sniegšanas rīkojuma izdošana vai apstiprināšana šo kategoriju datu sniegšanas vajadzībām ir jāpārskata tiesnesim. Tā kā abonentu un piekļuves dati ir mazāk sensitīvi, Eiropas e-pierādījumu sniegšanas rīkojumus to izpaušanai var izdot vai apstiprināt arī kompetentie prokurori.
- 31) Tā paša iemesla dēļ ir jānošķir šīs regulas materiālā piemērošanas joma: rīkojumus par abonentu un piekļuves datu sniegšanu var izdot par jebkuru noziedzīgu nodarījumu, savukārt attiecībā uz piekļuvi darījumu un satura datiem vajadzētu piemērot stingrākas prasības, lai atspoguļotu šādu datu sensitīvo būtību. Lai nodrošinātu proporcionalitātes principa un iesaistīto personu tiesību ievērošanu, proporcionālāku pieeju ļauj nodrošināt priekšlikumā noteiktais sliekšnis kopā ar vairākiem citiem *ex ante* un *ex post* nosacījumiem un aizsardzības pasākumiem. Tajā pašā laikā sliekšnim nevajadzētu ierobežot instrumenta efektivitāti un tā praktisku izmantošanu. Atļaujot izdot rīkojumus tādu nodarījumu izmeklēšanā, par kuriem paredzēts maksimālais brīvības atņemšanas sods uz vismaz trīs gadiem, instrumenta darbības joma tiek ierobežota attiecībā uz smagākiem noziegumiem, pārmērīgi neierobežojot tā praktisku izmantošanu. Tas izslēdz no darbības jomas ievērojamu skaitu noziegumu, kas dalībvalstīs tiek uzskatīti par mazāk smagiem, par ko liecina mazāks piemērojamais maksimālais sods. Turklāt tā priekšrocība ir vienkāršā praktiskā izmantošana.
- 32) Noteiktu nodarījumu gadījumā pierādījumi parasti būs pieejami tikai elektroniskā formā, kam ir raksturīgs īslaicīgums. Tas attiecas uz kibernetiskiem noziegumiem, pat tādiem, kuri būtībā un paši par sevi nav uzskatāmi par smagiem noziegumiem, taču var radīt ievērojamu vai būtisku kaitējumu, jo īpaši gadījumos, kad to ietekme uz atsevišķiem indivīdiem ir neliela, taču nodarītā kaitējuma apjoms ir liels un vispārējs. Vairākumā gadījumu, kad nodarījums tiek izdarīts, izmantojot informācijas sistēmu, tāda paša sliekšņa piemērošana kā citiem nodarījumu veidiem var novest pie nesodāmības. Tas pamato regulas piemērošanu arī tiem nodarījumiem, par kuriem piemēro sodu ar

³⁶ Eiropas Parlamenta un Padomes [Regula \(ES\) 1215/2012](#) (2012. gada 12. decembris) par jurisdikciju un spriedumu atzīšanu un izpildi civillietās un komerclietās (OV L 351, 20.12.2012., 1. lpp.).

³⁷ Eiropas Parlamenta un Padomes [Regula \(ES\) 2018/302](#) (2018. gada 28. februāris), ar ko novērš nepamatotu ģeogrāfisko bloķēšanu un citus diskriminācijas veidus iekšējā tirgū klientu valstspiederības, dzīvesvietas vai uzņēmējdarbības veikšanas vietas dēļ un groza Regulas (EK) Nr. 2006/2004 un (ES) 2017/2394 un Direktīvu 2009/22/EK (OV L 601, 2.3.2018., 1. lpp.).

brīvības atņemšanu līdz trīs gadiem. Par teroristu nodarījumiem, kā noteikts Direktīvā 2017/541/ES, nav jāpiemēro minimālais maksimālais trīs gadu sliekšnis.

- 33) Turklāt nepieciešams noteikt, ka Eiropas e-pierādījumu sniegšanas rīkojumu drīkst izdot tikai tad, ja līdzīgs rīkojums būtu pieejams tāda paša noziedzīga nodarījuma gadījumā salīdzināmā iekšzemes situācijā izdevējvalstī.
- 34) Gadījumos, kad pieprasītie dati tiek glabāti vai apstrādāti kā daļa no infrastruktūras, ko pakalpojumu sniedzējs nodrošina uzņēmumam vai citai struktūrai, kura nav fiziskas personas — parasti mitināšanas pakalpojumu gadījumā —, Eiropas e-pierādījumu sniegšanas rīkojums būtu jāizmanto tikai tad, ja citi izmeklēšanas pasākumi, kas ir vērsti uz uzņēmumu vai struktūru, nav piemēroti, jo īpaši, ja tas apdraudētu izmeklēšanu. Tas ir jo īpaši būtiski, ja runa ir par lielākām struktūrām, piemēram, korporācijām vai valdības struktūrām, kuras izmanto pakalpojumu sniedzēju pakalpojumus, lai nodrošinātu savu korporatīvo IT infrastruktūru vai pakalpojumus, vai abus. Pirmajam Eiropas e-pierādījumu sniegšanas rīkojuma adresātam šādās situācijās vajadzētu būt uzņēmumam vai citai struktūrai. Šis uzņēmums vai cita struktūra var nebūt pakalpojumu sniedzējs, uz kuru attiecas šīs regulas darbības joma. Tomēr gadījumos, kad nav piemēroti vērsties pie šīs struktūras, jo tā, piemēram, tiek turēta aizdomās par iesaistīšanos attiecīgajā lietā, vai arī ir norādes par slepenu vienošanos ar izmeklēšanas objektu, kompetentajām iestādēm vajadzētu būt iespējai ar lūgumu iesniegt prasītos datus vērsties pie pakalpojumu sniedzēja, kurš nodrošina attiecīgo infrastruktūru. Šis noteikums neskar tiesības pieprasīt pakalpojumu sniedzējam saglabāt datus.
- 35) Imunitāte un privilēģijas, kas var attiekties uz personu kategorijām (piemēram, diplomātiem) vai īpaši aizsargātām attiecībām (piemēram, advokāta un klienta saziņas konfidencialitāte), ir minētas citos savstarpējās atzīšanas instrumentos, piemēram, Eiropas izmeklēšanas rīkojumā. To tvērums un ietekme atšķiras atkarībā no piemērojamiem valsts tiesību aktiem, kas būtu jāņem vērā rīkojuma izdošanas laikā, jo izdevējiestāde var izdot rīkojumu tikai tad, ja līdzīgs rīkojums būtu pieejams salīdzināmā iekšzemes situācijā. Papildus šim pamatprincipam imunitāte un privilēģijas, kas aizsargā piekļuvi, darījumu vai satura datus pakalpojumu sniedzēja dalībvalstī, cik vien iespējams jāņem vērā izdevējvalstī tādā pašā veidā kā tad, ja tos paredzētu izdevējvalsts tiesību akti. Tas jo īpaši attiecas uz gadījumiem, kad dalībvalsts, kurā vēršas pie pakalpojumu sniedzēja vai tā juridiskā pārstāvja, tiesību akti nodrošinātu lielāku aizsardzību, nekā to nodrošina izdevējvalsts tiesību akti. Tāpat šis noteikums nodrošina to, ka tiek ņemti vērā gadījumi, kad datu izpaušana var ietekmēt minētās dalībvalsts pamatintereses, piemēram, valsts drošību un aizsardzību. Kā papildu drošības līdzeklis šie aspekti būtu jāņem vērā ne tikai tad, kad tiek izdots rīkojums, bet arī vēlāk, izvērtējot attiecīgo datu atbilstību un pieņemamību attiecīgajā kriminālprocesa posmā, un izpildes procedūras gadījumā šie aspekti būtu jāņem vērā izpildes iestādei.
- 36) Eiropas e-pierādījumu saglabāšanas rīkojumu var izdot par jebkuru nodarījumu. Tā mērķis ir novērst attiecīgo datu izņemšanu, dzēšanu vai grozīšanu situācijās, kad šo datu sniegšanai var būt nepieciešams ilgāks laiks, piemēram, tāpēc, ka tiks izmantoti tiesiskās sadarbības kanāli.
- 37) Eiropas e-pierādījumu sniegšanas un saglabāšanas rīkojumi būtu jāadresē pakalpojumu sniedzēja izraudzītajam juridiskajam pārstāvim. Ja juridiskais pārstāvis nav izraudzīts, rīkojumus var adresēt pakalpojumu sniedzēja uzņēmumam Savienībā. Tas var attiekties uz gadījumiem, kad pakalpojumu sniedzējam nav juridiska pienākuma iecelt

juridisko pārstāvi. Ja juridiskais pārstāvis nepilda prasības ārkārtas situācijās, Eiropas e-pierādījumu sniegšanas vai saglabāšanas rīkojumu var adresēt arī pakalpojumu sniedzējam papildus oriģinālā rīkojuma izpildei vai tās vietā saskaņā ar 14. panta noteikumiem. Ja juridiskais pārstāvis nepilda prasības situācijās, kas nav ārkārtas, taču nepārprotami pastāv datu zuduma risks, Eiropas e-pierādījumu sniegšanas vai saglabāšanas rīkojumu var adresēt arī jebkuram pakalpojumu sniedzēja uzņēmumam Savienībā. Šo dažādo iespējamo scenāriju dēļ noteikumos tiek izmantots vispārējais jēdziens “adresāts”. Ja pienākums, piemēram, konfidencialitātes ievērošana, attiecas ne tikai uz adresātu, bet arī uz pakalpojumu sniedzēju, kas nav adresāts, tas ir norādīts attiecīgajā noteikumā.

