Mnenje št. 23/2018 o predlogih Komisije o evropskem nalogu za predložitev in evropskem nalogu za zavarovanje elektronskih dokazov v kazenskih zadevah (člen 70(1)(b))

Sprejeto 26. septembra 2018

Vsebina

Evropski odbor za varstvo podatkov

je ob upoštevanju člena 70(1)(b) Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES

SPREJEL NASLEDNJE MNENJE:

Uvod

Komisija je aprila 2018 predstavila predlog uredbe o evropskem nalogu za predložitev in evropskem nalogu za zavarovanje elektronskih dokazov v kazenskih zadevah ter predlog direktive o določitvi harmoniziranih pravil o imenovanju pravnih zastopnikov za namene zbiranja dokazov v kazenskih postopkih. Predloga COM(2018) 225 final in COM(2018) 226 final se dopolnjujeta. Splošni cilj, za uresničitev katerega si prizadeva Komisija, je izboljšanje sodelovanja med organi držav članic in ponudniki storitev, vključno s tistimi iz držav nečlanic EU, ter predlaganje rešitev za težave pri opredeljevanju in izvrševanju pristojnosti v kibernetskem prostoru.

V osnutku uredbe so predvidena pravila in postopki, ki se uporabljajo za izdajo in izvršitev nalogov za predložitev in zavarovanje dokazov ter njihovo vročitev ponudnikom elektronskih komunikacijskih storitev, osnutek direktive pa določa minimalna pravila za imenovanje pravnega zastopnika za ponudnike storitev, ki nimajo poslovne enote v EU.

Delovna skupina iz člena 29 je novembra 2017[1], preden je Komisija predložila katerega od osnutkov predlogov, opozorila na potrebo po zagotovitvi, da je vsak zakonodajni predlog popolnoma v skladu zlasti z veljavnim pravnim redom EU na področju varstva podatkov ter pravom EU in sodno prakso na splošno.

Delovna skupina iz člena 29 je zlasti opozorila na omejitve pravic do varstva podatkov in zasebnosti v zvezi s podatki, ki jih obdelujejo ponudniki telekomunikacijskih storitev in storitev informacijske družbe, zlasti kadar jih nadalje obdelajo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, spomnila na potrebo po zagotovitvi skladnosti vsakega instrumenta EU z veljavno Konvencijo Sveta Evrope o kibernetski kriminaliteti, sklenjeno v Budimpešti, in direktivo EU o evropskem preiskovalnem nalogu (EPN) ter priporočila, naj se pojasnijo ustrezna postopkovna pravila, s katerimi se ureja dostop do elektronskih dokazov (e-dokazov) na nacionalni ravni in ravni EU, da bi se zagotovilo, da z novim instrumentom organom ne bodo podeljena nova pooblastila, ki jih na nacionalni ravni ne bi imeli. Delovna skupina iz člena 29 je poleg teh splošnih pripomb podala pripombe o zakonodajnih možnostih, ki jih je takrat proučevala Komisija ter ki so se nanašale na kategorije zadevnih podatkov in ustrezne zaščitne ukrepe za dostop do teh podatkov, o možnosti, da se z nalogi/zahtevami za predložitev podatkov od ponudnikov storitev zahteva predložitev podatkov, ki so zunaj EU, ter o vsebinskih in postopkovnih pogojih, ki so potrebni, da bi bili zaščitni ukrepi povezani z neposrednim dostopom do podatkov.

Ker sta zdaj na voljo konkretna predloga o e-dokazih, želi EOVP podati podrobnejšo analizo predlaganih pravnih instrumentov z vidika varstva podatkov.

[1] Glej izjavo Delovne skupine iz člena 29 (http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801).

1. Pravna podlaga predloga uredbe (člen 82 PDEU)

Pravna podlaga, predlagana za osnutek uredbe o e-dokazih, je člen 82(1) PDEU o pravosodnem sodelovanju v kazenskih zadevah, ki določa:

> „1. Pravosodno sodelovanje v kazenskih zadevah v Uniji temelji na načelu vzajemnega priznavanja sodb in sodnih odločb in vključuje približevanje zakonov in drugih predpisov držav članic na področjih, navedenih v odstavku 2 in v členu 83.
>
> Evropski parlament in Svet po rednem zakonodajnem postopku sprejmeta ukrepe za:
>
> (a) določitev pravil in postopkov za zagotovitev priznavanja vseh oblik sodb in sodnih odločb v celotni Uniji;
>
> (b) preprečevanje in reševanje sporov o pristojnosti med državami članicami;
>
> (c) spodbujanje usposabljanja sodnikov in sodnega osebja;
>
> (d) lažje sodelovanje med sodnimi ali drugimi enakovrednimi organi držav članic pri kazenskih postopkih in izvrševanju odločb.“