- 38) Eiropas e-pierādījumu sniegšanas un Eiropas e-pierādījumu saglabāšanas rīkojumi būtu jānosūta pakalpojumu sniedzējam, izmantojot Eiropas e-pierādījumu sniegšanas rīkojuma sertifikātu (*EPOC*) vai Eiropas e-pierādījumu saglabāšanas rīkojuma sertifikātu (*EPOC-PR*), kas būtu jāpārtulko. Lai novērstu izmeklēšanas apdraudējumu, sertifikātos vajadzētu būt norādītai tāai pašai obligātai informācijai kā rīkojumos, izņemot pasākuma nepieciešamības un proporcionālītātes pamatojumus vai sīkāku informāciju par lietu. Bet, tā kā sertifikāti ir daļa no paša rīkojuma, aizdomās turētajai personai ir iespēja apstrīdēt sertifikātus vēlāk kriminālprocesa laikā. Vajadzības gadījumā sertifikātu nepieciešams pārtulkot (vienā no) adresāta dalībvalsts oficiālajā(m) valodā(m) vai citā oficiālajā valodā, ko pakalpojumu sniedzējs ir paziņojis par pieņemamu.
- 39) Kompetentajai izdevējiestādei *EPOC* vai *EPOC-PR* būtu jānosūta tieši adresātam, izmantojot jebkādu līdzekļu, ar kuriem var iegūt rakstisku dokumentu ar nosacījumu, ka pakalpojumu sniedzējs var noteikt tā autentiskumu, piemēram, ierakstītā vēstulē, izmantojot drošu e-pasta sistēmu vai platformas vai citus drošus kanālus, tai skaitā pakalpojumu sniedzēja piedāvātos, vienlaikus ievērojot personas datu aizsardzības noteikumus.
- 40) Pieprasītie dati būtu jānosūta iestādēm ne vēlāk kā desmit dienu laikā pēc *EPOC* saņemšanas. Ārkārtas situācijās un gadījumos, kad izdevējiestāde norāda citus iemeslus atkāpei no desmit dienu termiņa, datu iesniedzējam būtu jāievēro īsāki termiņi. Tie varētu būt gadījumi, kad pastāv nenovēršami draudi, ka prasītie dati varētu tikt izdzēsti, kā arī apstākļi, kas saistīti ar notiekošu izmeklēšanu, piemēram, ja pieprasītie dati ir saistīti ar citiem steidzamiem izmeklēšanas pasākumiem, kurus nevar īstenot bez trūkstošiem datiem vai kuri ir citādi atkarīgi no šiem datiem.
- 41) Lai pakalpojumu sniedzējiem ļautu risināt formālas problēmas, nepieciešams noteikt procedūru saziņai starp pakalpojumu sniedzēju un izdevēju tiesu iestādi gadījumos, kad *EPOC* varētu būt nepilnīgs vai tajā ir acīmredzamas kļūdas vai trūkst informācijas rīkojuma izpildei. Turklāt, ja pakalpojumu sniedzējs nesniegtu pilnīgu vai savlaicīgu informāciju citu iemeslu dēļ, piemēram, ja viņš uzskata, ka tas ir pretrunā ar pienākumu, ko paredz trešās valsts tiesību akti, vai ka Eiropas e-pierādījumu sniegšanas rīkojums nav izdots saskaņā ar šajā regulā izklāstītajiem nosacījumiem, viņam vajadzētu sazināties ar izdevējiestādēm un sniegt atbilstīgus pamatojumus. Tādēļ saziņas procedūrai kopumā būtu jānodrošina iespēja izdevējiestādei agrīnā posmā labot vai pārskatīt *EPOC*. Lai garantētu datu pieejamību, pakalpojumu sniedzējam būtu jā saglabā dati, ja no tiem var identificēt pieprasītos datus.
- 42) Saņemot Eiropas e-pierādījumu saglabāšanas rīkojuma sertifikātu (*EPOC-PR*), pakalpojumu sniedzējam vajadzētu saglabāt pieprasītos datus ne ilgāk kā 60 dienas, ja vien izdevējiestāde neinformē pakalpojumu sniedzēju, ka tā ir sākusi procedūru

nākamajam pieprasījumam sniegt datus, tādā gadījumā dati jā saglabā ilgāku laiku. 60 dienu periods ir aprēķināts, lai varētu iesniegt oficiālu pieprasījumu. Šim nolūkam ir jāveic vismaz daži formāli pasākumi, piemēram, jānosūta tulkošanai savstarpējas tiesiskās palīdzības pieprasījums. Pēc minētās informācijas saņemšanas dati būtu jā saglabā tik ilgi, cik tas nepieciešams, līdz tos sniedz saskaņā ar turpmāku pieprasījumu sniegt datus.

- 43) Pakalpojumu sniedzējiem un to juridiskajiem pārstāvjiem būtu jānodrošina konfidencialitāte un, ja izdevējiestāde to pieprasa, lai garantētu noziedzīgu nodarījumu izmeklēšanu saskaņā ar Regulas (ES) 2016/679 23. pantu,³⁸ jāatturas informēt personu, kuras dati tiek pieprasīti. Tomēr lietotāja informācija ir būtisks elements, lai nodrošinātu pārskatīšanu un tiesisko aizsardzību, un, ja pakalpojumu sniedzējs tika lūgts neinformēt lietotāju, gadījumos, kad netiek apdraudēta notiekošā izmeklēšana, iestādei šī informācija būtu jāsniedz saskaņā ar valsts pasākumu, ar ko īsteno Direktīvas (ES) 2016/680 13. pantu³⁹.
- 44) Ja adresāts nepilda prasības, izdevējiestāde var nosūtīt visu rīkojumu, tostarp nepieciešamības un proporcionālītātes pamatojumu, kam pievienots sertifikāts, tās dalībvalsts kompetentajai iestādei, kurā sertifikāta adresāts dzīvo vai veic uzņēmējdarbību. Šai dalībvalstij būtu jāizpilda rīkojums saskaņā ar tās tiesību aktiem. Ja tiek pārkāpti šajā regulā noteiktie pienākumi, dalībvalstīm būtu jānodrošina iedarbīgu, samērīgu un atturošu finansiālo sankciju piemērošana.
- 45) Izpildes procedūra ir procedūra, kurā adresāts var iebilst pret izpildi konkrētu ierobežotu iemeslu dēļ. Izpildes iestāde var atteikties atzīt un izpildīt rīkojumu, pamatojoties uz tiem pašiem iemesliem, vai ja saskaņā ar tās valsts tiesību aktiem ir spēkā imunitāte un privilēģijas vai arī informācijas izpaušana var ietekmēt valsts pamatintereses, piemēram, valsts drošību un aizsardzību. Izpildes iestādei jāapspriežas ar izdevējiestādi pirms atteikuma atzīt vai izpildīt rīkojumu, pamatojoties uz minētajiem iemesliem. Prasību neizpildes gadījumā iestādes var piemērot sankcijas. Šīm sankcijām jābūt samērīgām, turklāt jāņem vērā konkrētie apstākļi, piemēram, atkārtota vai sistemātiska prasību neizpilde.
- 46) Neatkarīgi no to datu aizsardzības pienākumiem pakalpojumu sniedzējiem nebūtu jāuzņemas atbildība par kaitējumu, kas nodarīts viņu lietotājiem vai trešajām personām tikai tādēļ, ka pakalpojumu sniedzēji ir labticīgi ievērojuši *EPOC* vai *EPOC-PR* prasības.
- 47) Papildus personām, kuru dati tiek pieprasīti, izmeklēšanas pasākums var ietekmēt pakalpojumu sniedzējus un trešās valstis. Lai nodrošinātu trešo valstu suverēno interešu atzīšanu, aizsargātu attiecīgo personu un novērstu pretrunīgus pienākumus pakalpojumu sniedzējiem, šis instruments nodrošina īpašu mehānismu pārskatīšanai tiesā, ja Eiropas e-pierādījumu sniegšanas rīkojuma prasību ievērošana neļautu pakalpojumu sniedzējiem ievērot juridiskos pienākumus, kas izriet no trešās valsts tiesību aktiem.

³⁸ Eiropas Parlamenta un Padomes [Regula \(ES\) 2016/679](#) (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

³⁹ Eiropas Parlamenta un Padomes [Direktīva \(ES\) 2016/680](#) (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu kriminālsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI (OV L 119, 4.5.2016., 89. lpp.).

- 48) Šajā nolūkā, ja adresāts uzskata, ka ar Eiropas e-pierādījumu sniegšanas rīkojumu konkrētajā gadījumā tiks pārkāpts juridiskais pienākums, kas izriet no trešās valsts tiesību aktiem, viņam par to būtu jāinformē izdevējiestāde, iesniedzot pamatotu iebildumu un izmantojot pielikumā pievienotās veidlapas. Izdevējiestādei tad būtu jāpārskata Eiropas e-pierādījumu sniegšanas rīkojums atbilstoši pamatotajam iebildumam, ņemot vērā tos pašus kritērijus, kas būtu jāievēro kompetentai tiesai. Ja iestāde nolemj apstiprināt rīkojumu, procedūra būtu jānodod attiecīgās dalībvalsts paziņotajai kompetentajai tiesai, kura pēc tam pārskata rīkojumu.
- 49) Lai noteiktu pretrunīga pienākuma esību izskatāmās lietas konkrētajos apstākļos, kompetentā tiesa vajadzības gadījumā var paļauties uz attiecīgu ārējo ekspertu atzinumu, piemēram, ja pārskatīšanas laikā rodas jautājumi par attiecīgās trešās valsts tiesību aktu interpretāciju. Piemēram, tās varētu būt apspriedes ar šīs valsts centrālajām iestādēm.
- 50) Zināšanas par tiesību aktu interpretāciju var nodrošināt arī ekspertu atzinumi, ja tādi ir pieejami. Informācijai un tiesu praksei par trešo valstu tiesību aktu interpretāciju un dalībvalstu kolīziju procedūrām vajadzētu būt pieejamai centrālajā platformā, piemēram, *SIRIUS* projektā un/vai Eiropas Tiesiskās sadarbības tīklā. Tam būtu jānodrošina iespēja tiesām izmantot citu valstu tiesu uzkrāto pieredzi un zināšanas par tiem pašiem vai līdzīgiem jautājumiem. Tam nevajadzētu kavēt jaunu apspriešanos ar trešo valsti, ja tāda ir nepieciešama.
- 51) Ja pastāv pretrunīgi pienākumi, tiesai būtu jānosaka, vai trešās valsts pretrunīgie noteikumi aizliedz attiecīgo datu izpaušanu, pamatojoties uz to, ka tas ir nepieciešams attiecīgo personu pamattiesību aizsardzību vai trešās valsts pamatinteresu saistībā ar valsts drošību vai aizsardzību nodrošināšanu. Veicot šo novērtējumu, tiesai būtu jāņem vērā, vai trešās valsts tiesību akti tā vietā, lai aizsargātu pamattiesības vai trešās valsts pamatintereses, kas saistītas ar valsts drošību vai aizsardzību, acīmredzami cenšas aizsargāt citas intereses vai arī ir vērsti uz to, lai kriminālizmeklēšanas ietvaros aizsargātu nelikumīgas darbības no tiesībaizsardzības iestāžu pieprasījumiem. Ja tiesa secina, ka trešās valsts pretrunīgie noteikumi aizliedz attiecīgo datu izpaušanu, pamatojoties uz apsvērumiem, ka tas ir nepieciešams, lai aizsargātu attiecīgo personu pamattiesības vai trešās valsts pamatintereses saistībā ar valsts drošību vai aizsardzību, tai būtu jāapspriežas ar trešo valsti ar tās centrālo iestāžu starpniecību, kuras savstarpējas tiesiskās palīdzības nolūkos jau ir izveidotas lielākajā daļā pasaules reģionu. Tiesai būtu jānosaka termiņš, līdz kuram trešā valsts var iesniegt iebildumus pret Eiropas e-pierādījumu sniegšanas rīkojuma izpildi; ja trešās valsts iestādes nereaģē noteiktajā (pagarinātajā) termiņā, neraugoties uz atgādinājumu, kurā tās ir informētas par atbildes nesniegšanas sekām, tiesa apstiprina rīkojumu. Ja trešās valsts iestādes iebilst pret informācijas izpaušanu, tiesai ir jāatceļ rīkojums.
- 52) Visos pārējos pretrunīgo pienākumu gadījumos, kas neattiecas uz personas pamattiesībām vai trešās valsts pamatinteresēm saistībā ar valsts drošību vai aizsardzību, tiesai būtu jāpieņem lēmums par to, vai apstiprināt Eiropas e-pierādījumu sniegšanas rīkojumu, apsverot vairākus elementus, kas ir izstrādāti, lai pārliecinātos, cik stipra ir saikne ar kādu no abām iesaistītajām jurisdikcijām, kādas ir attiecīgās intereses iegūt datus vai nepieļaut to izpaušanu, kā arī kādas ir iespējamās sekas pakalpojumu sniedzējam, ja tas pildīs rīkojuma prasības. Attiecībā uz kibernetizāciju ir svarīgi, ka nozieguma izdarīšanas vieta attiecas gan uz vietu(-ām), kurā(-ās) tika veikta darbība, gan uz vietu(-ām), kur ir īstenojušās nodarījuma sekas.

- 53) Regulas 9. pantā izklāstītie nosacījumi ir piemērojami arī gadījumos, kad rodas pretrunīgi pienākumi, kas izriet no trešās valsts tiesību aktiem. Šīs procedūras laikā dati būtu jāsaglabā. Ja rīkojums tiek atcelts, var izdot jaunu datu saglabāšanas rīkojumu, lai ļautu izdevējiestādei prasīt sniegt datus, izmantojot citus kanālus, piemēram, savstarpēju tiesisko palīdzību.
- 54) Ir būtiski, lai visām personām, kuru dati tiek pieprasīti kriminālizmeklēšanā vai tiesvedībā, būtu pieejami efektīvi tiesiskās aizsardzības līdzekļi saskaņā ar Eiropas Savienības Pamattiesību hartas 47. pantu. Aizdomās turētajām un apsūdzētajām personām vajadzētu būt tiesībām uz efektīvu tiesisko aizsardzību kriminālprocesā. Tas var ietekmēt ar šādiem līdzekļiem iegūto pierādījumu pieņemamību vai attiecīgā gadījumā to nozīmīgumu tiesvedībā. Turklāt minētajām personām tiek piešķirtas visas piemērojamās procesuālās garantijas, piemēram, tiesības uz informāciju. Tiesības uz efektīvu tiesisko aizsardzību būtu jānodrošina arī citām personām, kuras nav aizdomās turētās vai apsūdzētās personas. Tādēļ būtu jānodrošina vismaz iespēja apstrīdēt Eiropas e-pierādījumu sniegšanas rīkojuma likumību, tostarp rīkojuma nepieciešamību un proporcionālītāti. Šai regulai nebūtu jāierobežo iespējamie pamatojumi rīkojuma likumības apstrīdēšanai. Šie tiesiskās aizsardzības līdzekļi būtu jāizmanto izdevējvalstī saskaņā ar valsts tiesību aktiem. Noteikumi par pagaidu noregulējumu būtu jāreglamentē valsts tiesību aktiem.
- 55) Turklāt izpildes procedūras laikā un izmantojot turpmākos tiesiskās aizsardzības līdzekļus, adresāts var iebilst pret Eiropas e-pierādījumu sniegšanas vai saglabāšanas rīkojuma izpildi vairāku ierobežotu iemeslu dēļ, tostarp tādēļ, ka rīkojumu nav izdevusi vai apstiprinājusi kompetenta iestāde vai ka rīkojums acīmredzami pārkāpj Eiropas Savienības Pamattiesību hartu vai ir acīmredzami ļaunprātīgs. Piemēram, rīkojums sniegt satura datus, kuri attiecas uz nenoteiktu cilvēku grupu kādā ģeogrāfiskajā apgabalā vai kuriem nav saiknes ar konkrētu kriminālprocesu, acīmredzami ignorētu šajā regulā noteiktos Eiropas e-pierādījumu sniegšanas rīkojuma izdošanas nosacījumus.
- 56) Fizisko personu aizsardzība attiecībā uz personas datu apstrādi ir viena no pamattiesībām. Saskaņā ar Eiropas Savienības Pamattiesību hartas 8. panta 1. punktu un LESD 16. panta 1. punktu ikvienai personai ir tiesības uz savu personas datu aizsardzību. Īstenojot šo regulu, dalībvalstīm būtu jānodrošina, ka personas dati tiek aizsargāti un ka tos var apstrādāt tikai saskaņā ar Regulu (ES) 2016/679 un Direktīvu (ES) 2016/680.
- 57) Personas dati, kas iegūti saskaņā ar šo regulu, būtu jāapstrādā tikai tad, ja tas ir nepieciešami un proporcionāli noziedzīgu nodarījumu novēršanai, izmeklēšanai, atklāšanai un kriminālvajāšanai par tiem vai kriminālsodu izpildei un lai īstenotu tiesības uz aizstāvību. Jo īpaši dalībvalstīm jānodrošina attiecīgas datu aizsardzības politikas un pasākumu piemērošana gadījumos, kad attiecīgās iestādes pārsūta pakalpojumu sniedzējiem personas datus šīs regulas vajadzībām, kā arī pasākumi datu drošībai. Pakalpojumu sniedzējiem tas pats jānodrošina, nosūtot personas datus attiecīgajām iestādēm. Tikai pilnvarotas personas var saņemt piekļuvi informācijai, kas satur personas datus, kurus var iegūt, izmantojot autentifikācijas procesus. Nepieciešams apsvērt autentiskuma nodrošināšanas mehānismu izmantošanu, piemēram, paziņotās valsts elektroniskās identifikācijas sistēmas vai uzticamības pakalpojumus, kā paredzēts Eiropas Parlamenta un Padomes Regulā (ES) Nr. 910/2014 (2014. gada 23. jūlijs) par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK.

- 58) Komisijai būtu jāveic šīs regulas izvērtējums, pamatojoties uz pieciem kritērijiem: efektivitāte, lietderība, atbilstība, saskaņotība un ES pievienotā vērtība, un šis izvērtējums kalpotu par pamatu iespējamo turpmāko pasākumu ietekmes novērtējumam. Regulāri būtu jāvāc informācija šīs regulas izvērtēšanas vajadzībām.
- 59) Iepriekš iztulkotu un standartizētu veidlapu izmantošana sekmē sadarbību un informācijas apmaiņu starp tiesu iestādēm un pakalpojumu sniedzējiem, ļaujot tiem ātrāk un efektīvāk nodrošināt un pārsūtīt elektroniskus pierādījumus, vienlaikus izpildot nepieciešamās drošības prasības lietotājam draudzīgā veidā. Veidlapas samazina tulkošanas izmaksas un veicina augstus kvalitātes standartus. Tāpat atbildes veidlapas nodrošina standartizētu informācijas apmaiņu, jo īpaši gadījumos, kad pakalpojumu sniedzēji nespēj izpildīt prasības tāpēc, ka konts nepastāv vai nav pieejami dati. Turklāt šīs veidlapas atvieglo statistikas vākšanu.
- 60) Lai efektīvi risinātu iespējamo nepieciešamību uzlabot *EPOC* un *EPOC-PR* un to veidlapu saturu, kas jāizmanto, lai sniegtu informāciju par nespēju izpildīt *EPOC* vai *EPOC-PR*, Komisijai būtu jādeleģē pilnvaras pieņemt aktus saskaņā ar Līguma par Eiropas Savienības darbību 290. pantu attiecībā uz šīs regulas I, II un III pielikuma grozīšanu. Ir īpaši būtiski, lai Komisija, veicot sagatavošanas darbus, rīkotu atbilstīgas apspriešanās, tostarp ekspertu līmenī, un lai minētās apspriešanās tiktu rīkotas saskaņā ar principiem, kas noteikti 2016. gada 13. aprīļa Iestāžu nolīgumā par labāku likumdošanas procesu⁴⁰. Jo īpaši, lai deleģēto aktu sagatavošanā nodrošinātu vienādu dalību, Eiropas Parlaments un Padome visus dokumentus saņem vienlaikus ar dalībvalstu ekspertiem, un minēto iestāžu ekspertiem ir sistemātiska piekļuve Komisijas ekspertu grupu sanāksmēm, kurās notiek deleģēto aktu sagatavošana.
- 61) Lai iegūtu elektroniskos pierādījumus, pasākumiem, kas pamatojas uz šo regulu, nevajadzētu aizstāt Eiropas izmeklēšanas rīkojumus atbilstoši Eiropas Parlamenta un Padomes Direktīvai 2014/41/ES⁴¹. Dalībvalstu iestādēm būtu jāizvēlas to situācijai vispiemērotākais instruments, tās var izvēlēties izmantot Eiropas izmeklēšanas rīkojumu, pieprasot dažādu veidu izmeklēšanas pasākumus, tostarp, bet ne tikai, citas dalībvalsts elektronisko pierādījumu sniegšanu.
- 62) Turpinoties tehnoloģiju attīstībai, dažu gadu laikā var sākt dominēt jauni saziņas līdzekļu veidi, vai šīs regulas piemērošanā var rasties nepilnības. Tādēļ ir svarīgi paredzēt pārskatīt regulas piemērošanu.
- 63) Tā kā šīs regulas mērķi, proti, uzlabot pārrobežu elektronisko pierādījumu nodrošināšanu un iegūšanu, nevar pietiekami labi sasniegt atsevišķās dalībvalstīs mērķa pārrobežu rakstura dēļ, bet var labāk sasniegt Savienības līmenī, Savienība var pieņemt pasākumus saskaņā ar Līguma par Eiropas Savienību 5. pantā noteikto subsidiaritātes principu. Saskaņā ar minētajā pantā noteikto proporcionalitātes principu šajā regulā paredz vienīgi tos pasākumus, kas ir vajadzīgi minēto mērķu sasniegšanai.
- 64) Saskaņā ar 3. pantu Protokolā par Apvienotās Karalistes un Īrijas nostāju saistībā ar brīvības, drošības un tiesiskuma telpu, kas pievienots Līgumam par Eiropas Savienību un Līgumam par Eiropas Savienības darbību, *[Apvienotā Karaliste / Īrija ir paziņojušas, ka tās vēlas piedalīties šīs regulas pieņemšanā un piemērošanā]* vai *[un,*

⁴⁰ OV L 123, 12.5.2016., 1. lpp.

⁴¹ [Direktīva 2014/41/ES](#) (2014. gada 3. aprīlis) par Eiropas izmeklēšanas rīkojumu krimināllietās (OV L 130, 1.5.2014., 1. lpp.).

neskarot minētā protokola 4. pantu, Apvienotā Karaliste / Īrija nepiedalās šīs regulas pieņemšanā, un regula tām nav saistoša un nav jāpiemēro].

- 65) Saskaņā ar 1. un 2. pantu Protokolā Nr. 22 par Dānijas nostāju, kas pievienots Līgumam par Eiropas Savienību un Līgumam par Eiropas Savienības darbību, Dānija nepiedalās šīs regulas pieņemšanā, un Dānijai šī regula nav saistoša un nav jāpiemēro.
- 66) Ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju saskaņā ar Eiropas Parlamenta un Padomes Regulas (EK) Nr. 45/2001 28. panta 2. punktu⁴², un tas sniedza atzinumu (...) ⁴³,

IR PIENĒMUŠI ŠO REGULU.

1. nodaļa. Priekšmets, definīcijas un darbības joma

1. pants

Priekšmets

- 1. Ar šo regulu paredz noteikumus, saskaņā ar kuriem dalībvalsts iestāde var pieprasīt pakalpojumu sniedzējam, kas Savienībā piedāvā pakalpojumus, sniegt vai saglabāt elektroniskos pierādījumus neatkarīgi no datu atrašanās vietas. Šī regula neskar valstu iestāžu pilnvaras likt pakalpojumu sniedzējiem, kas veic uzņēmējdarbību vai ir pārstāvēti to teritorijā, ievērot līdzīgus valsts pasākumus.
- 2. Ar šo regulu negroza pienākumu ievērot pamattiesības un tiesību pamatprincipus, kas noteikti LES 6. pantā, tostarp personu, pret kurām notiek kriminālprocess, tiesības uz aizstāvību, un tā neskar tiesībaizsardzības un tiesu iestāžu jebkādos pienākumus šajā sakarā.

2. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

- (1) “Eiropas e-pierādījumu sniegšanas rīkojums” ir dalībvalsts izdevējiestādes saistošs lēmums, ar ko pakalpojumu sniedzējam, kurš piedāvā pakalpojumus Savienībā un veic uzņēmējdarbību vai ir pārstāvēts citā dalībvalstī, liek sniegt elektroniskos pierādījumus;
- (2) “Eiropas e-pierādījumu saglabāšanas rīkojums” ir dalībvalsts izdevējiestādes saistošs lēmums, ar ko pakalpojumu sniedzējam, kurš piedāvā pakalpojumus Savienībā un veic uzņēmējdarbību vai ir pārstāvēts citā dalībvalstī, liek saglabāt elektroniskos pierādījumus, ņemot vērā turpmāku pieprasījumu sniegt datus;
- (3) “pakalpojumu sniedzējs” ir jebkura fiziska vai juridiska persona, kas sniedz vienu vai vairākus šādu kategoriju pakalpojumus:

⁴² Eiropas Parlamenta un Padomes Regula (EK) Nr. 45/2001 (2000. gada 18. decembris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti (OV L 8, 12.1.2001., 1. lpp.).

⁴³ OV C , lpp.

- (a) elektronisko sakaru pakalpojums, kā noteikts [Direktīvas, ar ko izveido Eiropas Elektronisko sakaru kodeksu] 2. panta 4. punktā;
 - (b) informācijas sabiedrības pakalpojumi, kā noteikts Eiropas Parlamenta un Padomes Direktīvas (ES) 2015/1535 1. panta 1. punkta b) apakšpunktā⁴⁴, attiecībā uz kuriem datu glabāšana ir lietotājam sniegtā pakalpojuma pamatelements; tie ietver sociālos tīklus, tiešsaistes tirgus, kas sekmē darījumus starp to lietotājiem, un citus mitināšanas pakalpojumu sniedzējus;
 - (c) interneta domēna nosaukumu un IP numerācijas pakalpojumi, piemēram, IP adreses sniedzēji, domēna nosaukumu reģistri, domēna nosaukumu reģistratori un saistītie privātuma un starpnieku pakalpojumi;
- (4) “pakalpojumu piedāvāšana Savienībā” nozīmē:
- (a) iespēja juridiskām vai fiziskām personām vienā vai vairākās dalībvalstīs izmantot 3. punktā minētos pakalpojumus un
 - (b) būtiska saikne ar a) punktā minēto(-ajām) dalībvalsti(-īm);
- (5) “uzņēmējdarbības veikšana” ir faktiskā 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;
- (6) “elektroniskie pierādījumi” ir pierādījumi, kurus pakalpojumu sniedzējs vai kāds cits tā vārdā glabā elektroniskā formā brīdī, kad tiek saņemts e-pierādījumu sniegšanas vai saglabāšanas rīkojuma sertifikāts, un tie ietver uzglabātus abonenta datus, piekļuves datus, darījumu datus un satura datus;
- (7) “abonenta dati” ir visi dati, kas attiecas uz:
- (a) abonenta vai klienta identitāti, piemēram, norādīto vārdu un uzvārdu, dzimšanas datumu, pasta vai ģeogrāfisko adresi, norēķinu un maksājumu datiem, telefona numuru vai e-pasta adresi;
 - (b) pakalpojuma veidu un tā ilgumu, ieskaitot tehniskos datus un datus, ar kuriem identificē saistītos tehniskos pasākumus vai saskarnes, ko izmanto vai ko sniedz abonents vai klients, un datus, kas ir saistīti ar pakalpojuma izmantošanas apstiprināšanu, izņemot paroles vai citus autentifikācijas līdzekļus, ko izmanto paroles vietā un ko nodrošina lietotājs, vai ko izveido pēc lietotāja pieprasījuma;
- (8) “piekļuves dati” ir dati, kas attiecas uz lietotāja piekļuves sesijas pakalpojumam sākumu un beigām un ir noteikti nepieciešami vienīgi pakalpojuma lietotāja identificēšanai, piemēram, izmantošanas datums un laiks, vai laiks, kad lietotājs ir pieteicies pakalpojumam un atteicies no tā, kopā ar IP adresi, ko interneta piekļuves pakalpojumu sniedzējs piešķir pakalpojuma lietotājam, kā arī dati, kas identificē izmantoto saskarni un lietotāja ID. Tas ietver elektronisko sakaru metadatus, kas definēti [Regulas par privātās dzīves neaizskaramību un personas datu aizsardzību elektronisko sakaru jomā] 4. panta 3. punkta g) apakšpunktā;

⁴⁴ Eiropas Parlamenta un Padomes 2015. gada 9. septembra [Direktīva \(ES\) 2015/1535](#), ar ko nosaka informācijas sniegšanas kārtību tehnisko noteikumu un Informācijas sabiedrības pakalpojumu noteikumu jomā (OV L 241, 17.9.2015., 1. lpp.).

- (9) “darījumu dati” ir dati, kas attiecas uz pakalpojumu sniedzēja piedāvātā pakalpojuma sniegšanu un nodrošina kontekstu vai papildu informāciju par šādu pakalpojumu un ko ģenerē vai apstrādā pakalpojumu sniedzēja informācijas sistēma, piemēram, ziņas vai cita veida mijiedarbības avots un galamērķis, dati par ierīces atrašanās vietu, datums, laiks, ilgums, lielums, maršruts, formāts, izmantotais protokols un saspiešanas veids, ja vien šādi dati nav daļa no piekļuves datiem. Tas ietver elektronisko sakaru metadatus, kas definēti [Regulas par privātās dzīves neaizskaramību un personas datu aizsardzību elektronisko sakaru jomā] 4. panta 3. punkta g) apakšpunktā;
- (10) “satura dati” ir visi elektroniskā formātā uzglabātie dati, piemēram, teksts, balss, video, attēli un skaņa, kas nav abonenta, piekļuves vai darījumu dati;
- (11) “informācijas sistēma” ir informācijas sistēma, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2013/40/ES 2. panta a) apakšpunktā⁴⁵;
- (12) “izdevējvalsts” ir dalībvalsts, kurā ir izdots Eiropas e-pierādījumu sniegšanas rīkojums vai Eiropas e-pierādījumu saglabāšanas rīkojums;
- (13) “izpildes valsts” ir dalībvalsts, kurā atrodas vai veic uzņēmējdarbību Eiropas e-pierādījumu sniegšanas rīkojuma vai Eiropas e-pierādījumu saglabāšanas rīkojuma adresāts un kurai tiek nosūtīti izpildei Eiropas e-pierādījumu sniegšanas rīkojums un Eiropas e-pierādījumu sniegšanas rīkojuma sertifikāts vai Eiropas e-pierādījumu saglabāšanas rīkojums un Eiropas e-pierādījumu saglabāšanas rīkojuma sertifikāts;
- (14) “izpildes iestāde” ir izpildes valsts kompetentā iestāde, kurai izdevējvalsts nosūta Eiropas e-pierādījumu sniegšanas rīkojumu un Eiropas e-pierādījumu sniegšanas rīkojuma sertifikātu vai Eiropas e-pierādījumu saglabāšanas rīkojumu un Eiropas e-pierādījumu saglabāšanas rīkojuma sertifikātu;
- (15) “ārkārtas gadījumi” ir situācijas, kad pastāv nenovēršami draudi personas dzīvībai vai fiziskai neaizskaramībai vai kritiskai infrastruktūrai, kā definēts Padomes Direktīvas 2008/114/EK 2. panta a) punktā⁴⁶.

3. pants Darbības joma

1. Šī regula attiecas uz pakalpojumu sniedzējiem, kas piedāvā pakalpojumus Savienībā.
2. Eiropas e-pierādījumu sniegšanas rīkojumus un Eiropas e-pierādījumu saglabāšanas rīkojumus var izdot tikai kriminālprocesā gan pirmstiesas, gan tiesas posmā. Rīkojumus var izdot arī tiesvedībā par noziedzīgu nodarījumu, par kuru izdevējvalstī var saukt pie atbildības vai sodīt juridisku personu.
3. Šajā regulā paredzētos rīkojumus var izdot tikai par datiem, kas attiecas uz Savienībā piedāvātajiem pakalpojumiem, kuri definēti 2. panta 3. punktā.

⁴⁵ Eiropas Parlamenta un Padomes [Direktīva 2013/40/ES](#) (2013. gada 12. augusts) par uzbrukumiem informācijas sistēmām un ar kuru aizstāj Padomes Pamatlēmumu 2005/222/TI (OV L 218, 14.8.2013., 8. lpp.).

⁴⁶ [Padomes Direktīva 2008/114/EK](#) (2008. gada 8. decembris) par to, lai apzinātu un noteiktu Eiropas Kritiskās infrastruktūras un novērtētu vajadzību uzlabot to aizsardzību (OV L 345 23.12.2008., 75. lpp.).

2. nodaļa. Eiropas e-pierādījumu sniegšanas rīkojums, Eiropas e-pierādījumu saglabāšanas rīkojums un sertifikāti

4. pants Izdevējiestāde

1. Eiropas e-pierādījumu sniegšanas rīkojumu par abonenta datiem un piekļuves datiem var izdot
 - (a) tiesnesis, tiesa, izmeklēšanas tiesnesis vai prokurors, kas ir kompetents attiecīgajā lietā, vai
 - (b) cita izdevējvalsts noteikta kompetenta iestāde, kura konkrētajā gadījumā rīkojas kā izmeklēšanas iestāde kriminālprocesā un kuras kompetencē ir pieprasīt pierādījumu vākšanu saskaņā ar valsts tiesību aktiem. Pēc tam, kad ir pārbaudīta Eiropas e-pierādījumu sniegšanas rīkojuma atbilstība Eiropas e-pierādījumu sniegšanas rīkojuma izdošanas nosacījumiem atbilstīgi šai regulai, šādu rīkojumu apstiprina tiesnesis, tiesa, izmeklēšanas tiesnesis vai prokurors izdevējvalstī.
2. Eiropas e-pierādījumu sniegšanas rīkojumu par darījumu un satura datiem var izdot tikai
 - (a) tiesnesis, tiesa vai izmeklēšanas tiesnesis, kas ir kompetents attiecīgajā lietā, vai
 - (b) cita izdevējvalsts noteikta kompetenta iestāde, kura konkrētajā gadījumā rīkojas kā izmeklēšanas iestāde kriminālprocesā un kuras kompetencē ir pieprasīt pierādījumu vākšanu saskaņā ar valsts tiesību aktiem. Pēc tam, kad ir pārbaudīta Eiropas e-pierādījumu sniegšanas rīkojuma atbilstība Eiropas e-pierādījumu sniegšanas rīkojuma izdošanas nosacījumiem atbilstīgi šai regulai, šādu rīkojumu apstiprina tiesnesis, tiesa vai izmeklēšanas tiesnesis izdevējvalstī.
3. Eiropas e-pierādījumu saglabāšanas rīkojumu var izdot:
 - (a) tiesnesis, tiesa, izmeklēšanas tiesnesis vai prokurors, kas ir kompetents attiecīgajā lietā; vai
 - (b) cita izdevējvalsts noteikta kompetenta iestāde, kura konkrētajā gadījumā rīkojas kā izmeklēšanas iestāde kriminālprocesā un kuras kompetencē ir pieprasīt pierādījumu vākšanu saskaņā ar valsts tiesību aktiem. Pēc tam, kad ir pārbaudīta Eiropas e-pierādījumu saglabāšanas rīkojuma atbilstība Eiropas e-pierādījumu saglabāšanas rīkojuma izdošanas nosacījumiem atbilstīgi šai regulai, šādu rīkojumu apstiprina tiesnesis, tiesa, izmeklēšanas tiesnesis vai prokurors izdevējvalstī.
4. Ja rīkojumu ir apstiprinājusi tiesu iestāde saskaņā ar 1. punkta b) apakšpunktu, 2. punkta b) apakšpunktu un 3. punkta b) apakšpunktu, minēto iestādi var uzskatīt arī par izdevējiestādi Eiropas e-pierādījumu sniegšanas rīkojuma sertifikāta un Eiropas e-pierādījumu saglabāšanas rīkojuma sertifikāta nosūtīšanas vajadzībām.

5. pants

Eiropas elektronisko pierādījumu sniegšanas rīkojuma izdošanas nosacījumi

1. Izdevējiestāde var izdot Eiropas e-pierādījumu sniegšanas rīkojumu tikai tad, ja ir izpildīti šajā pantā izklāstītie nosacījumi.
2. Eiropas e-pierādījumu sniegšanas rīkojums ir nepieciešams un proporcionāls 3. panta 2. punktā minētās tiesvedības vajadzībām, un to var izdot tikai tad, ja līdzīgs pasākums par tādu pašu noziedzīgu nodarījumu būtu pieejams salīdzināmā iekšzemes situācijā izdevējvalstī.
3. Eiropas e-pierādījumu sniegšanas rīkojumus par abonenta datu vai piekļuves datu sniegšanu var izdot par visiem noziedzīgiem nodarījumiem.
4. Eiropas e-pierādījumu sniegšanas rīkojumus par darījumu datu vai satura datu sniegšanu var izdot vienīgi
 - (a) par noziedzīgiem nodarījumiem, par kuriem izdevējvalstī ir paredzēta brīvības atņemšanas sods maksimālo ilgumu vismaz trīs gadi, vai
 - (b) par šādiem noziedzīgiem nodarījumiem, ja tie pilnībā vai daļēji ir izdarīti, izmantojot informācijas sistēmu:
 - par nodarījumiem, kas definēti Padomes Pamatlēmuma 2001/413/TI 3., 4. un 5. pantā⁴⁷;
 - par nodarījumiem, kas definēti Eiropas Parlamenta un Padomes Direktīvas 2011/93/ES 3. līdz 7. pantā⁴⁸;
 - par nodarījumiem, kas definēti Eiropas Parlamenta un Padomes 3. līdz 8. pantā;
 - (c) par noziedzīgiem nodarījumiem, kas definēti Eiropas Parlamenta un Padomes Direktīvas (ES) 2017/541 3. līdz 12. pantā un 14. pantā⁴⁹.
5. Eiropas e-pierādījumu sniegšanas rīkojumā iekļauj šādu informāciju:
 - (a) izdevējiestāde un (ja piemērojams) apstiprinātāja iestāde;
 - (b) Eiropas e-pierādījumu sniegšanas rīkojuma adresāts, kā minēts 7. pantā;
 - (c) personas, kuru dati tiek pieprasīti, izņemot gadījumus, kad rīkojuma vienīgais mērķis ir personas identificēšana;
 - (d) pieprasīto datu kategorija (abonenta dati, piekļuves dati, darījumu dati vai satura dati);
 - (e) laika periods, par kuru pieprasīts sniegt datus (ja piemērojams);
 - (f) izdevējvalsts krimināltiesību piemērojamās normas;
 - (g) ārkārtas situācijās vai pieprasījuma datus izpaust agrāk pamatojums;

⁴⁷ [Padomes Pamatlēmums 2001/413/TI](#) (2001. gada 28. maijs) par krāpšanas un viltošanas apkarošanu attiecībā uz bezskaidras naudas maksāšanas līdzekļiem (OV L 149, 2.6.2001., 1. lpp.).

⁴⁸ Eiropas Parlamenta un Padomes [Direktīva 2011/93/ES](#) (2011. gada 13. decembris) par seksuālas vardarbības pret bērniem, bērnu seksuālas izmantošanas un bērnu pornogrāfijas apkarošanu, un ar kuru aizstāj Padomes Pamatlēmumu 2004/68/TI (OV L 335, 17.12.2011., 1. lpp.).

⁴⁹ Eiropas Parlamenta un Padomes [Direktīva \(ES\) 2017/541](#) (2017. gada 15. marts) par terorisma apkarošanu un ar ko aizstāj Padomes Pamatlēmumu 2002/475/TI un groza Padomes Lēmumu 2005/671/TI (OV L 88, 31.3.2017., 6. lpp.).

- (h) gadījumos, kad pieprasītie dati tiek glabāti vai apstrādāti kā daļa no infrastruktūras, ko pakalpojumu sniedzējs nodrošina uzņēmumam vai citai struktūrai, kura nav fiziskas personas, apstiprinājums, ka rīkojums ir pieņemts saskaņā ar 6. punktu;
- (i) pasākuma nepieciešamības un proporcionalitātes pamatojums.
6. Gadījumos, kad pieprasītie dati tiek glabāti vai apstrādāti kā daļa no infrastruktūras, ko pakalpojumu sniedzējs nodrošina uzņēmumam vai citai struktūrai, kura nav fiziskas personas, Eiropas e-pierādījumu sniegšanas rīkojumu var adresēt tikai pakalpojumu sniedzējam, ja uzņēmumam vai struktūrai adresēti izmeklēšanas pasākumi vai uzņēmums nav piemēroti, jo īpaši tāpēc, ka tie varētu apdraudēt izmeklēšanu.
7. Ja izdevējiestādei ir iemesls uzskatīt, ka pieprasītos darījumu vai satura datus aizsargā imunitātes un privilēģijas, kas piešķirtas saskaņā ar tās dalībvalsts tiesību aktiem, kurā pakalpojumu sniedzējs ir adresāts, vai arī to izpaušana var ietekmēt attiecīgās dalībvalsts pamatintereses, piemēram, valsts drošības un aizsardzības jomā, izdevējiestādei pirms Eiropas e-pierādījumu sniegšanas rīkojuma izdošanas jālūdz precizējums, tostarp apspriežoties ar attiecīgās dalībvalsts kompetentajām iestādēm vai nu tieši, vai ar *Eurojust* vai Eiropas Tiesiskās sadarbības tīkla starpniecību. Ja izdevējiestāde konstatē, ka pieprasītos piekļuves, darījumu vai satura datus aizsargā šāda imunitāte un privilēģijas vai arī to izpaušana varētu ietekmēt citas dalībvalsts pamatintereses, tā neizdod Eiropas e-pierādījumu sniegšanas rīkojumu.

6. pants

Eiropas elektronisko pierādījumu saglabāšanas rīkojuma izdošanas nosacījumi

1. Izdevējiestāde var izdot Eiropas e-pierādījumu saglabāšanas rīkojumu tikai tad, ja ir izpildīti šajā pantā izklāstītie nosacījumi.
2. To var izdot, ja tas ir nepieciešams un proporcionāls, lai novērstu datu izņemšanu, dzēšanu vai grozīšanu, ņemot vērā turpmāku pieprasījumu sniegt šos datus, izmantojot savstarpēju tiesisko palīdzību, Eiropas izmeklēšanas rīkojumu vai Eiropas e-pierādījumu sniegšanas rīkojumu. Eiropas e-pierādījumu saglabāšanas rīkojumus var izsniegt par visiem noziedzīgiem nodarījumiem.
3. Eiropas e-pierādījumu saglabāšanas rīkojumā tiek iekļauta šāda informācija:
- (a) izdevējiestāde un (ja piemērojams) apstiprinātāja iestāde;
 - (b) Eiropas e-pierādījumu saglabāšanas rīkojuma adresāts, kā minēts 7. pantā;
 - (c) personas, kuru dati jāsaglabā, izņemot gadījumus, kad rīkojuma vienīgais mērķis ir personas identificēšana;
 - (d) saglabājamo datu kategorija (abonenta dati, piekļuves dati, darījumu dati vai satura dati);
 - (e) laika periods, par kuru pieprasīts saglabāt datus (ja piemērojams);
 - (f) izdevējvalsts krimināltiesību piemērojamās normas;
 - (g) pasākuma nepieciešamības un proporcionalitātes pamatojums.

7. pants

Eiropas elektronisko pierādījumu sniegšanas rīkojuma un Eiropas elektronisko pierādījumu saglabāšanas rīkojuma adresāts

1. Eiropas e-pierādījumu sniegšanas rīkojumu un Eiropas e-pierādījumu saglabāšanas rīkojumu adresē tieši juridiskajam pārstāvim, ko izraudzījies pakalpojumu sniedzējs ar mērķi vākt pierādījumus kriminālprocesā.
2. Ja nav iecelts neviens īpašais juridiskais pārstāvis, Eiropas e-pierādījumu sniegšanas rīkojumu un Eiropas e-pierādījumu saglabāšanas rīkojumu var adresēt jebkuram pakalpojumu sniedzēja uzņēmumam Savienībā.
3. Ja juridiskais pārstāvis neatbilst *EPOC* prasībām, ārkārtas situācijā saskaņā ar 9. panta 2. punktu *EPOC* var adresēt jebkuram pakalpojumu sniedzēja uzņēmumam Savienībā.
4. Ja juridiskais pārstāvis nepilda savus pienākumus, kas paredzēti 9. vai 10. pantā, un izdevējiestāde uzskata, ka pastāv nopietns datu zaudēšanas risks, Eiropas e-pierādījumu sniegšanas rīkojumu vai Eiropas e-pierādījumu saglabāšanas rīkojumu var adresēt jebkuram pakalpojumu sniedzēja uzņēmumam Savienībā.

8. pants

Eiropas e-pierādījumu sniegšanas un e-pierādījumu saglabāšanas rīkojuma sertifikāts

1. Eiropas e-pierādījumu sniegšanas vai e-pierādījumu saglabāšanas rīkojums tiek nosūtīts adresātam, kā definēts 7. pantā, izmantojot Eiropas e-pierādījumu sniegšanas rīkojuma sertifikātu (*EPOC*) vai Eiropas e-pierādījumu saglabāšanas rīkojuma sertifikātu (*EPOC-PR*).

Izdevēja vai apstiprinātāja iestāde aizpilda *EPOC*, kas pievienots regulas I pielikumā, vai *EPOC-PR*, kas pievienots regulas II pielikumā, paraksta to un apliecina tā saturu kā precīzu un pareizu.
2. *EPOC* vai *EPOC-PR* jānosūta tieši, izmantojot jebkākus līdzekļus, ar kuriem var iegūt rakstisku dokumentu ar nosacījumu, ka adresāts var noteikt tā autentiskumu.

Ja pakalpojumu sniedzēji, dalībvalstis vai Savienības iestādes ir izveidojušas īpašas platformas vai citus drošus kanālus, kas ļauj tiesībaizsardzības un tiesu iestādēm apstrādāt datu pieprasījumus, izdevējiestāde var izvēlēties nosūtīt sertifikātu, arī izmantojot šos kanālus.
3. *EPOC* ietver informāciju, kas minēta 5. panta 5. punkta a) līdz h) apakšpunktā, tostarp pietiekamu informāciju, kas adresātam ļauj identificēt izdevējiestādi un sazināties ar to. Sertifikātā neietver pasākuma nepieciešamības un proporcionalitātes pamatojumu, kā arī sīkāku informāciju par izmeklēšanu.
4. *EPOC-PR* ietver informāciju, kas minēta 6. panta 3. punkta a) līdz f) apakšpunktā, tostarp pietiekamu informāciju, kas adresātam ļauj identificēt izdevējiestādi un sazināties ar to. Sertifikātā neietver pasākuma nepieciešamības un proporcionalitātes pamatojumu, kā arī sīkāku informāciju par izmeklēšanu.
5. Vajadzības gadījumā *EPOC* vai *EPOC-PR* iztulko kādā no Savienības oficiālajām valodām, kas ir pieņemama adresātam. Ja nav norādīta neviena valoda, *EPOC* vai *EPOC-PR* tulko vienā no oficiālajām valodām tajā dalībvalstī, kurā dzīvo vai veic uzņēmējdarbību juridiskais pārstāvis.

9. pants
EPOC izpilde

1. Saņemot *EPOC*, adresāts nodrošina, ka pieprasītie dati tiek nosūtīti tieši izdevējiestādei vai tiesībaizsardzības iestādēm, kā norādīts *EPOC*, ne vēlāk kā 10 dienu laikā pēc *EPOC* saņemšanas, ja vien izdevējiestāde nav norādījusi pamatojumu pieprasījumam datus izpaust agrāk.
2. Ārkārtas gadījumos adresāts nosūta pieprasītos datus bez liekas kavēšanās, vēlākais, 6 stundu laikā pēc *EPOC* saņemšanas.
3. Ja adresāts nevar izpildīt savus pienākumus tādēļ, ka *EPOC* ir nepilnīgs, tajā ir acīmredzamas kļūdas vai nav norādīta pietiekama informācija *EPOC* izpildei, adresāts, izmantojot III pielikumā pievienoto veidlapu, bez liekas kavēšanās informē *EPOC* minēto iestādi un lūdz precizējumu. Adresāts informē izdevējiestādi, vai bija iespējams identificēt un saglabāt datus, kā izklāstīts 6. punktā. Izdevējiestāde reaģē nekavējoties un ne vēlāk kā 5 dienu laikā. Termiņi, kas noteikti 1. un 2. punktā, nav spēkā, kamēr nav sniegts precizējums.
4. Ja adresāts nevar izpildīt savus pienākumus nepārvaramas varas vai faktiskas neiespējamības apstākļu dēļ, kas nav attiecināmi uz adresātu vai pakalpojumu sniedzēju, ja tās ir dažādas personas, jo īpaši tāpēc, ka persona, kuras dati tiek pieprasīti, nav viņu klients vai dati tika dzēsti pirms *EPOC* saņemšanas, adresāts, izmantojot III pielikumā pievienoto veidlapu, nekavējoties informē *EPOC* minēto izdevējiestādi un paskaidro iemeslus. Ja ir izpildīti attiecīgie nosacījumi, izdevējiestāde atsauc *EPOC*.
5. Visos gadījumos, kad adresāts nesniedz pieprasīto informāciju, sniedz to nepilnīgi vai nenodrošina to noteiktajā termiņā citu iemeslu dēļ, viņš, izmantojot III pielikumā pievienoto veidlapu, bez liekas kavēšanās un vēlākais 1. un 2. punktā noteiktajos termiņos paziņo izdevējiestādei iemeslus. Izdevējiestāde pārskata rīkojumu, ņemot vērā pakalpojumu sniedzēja norādīto informāciju, un, ja nepieciešams, nosaka pakalpojumu sniedzējam jaunu termiņu datu sniegšanai.

Ja adresāts uzskata, ka *EPOC* nevar izpildīt, jo, pamatojoties tikai uz *EPOC* ietvertu informāciju, ir acīmredzams, ka sertifikāts acīmredzami pārkāpj Eiropas Savienības Pamattiesību hartu vai ir acīmredzami ļaunprātīgs, adresāts nosūta III pielikumā pievienoto veidlapu arī adresāta dalībvalsts kompetentajai izpildes iestādei. Šādos gadījumos kompetentā izpildes iestāde var tieši vai ar *Eurojust* vai Eiropas Tiesiskās sadarbības tīkla starpniecību lūgt izdevējiestādei precizējumu par Eiropas e-pierādījumu sniegšanas rīkojumu.
6. Ja adresāts nesniedz prasītos datus nekavējoties, viņš tos saglabā, izņemot gadījumu, kad *EPOC* ietvertā informācija neļauj adresātam identificēt pieprasītos datus, šādā gadījumā adresāts lūdz precizējumu saskaņā ar 3. punktu. Datus saglabā līdz brīdim, kad tie tiek sniegti vai nu pamatojoties uz precizētu Eiropas e-pierādījumu sniegšanas rīkojumu un tā sertifikātu, vai izmantojot citus kanālus, piemēram, savstarpēju tiesisko palīdzību. Ja datu sniegšana un saglabāšana vairs nav nepieciešama, izdevējiestāde un attiecīgā gadījumā izpildes iestāde saskaņā ar 14. panta 8. punktu informē par to adresātu bez liekas kavēšanās.

10. pants
EPOC-PR izpilde

1. Saņemot *EPOC-PR*, adresāts bez liekas kavēšanās saglabā prasītos datus. Datu saglabāšana tiek pārtraukta pēc 60 dienām, ja vien izdevējiestāde neapstiprina, ka ir izdots nākamais pieprasījums sniegt datus.
2. Ja izdevējiestāde 1. punktā noteiktajā termiņā apstiprina, ka ir izdots nākamais pieprasījums sniegt datus, adresāts saglabā datus tik ilgi, cik nepieciešams, lai sniegtu datus pēc nākamā pieprasījuma sniegt datus saņemšanas.
3. Ja datu saglabāšana vairs nav nepieciešama, izdevējiestāde bez liekas kavēšanās informē par to adresātu.
4. Ja adresāts nevar izpildīt savus pienākumus tādēļ, ka sertifikāts ir nepilnīgs, tajā ir acīmredzamas kļūdas vai nav norādīta pietiekama informācija *EPOC-PR* izpildei, adresāts, izmantojot III pielikumā pievienoto veidlapu, bez liekas kavēšanās informē par to *EPOC-PR* minēto iestādi un lūdz precizējumu. Izdevējiestāde reaģē nekavējoties un ne vēlāk kā 5 dienu laikā. Adresāts no savas puses nodrošina iespēju saņemt vajadzīgo precizējumu, lai izpildītu 1. punktā noteikto pienākumu.
5. Ja adresāts nevar izpildīt savus pienākumus nepārvaramas varas vai faktiskas neiespējamības apstākļu dēļ, kas nav attiecināmi uz adresātu vai pakalpojumu sniedzēju, ja tās ir dažādas personas, it īpaši tāpēc, ka persona, kuras dati tiek pieprasīti, nav viņu klients vai dati tika dzēsti pirms rīkojuma saņemšanas, adresāts, izmantojot III pielikumā pievienoto veidlapu, nekavējoties informē *EPOC-PR* minēto izdevējiestādi un paskaidro iemeslus. Ja šie nosacījumi ir izpildīti, izdevējiestāde atsauc *EPOC-PR*.
6. Visos gadījumos, kad adresāts nesaglabā prasīto informāciju citu iemeslu dēļ, kas norādīti III veidlapā, adresāts paziņo izdevējiestādei savas rīcības iemeslus bez liekas kavēšanās, izmantojot III pielikumā pievienoto veidlapu. Izdevējiestāde pārskata rīkojumu, ņemot vērā pakalpojumu sniedzēja sniegto informāciju.

11. pants
Konfidencialitāte un lietotāja informācija

1. Adresāti un pakalpojumu sniedzēji, ja tās ir dažādas personas, veic nepieciešamos pasākumus, lai nodrošinātu *EPOC* vai *EPOC-PR* konfidencialitāti, kā arī sniegto vai saglabāto datu konfidencialitāti un, ja to pieprasa izdevējiestāde, lai netraucētu attiecīgo kriminālprocesu, viņi atturas informēt personu, kuras dati tiek saglabāti.
2. Ja izdevējiestāde ir lūgusi adresātam neinformēt personu, kuras dati tiek pieprasīti, izdevējiestāde bez liekas kavēšanās par datu sniegšanu informē personu, kuras dati tiek pieprasīti, pamatojoties uz *EPOC*. Šī informācija var tikt aizkavēta tik ilgi, cik tas ir nepieciešami un proporcionāli, lai netraucētu attiecīgo kriminālprocesu.
3. Informējot personu, izdevējiestāde ietver informāciju par visiem pieejamajiem tiesiskās aizsardzības līdzekļiem, kas minēti 17. pantā.

12. pants
Izmaksu atlīdzināšana

Pakalpojumu sniedzējs var pieprasīt izdevējvalstij atlīdzināt viņa izdevumus, ja to paredz izdevējvalsts tiesību akti par iekšzemes rīkojumiem līdzīgās situācijās, pamatojoties uz šīm tiesību normām.

3. nodaļa. Sankcijas un to izpilde

13. pants

Sankcijas

Neskarot valsts tiesību aktus, kas paredz kriminālsodu piemērošanu, dalībvalstis nosaka noteikumus par finansiālām sankcijām, kuras piemērojamas par pienākumu pārkāpumiem saskaņā ar šīs regulas 9., 10. un 11. pantu, un veic visus vajadzīgos pasākumus, lai nodrošinātu, ka tās tiek izpildītas. Paredzētās finansiālās sankcijas ir efektīvas, proporcionālas un preventīvas. Dalībvalstis nekavējoties paziņo Komisijai par šiem noteikumiem un šiem pasākumiem, kā arī par jebkādiem turpmākiem grozījumiem, kas tos ietekmē.

14. pants

Izpildes procedūra

1. Ja adresāts, nenorādot izdevējiestādei pieņemamus iemeslus, neizpilda *EPOC* vai *EPOC-PR* prasības noteiktajā termiņā, izdevējiestāde, izmantojot jebkākus līdzekļus, ar kuriem var iegūt rakstisku dokumentu ar nosacījumu, ka izpildes iestāde var noteikt tā autentiskumu, var nosūtīt izpildes valsts kompetentajai iestādei Eiropas e-pierādījumu sniegšanas rīkojumu kopā ar *EPOC* vai Eiropas e-pierādījumu saglabāšanas rīkojumu kopā ar *EPOC-PR*, kā arī adresāta aizpildītu III pielikumā pievienoto veidlapu un jebkuru citu nozīmīgu dokumentu ar mērķi izpildīt rīkojumu. Šim nolūkam izdevējiestāde pārtulko rīkojumu, veidlapu un visus citus pievienotos dokumentus vienā no šīs dalībvalsts oficiālajām valodām un informē adresātu par to nosūtīšanu.
2. Pēc saņemšanas izpildes iestāde bez papildu formalitātēm atzīst Eiropas e-pierādījumu sniegšanas rīkojumu vai Eiropas e-pierādījumu saglabāšanas rīkojumu, kas nosūtīts saskaņā ar 1. punktu, un veic vajadzīgos pasākumus tā izpildei, izņemot gadījumus, kad izpildes iestāde uzskata, ka ir piemērojam viens no 4. vai 5. punktā norādītajiem pamatojumiem vai ka attiecīgos datus aizsargā imunitāte vai privilēģijas saskaņā ar tās valsts tiesību aktiem, vai ka to izpaušana var ietekmēt tās pamatintereses, piemēram, valsts drošību un aizsardzību. Izpildes iestāde pieņem lēmumu atzīt rīkojumu bez liekas kavēšanās un ne vēlāk kā 5 darba dienas pēc rīkojuma saņemšanas.
3. Ja izpildes iestāde atzīst rīkojumu, tā oficiāli pieprasa adresātam izpildīt attiecīgo pienākumu, informējot adresātu par iespēju iebilst pret tā izpildi, atsaucoties uz 4. vai 5. punktā minētajiem pamatojumiem, kā arī par piemērojamām sankcijām prasību neizpildes gadījumā, un nosaka termiņu prasību izpildei vai iebildumu iesniegšanai.
4. Adresāts var iebilst pret Eiropas e-pierādījumu sniegšanas rīkojuma izpildi, tikai pamatojoties uz šādiem iemesliem:
 - (a) izdevējiestāde nav izdevusi vai apstiprinājusi Eiropas e-pierādījumu sniegšanas rīkojumu, kā paredzēts 4. pantā;
 - (b) Eiropas e-pierādījumu sniegšanas rīkojums nav izdots par pārkāpumu, kas paredzēts 5. panta 4. punktā;

- (c) adresāts nevarēja izpildīt *EPOC* prasības faktiskās neiespējamības vai nepārvaramas varas apstākļu dēļ vai tāpēc, ka *EPOC* ir pieļautas acīmredzamas kļūdas;
 - (d) Eiropas e-pierādījumu sniegšanas rīkojums neattiecas uz datiem, kurus pakalpojumu sniedzējs pats vai cita persona viņa vārdā glabā brīdī, kad tiek saņemts *EPOC*;
 - (e) uz pakalpojumu neattiecas šī regula;
 - (f) no *EPOC* ietvertās informācijas vien skaidri izriet, ka rīkojums acīmredzami pārkāpj Hartu vai ir acīmredzami ļaunprātīgs.
5. Adresāts var iebilst pret Eiropas e-pierādījumu saglabāšanas rīkojuma izpildi, tikai pamatojoties uz šādiem iemesliem:
- (a) izdevējiestāde nav izdevusi vai apstiprinājusi Eiropas e-pierādījumu saglabāšanas rīkojumu, kā noteikts 4. pantā;
 - (b) pakalpojumu sniedzējs nevarēja ievērot *EPOC-PR* faktiskās neiespējamības vai nepārvaramas varas apstākļu dēļ vai tāpēc, ka *EPOC-PR* ir pieļautas acīmredzamas kļūdas;
 - (c) Eiropas e-pierādījumu saglabāšanas rīkojums neattiecas uz datiem, kurus pakalpojumi sniedzējs vai cita persona viņa vārdā glabā *EPOC-PR* izdošanas brīdī;
 - (d) pakalpojums neattiecas uz šīs regulas darbības jomu;
 - (e) no *EPOC-PR* ietvertās informācijas vien skaidri izriet, ka rīkojums acīmredzami pārkāpj Hartu vai ir acīmredzami ļaunprātīgs.
6. Adresāta iebilduma gadījumā izpildes iestāde lemj, vai izpildīt rīkojumu, ņemot vērā adresāta sniegto informāciju, un vajadzības gadījumā papildu informāciju, kas iegūta no izdevējiestādes saskaņā ar 7. punktu.
7. Pirms pieņemt lēmumu par rīkojuma neatzīšanu vai nepildīšanu saskaņā ar 2. un 6. punktu, izpildes iestāde apspriežas ar izdevējiestādi, izmantojot jebkādas piemērotus līdzekļus. Vajadzības gadījumā tā pieprasa papildu informāciju no izdevējiestādes. Izdevējiestāde atbild uz šādu pieprasījumu 5 darba dienu laikā.
8. Visus lēmumus nekavējoties paziņo izdevējiestādei un adresātam, izmantojot jebkādas līdzekļus, ar kuriem var iegūt rakstisku dokumentu.
9. Ja izpildes iestāde iegūst datus no adresāta, tā nosūta tos izdevējiestādei 2 darba dienu laikā, izņemot gadījumus, kad attiecīgos datus aizsargā imunitāte vai privilēģijas saskaņā ar tās valsts iekšzemes tiesību aktiem vai arī to izpaušana ietekmē valsts pamatintereses, piemēram, valsts drošību un aizsardzību. Šādā gadījumā tā informē izdevējiestādi par iemesliem, kāpēc dati nav nosūtīti.
10. Gadījumā, ja adresāts nepilda savus pienākumus saskaņā ar atzītu rīkojumu, kura izpildāmību ir apstiprinājusi izpildes iestāde, minētā iestāde saskaņā ar tās valsts tiesību aktiem piemēro finansiālas sankcijas. Pret lēmumu uzlikt naudas sodu ir pieejams efektīvs tiesiskās aizsardzības līdzeklis.

4. nodaļa. Tiesiskās aizsardzības līdzekļi

15. pants

Pārskatīšanas procedūra pretrunīgu pienākumu gadījumā, kuru pamatā ir trešās valsts pamattiesības vai pamatintereses

1. Ja adresāts uzskata, ka Eiropas e-pierādījumu sniegšanas rīkojuma izpilde būtu pretrunā ar piemērojamiem trešās valsts tiesību aktiem, kas aizliedz attiecīgo datu izpaušanu, pamatojoties uz to, ka tas ir nepieciešams, lai aizsargātu attiecīgo personu pamattiesības vai trešās valsts pamatintereses saistībā ar valsts drošību vai aizsardzību, tā saskaņā ar 9. panta 5. punktā minēto procedūru informē izdevējiestādi par Eiropas e-pierādījumu sniegšanas rīkojuma neizpildes iemesliem.
2. Pamatotajā iebildumā ietver visu būtisko informāciju par trešās valsts tiesību aktiem, to piemērojamību attiecīgajai lietai un pretrunīgā pienākuma raksturojumu. Iebildumu nevar pamatot ar faktu, ka trešās valsts piemērojamie tiesību akti neparedz līdzīgus noteikumus par e-pierādījumu sniegšanas rīkojuma izdošanas nosacījumiem, formalitātēm un procedūrām, vai tikai ar apstākli, ka dati tiek glabāti trešā valstī.
3. Ņemot vērā pamatoto iebildumu, izdevējiestāde pārskata Eiropas e-pierādījumu sniegšanas rīkojumu. Ja izdevējiestāde plāno apstiprināt Eiropas e-pierādījumu sniegšanas rīkojumu, tā pieprasa tās dalībvalsts kompetentajai tiesai veikt pārskatīšanu. Rīkojuma izpilde tiek apturēta līdz pārskatīšanas procedūras beigām.
Kompetentā tiesa vispirms novērtē, vai pastāv pretruna, balstoties uz pārbaudi par to,
 - (a) vai, pamatojoties uz lietas konkrētajiem apstākļiem, ir piemērojami trešās valsts tiesību akti, un ja ir, tad –
 - (b) vai trešās valsts akti, kas attiecas uz konkrētās lietas īpašajiem apstākļiem, aizliedz attiecīgo datu izpaušanu.
4. Veicot šo novērtējumu, tiesai būtu jāņem vērā, vai trešās valsts tiesību akti tā vietā, lai aizsargātu pamattiesības vai trešās valsts pamatintereses, kas saistītas ar valsts drošību vai aizsardzību, acīmredzami cenšas aizsargāt citas intereses vai arī ir vērsti uz to, lai kriminālizmeklēšanas ietvaros aizsargātu nelikumīgas darbības no tiesībaizsardzības iestāžu pieprasījumiem.
5. Ja kompetentā tiesa konstatē, ka nepastāv būtiskas pretrunas 1. un 4. punkta nozīmē, tā apstiprina šo rīkojumu. Ja kompetentā tiesa konstatē būtisku pretrunu 1. un 4. punkta nozīmē, tā ar savas valsts centrālās iestādes starpniecību nosūta attiecīgās trešās valsts centrālajām iestādēm visus attiecīgos faktus un juridisko informāciju attiecībā uz lietu, nosakot 15 dienu termiņu atbildes sniegšanai. Pēc trešās valsts centrālās iestādes pamatota pieprasījuma termiņu var pagarināt līdz 30 dienām.
6. Ja trešās valsts centrālā iestāde noteiktajā termiņā informē kompetento tiesu par to, ka tā iebilst pret Eiropas e-pierādījumu sniegšanas rīkojuma izpildi šajā lietā, kompetentā tiesa atceļ rīkojumu un informē izdevējiestādi un adresātu. Ja (pagarinātajā) termiņā netiek saņemti nekādi iebildumi, kompetentā tiesa nosūta atgādinājumu trešās valsts centrālajai iestādei, dodot tai vēl 5 dienas atbildes sniegšanai un informējot par atbildes nesniegšanas sekām. Ja šajā papildu termiņā netiek saņemti nekādi iebildumi, kompetentā tiesa apstiprina rīkojumu.
7. Ja kompetentā tiesa konstatē, ka rīkojums ir jāapstiprina, tā par to informē izdevējiestādi un adresātu, kurš rīkojumu izpilda.

16. pants

Pārskatīšanas procedūra pretrunīgu pienākumu gadījumā, kuru pamatā ir citi iemesli

1. Ja adresāts uzskata, ka Eiropas e-pierādījumu sniegšanas rīkojuma izpilde būtu pretrunā ar piemērojamiem trešās valsts tiesību aktiem, kas aizliedz atklāt attiecīgos datus, pamatojoties uz citiem iemesliem, nevis tiem, kas minēti 15. pantā, tā saskaņā ar 9. panta 5. punktā minēto procedūru informē izdevējiestādi par Eiropas e-pierādījumu sniegšanas rīkojuma neizpildes iemesliem.
2. Pamatotajā iebildumā jāietver visa būtiskā informācija par trešās valsts tiesību aktiem, to piemērojamība attiecīgajā lietā un pretrunīgā pienākuma raksturojums. Iebildumu nevar pamatot ar faktu, ka trešās valsts piemērojamie tiesību akti neparedz līdzīgus noteikumus par e-pierādījumu sniegšanas rīkojuma izdošanas nosacījumiem, formalitātēm un procedūrām, vai tikai ar apstākli, ka dati tiek glabāti trešā valstī.
3. Ņemot vērā pamatoto iebildumu, izdevējiestāde pārskata Eiropas e-pierādījumu sniegšanas rīkojumu. Ja izdevējiestāde plāno apstiprināt Eiropas e-pierādījumu sniegšanas rīkojumu, tā pieprasa tās dalībvalsts kompetentajai tiesai veikt pārskatīšanu. Rīkojuma izpilde tiek apturēta līdz pārskatīšanas procedūras beigām.
4. Kompetentā tiesa vispirms novērtē, vai pastāv pretruna, balstoties uz pārbaudi par to,
 - (a) vai, pamatojoties uz lietas konkrētajiem apstākļiem, ir piemērojami trešās valsts tiesību akti, un ja ir, tad –
 - (b) vai trešās valsts akti, kas attiecas uz konkrētās lietas īpašajiem apstākļiem, aizliedz attiecīgo datu izpaušanu.
5. Ja kompetentā tiesa konstatē, ka nepastāv būtiskas pretrunas 1. un 4. punkta nozīmē, tā apstiprina šo rīkojumu. Ja kompetentā tiesa konstatē, ka trešās valsts tiesību akts, ko piemēro izskatāmās lietas īpašajos apstākļos, aizliedz attiecīgo datu izpaušanu, kompetentā tiesa nosaka, vai apstiprināt vai atsaukt rīkojumu, jo īpaši pamatojoties uz šādiem faktoriem:
 - (a) intereses, ko aizsargā trešās valsts tiesību akti, tostarp trešās valsts intereses nepieļaut datu izpaušanu;
 - (b) kriminālprocesa, par kuru rīkojums tika izdots, saistības pakāpe ar kādu no abām jurisdikcijām, uz ko cita starpā norāda:

personas, kuras dati tiek prasīti, un/ vai cietušā(-o) atrašanās vieta, valstspiederība un dzīvesvieta;

vieta, kur izdarīts attiecīgais noziedzīgais nodarījums;
 - (c) pakalpojumu sniedzēja un attiecīgās trešās valsts saistības pakāpe; šajā sakarā datu glabāšanas vieta pati par sevi nav pietiekams faktors, lai konstatētu būtisku saistības pakāpi;
 - (d) izmeklēšanas valsts interese par attiecīgo pierādījumu iegūšanu, ņemot vērā nodarījuma smagumu un pierādījumu iegūšanas svarīgumu;
 - (e) iespējamās sekas adresātam vai pakalpojumu sniedzējam par Eiropas e-pierādījumu sniegšanas rīkojuma prasību izpildi, tostarp iespējamās sankcijas.

6. Ja kompetentā tiesa izlemj atcelt rīkojumu, tā informē par to izdevējiestādi un adresātu. . Ja kompetentā tiesa konstatē, ka rīkojums ir jāapstiprina, tā par lēmumu informē izdevējiestādi un adresātu, kurš rīkojumu izpilda.

17. pants

Efektīvi tiesiskās aizsardzības līdzekļi

1. Aizdomās turētās un apsūdzētās personas, kuru dati tika iegūti ar Eiropas e-pierādījumu sniegšanas rīkojumu, ir tiesīgas uz efektīviem tiesiskās aizsardzības līdzekļiem, lai vērstos pret Eiropas e-pierādījumu sniegšanas rīkojuma piemērošanu kriminālprocesā, par kuru tika izdots rīkojums, neskarot Direktīvā (ES) 2016/680 un Regulā (ES) Nr. 2016/679 paredzētos tiesiskās aizsardzības līdzekļus.
2. Ja persona, kuras dati tika iegūti, nav aizdomās turētā vai apsūdzētā persona kriminālprocesā, par kuru tika izdots rīkojums, šai personai ir tiesības uz efektīviem tiesiskās aizsardzības līdzekļiem, lai vērstos pret Eiropas e-pierādījumu sniegšanas rīkojumu izdevējvalstī, neskarot Direktīvā (ES) 2016/680 un Regulā (ES) 2016/679 paredzētos tiesiskās aizsardzības līdzekļus.
3. Šādas tiesības uz efektīvu tiesisko aizsardzību īsteno izdevējvalsts tiesā saskaņā ar tās valsts tiesību aktiem, un tiesības ietver iespēju apstrīdēt pasākuma likumību, tostarp tā nepieciešamību un proporcionalitāti.
4. Neskarot 11. pantu, izdevējiestāde veic attiecīgus pasākumus, lai nodrošinātu, ka tiek sniegta informācija par valsts tiesību aktos paredzētajām iespējām izmantot tiesiskās aizsardzības līdzekļus un par to efektīvu izmantošanu.
5. Tiesiskās aizsardzības līdzekļu izmantošanai piemēro tādus pašus termiņus vai citus nosacījumus kā līdzīgās iekšzemes lietās un tādā veidā, kas garantē attiecīgajām personām šo līdzekļu efektīvu īstenošanu.
6. Neskarot valstu procesuālos noteikumus, dalībvalstis nodrošina, ka, vērtējot pierādījumus, kas iegūti, izmantojot Eiropas e-pierādījumu sniegšanas rīkojumu, kriminālprocesā izdevējvalstī tiek ievērotas tiesības uz aizstāvību un taisnīgu lietas izskatīšanu.

18. pants

Privilēģiju un imunitātes nodrošināšana saskaņā ar izpildes valsts tiesību aktiem

Ja darījumu vai satura datus, kas iegūti ar Eiropas e-pierādījumu sniegšanas rīkojumu, aizsargā imunitāte vai privilēģijas, kuras piešķirtas saskaņā ar adresāta dalībvalsts tiesību aktiem, vai tie ietekmē attiecīgās dalībvalsts pamatintereses, piemēram, valsts drošību un aizsardzību, izdevējvalsts tiesa kriminālprocesa laikā, par kuru tika izdots rīkojums, nodrošina, ka šie iemesli tiek ņemti vērā tādā pašā veidā kā tad, ja tie būtu noteikti tās valsts tiesību aktos, novērtējot attiecīgo pierādījumu atbilstību un pieņemamību. Tiesa var apspriesties ar attiecīgās dalībvalsts iestādēm, Eiropas Tiesiskās sadarbības tīklu krimināllietās vai *Eurojust*.

5. nodaļa. Nobeiguma noteikumi

19. pants

Uzraudzība un ziņošana

1. Vēlākais līdz [šīs regulas piemērošanas datums] Komisija izstrādā detalizētu programmu šīs regulas iznākumu, rezultātu un ietekmes uzraudzībai. Uzraudzības programmā norāda izmantojamos līdzekļus un intervālus, kas jāievēro datu un citu nepieciešamo pierādījumu vākšanā. Tajā norāda darbības, kas Komisijai un dalībvalstīm jāveic, apkopojot un analizējot datus un citus pierādījumus.
2. Jebkurā gadījumā dalībvalstis apkopo un saglabā visaptverošu statistiku, kas saņemta no attiecīgajām iestādēm. Katru gadu līdz 31. martam apkopotos datus par iepriekšējo kalendāro gadu nosūta Komisijai, un šie dati ietver:
 - (a) izdoto *EPOC* un *EPOC-PR* skaitu pēc pieprasīto datu veida, pakalpojumu sniedzējiem, kam rīkojums adresēts, un situācijas (vai tas ir ārkārtas gadījums);
 - (b) izpildīto un neizpildīto *EPOC* skaitu pēc pieprasīto datu veida, pakalpojumu sniedzējiem, kam rīkojums adresēts, un situācijas (vai tas ir ārkārtas gadījums);
 - (c) attiecībā uz izpildītajiem *EPOC* — vidējo ilgumu pieprasīto datu saņemšanai no *EPOC* izdošanas brīža līdz datu sniegšanai pēc pieprasīto datu veida, pakalpojumu sniedzējiem, kam rīkojums adresēts, un situācijas (vai tas ir ārkārtas gadījums);
 - (d) izpildes valstij nosūtīto un tajā izpildei saņemto Eiropas e-pierādījumu sniegšanas rīkojumu skaitu pēc pieprasīto datu veida, pakalpojumu sniedzējiem, kam rīkojums adresēts, un situācijas (vai tas ir ārkārtas gadījums), un izpildīto rīkojumu skaitu;
 - (e) pret Eiropas e-pierādījumu sniegšanas rīkojumiem izmantojamo tiesiskās aizsardzības līdzekļu skaitu izdevējvalstī un izpildes valstī pēc pieprasīto datu veida.

20. pants

Grozījumi sertifikātos un veidlapās

Komisija saskaņā ar 21. pantu pieņem deleģētos aktus, lai grozītu I, II un III pielikumu ar mērķi efektīvi risināt iespējamu nepieciešamību veikt uzlabojumus *EPOC* saturā un *EPOC-PR* veidlapās, kā arī veidlapās, kas izmantojamas informācijas sniegšanai par neiespējamību izpildīt *EPOC* vai *EPOC-PR*.

21. pants

Deleģēšanas īstenošana

1. Pilnvaras pieņemt deleģētos aktus Komisijai piešķir, ievērojot šajā pantā izklāstītos nosacījumus.
2. Šīs regulas 20. pantā minētās pilnvaras deleģē uz nenoteiktu laiku no [šīs regulas piemērošanas diena].
3. Eiropas Parlaments vai Padome jebkurā laikā var atsaukt 20. pantā minēto pilnvaru deleģēšanu. Ar lēmumu par atsaukšanu izbeidz tajā norādīto pilnvaru deleģēšanu. Lēmums stājas spēkā nākamajā dienā pēc tā publicēšanas *Eiropas Savienības*

Oficiālajā Vēstnesī vai vēlākā dienā, kas tajā norādīta. Tas neskar jau spēkā esošos deleģētos aktus.

4. Pirms deleģētā akta pieņemšanas Komisija apspriežas ar katras dalībvalsts ieceltajiem speciālistiem saskaņā ar principiem, kas noteikti 2016. gada 13. aprīļa Iestāžu nolīgumā par labāku likumdošanas procesu⁵⁰.
5. Tiklīdz Komisija pieņem deleģēto aktu, tā par to paziņo vienlaikus Eiropas Parlamentam un Padomei.
6. Saskaņā ar 20. pantu pieņemts deleģētais akts stājas spēkā tikai tad, ja divos mēnešos no dienas, kad minētais akts paziņots Eiropas Parlamentam un Padomei, ne Eiropas Parlaments, ne Padome nav izteikuši iebildumus vai ja pirms minētā laikposma beigām gan Eiropas Parlaments, gan Padome ir informējuši Komisiju par savu nodomu neizteikt iebildumus. Pēc Eiropas Parlamenta vai Padomes iniciatīvas šo laikposmu pagarina par diviem mēnešiem.

22. pants Paziņojumi

1. Līdz [šīs regulas piemērošanas datums] katra dalībvalsts paziņo Komisijai šādu informāciju:
 - (a) iestādes, kuras saskaņā ar attiecīgās valsts tiesību aktiem ir kompetentas atbilstīgi 4. pantam izdot un/vai apstiprināt Eiropas e-pierādījumu sniegšanas rīkojumus un Eiropas e-pierādījumu saglabāšanas rīkojumus;
 - (b) izpildes iestāde vai iestādes, kas ir kompetentas citas dalībvalsts vārdā izpildīt Eiropas e-pierādījumu sniegšanas rīkojumus un Eiropas e-pierādījumu saglabāšanas rīkojumus;
 - (c) tiesas, kas ir kompetentas izskatīt adresātu pamatotus iebildumus saskaņā ar 15. un 16. pantu.
2. Saskaņā ar šo pantu saņemto informāciju Komisija dara publiski pieejamu īpašā tīmekļa vietnē vai Padomes Lēmuma 2008/976/TI 9. pantā minētajā Eiropas Tiesiskās sadarbības tīkla tīmekļa vietnē⁵¹.

23. pants Saistība ar Eiropas izmeklēšanas rīkojumiem

Dalībvalstu iestādes var turpināt izdot Eiropas izmeklēšanas rīkojumus saskaņā ar Direktīvu 2014/41/ES, lai vāktu pierādījumus, kas arī ietilptu šīs regulas darbības jomā.

24. pants Izvērtējums

Vēlākais [5 gadus pēc šīs regulas piemērošanas dienas] Komisija veic regulas izvērtējumu un iesniedz Eiropas Parlamentam un Padomei ziņojumu par šīs regulas darbību, ziņojumā iekļauj novērtējumu par nepieciešamību paplašināt regulas darbības jomu. Vajadzības gadījumā ziņojumam pievieno tiesību aktu priekšlikumus. Izvērtējumu veic saskaņā ar Komisijas

⁵⁰ OV L 123, 12.5.2016., 13. lpp.

⁵¹ Padomes Lēmums 2008/976/TI (2008. gada 16. decembris) par Eiropas Tiesiskās sadarbības tīklu (OV L 348, 24.12.2008., 130. lpp.).

pamatnostādnēm par labāku regulējumu. Dalībvalstis sniedz Komisijai informāciju, kas nepieciešama šā ziņojuma sagatavošanai.

*25. pants
Stāšanās spēkā*

Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

To piemēro no *[6 mēneši pēc tās stāšanās spēkā]*.

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs saskaņā ar Līgumiem.

Briselē,

*Eiropas Parlamenta vārdā –
priekšsēdētājs*

*Padomes vārdā –
priekšsēdētājs*