Kot je Komisija poudarila v oceni učinka, priloženi predlogoma, je v „členu 82(1) določeno, da pravosodno sodelovanje v kazenskih zadevah v Uniji temelji na načelu vzajemnega priznavanja. Ta pravna podlaga bi zajemala morebitno zakonodajo o neposrednem sodelovanju s ponudniki storitev, v okviru katerega bi organ v državi članici izdajateljici neposredno naslovil subjekt (ponudnika storitev) v državi izvršiteljici in mu celo naložil obveznosti. S tem bi bila v vzajemno priznavanje uvedena nova razsežnost, ki presega tradicionalno pravosodno sodelovanje v Uniji, ki za zdaj temelji na postopkih, v katere sta vključena dva pravosodna organa, eden v državi izdajateljici in drugi v državi izvršiteljici“ (poudarek je dodan).

Ker je uporaba te pravne podlage v okviru neposrednih zahtev med javnimi organi in zasebnimi strankami nova, EOVP obžaluje, da Komisija ni predložila nadaljnje analize ali ocene.

Kot je Delovna skupina že poudarila v prejšnji izjavi, EOVP še naprej poudarja svoje pomisleke glede ustreznosti te pravne podlage, ki so podprti z analizo Sodišča Evropske unije in njegovega generalnega pravobranilca v Mnenju št. 1/15. Med napredkom, doseženim glede veljavnosti člena 82 kot pravne podlage za osnutek sporazuma o evidencah podatkov o potnikih med EU in Kanado, je Sodišče Evropske unije poudarilo, da pristojni kanadski organ „ni niti sodni niti drug enakovreden organ“[2]. Zdi se, da si je v okviru predlogov o e-dokazih po navedbah Komisije treba prizadevati predvsem, da bi se izognili „preveč zamudnemu“ pravosodnemu sodelovanju. Zato predlog temelji na načelu, da bi moralo sodelovanje namesto med dvema organoma potekati med organom in ponudnikom storitev. V predvidenem postopku so zasebni subjekti zlasti prejemniki in se morajo odzvati na zahteve pravosodnih organov.

EOVP ugotavlja, da bi lahko postopek izvršitve naloga za predložitev ali naloga za zavarovanje dokazov pomenil vključitev organa prejemnika v primeru, ko ponudnik storitev, ki prejme nalog, ne izpolni svojih obveznosti, zaradi česar bo potreben poziv k naknadni izvršitvi naloga. Ker pa je glavni cilj vzpostavljenega postopka ravno ta, da se organ prejemnik ne vključi, EOVP dvomi, da bi ta pomožni postopek lahko upravičil uporabo člena 82 kot edine pravne podlage za zadevni instrument.

[2] Glej točko 103 Mnenja št. 1/15 in točko 108 sklepnih predlogov generalnega pravobranilca v tej zadevi.

EOVP zato meni, da se lahko člen 82 kot pravna podlaga uporabi za glavne postopkovne korake sodelovanja, ki poteka med dvema pravosodnima organoma, in da bi bilo treba za to vrsto sodelovanja uporabiti drugo pravno podlago.

2. Nujnost e-dokazov v primerjavi s pogodbami o medsebojni pravni pomoči in EPN

EOVP opozarja na zavezo Komisije, da bo proučila ovire za kazenske preiskave, zlasti v zvezi z vprašanjem dostopa do e-dokazov. Komisija je v obrazložitvenem memorandumu pojasnila ozadje predloga ter poudarila minljivost e-dokazov, njihovo mednarodno razsežnost in potrebo po prilagoditvi mehanizmov sodelovanja digitalni dobi. Namen predlogov uredbe in direktive za pošiljanje e-dokazov in dostop do njih ni nadomestiti prejšnje instrumente sodelovanja v kazenskih zadevah, kot so Budimpeška konvencija, pogodba o medsebojni pravni pomoči in evropski preiskovalni nalog (direktiva o EPN). Po navedbah Komisije sta predloga o e-dokazih namenjena izboljšanju pravosodnega sodelovanja v kazenskih zadevah med organi in ponudniki storitev v Evropski uniji, pa tudi s tretjimi državami, zlasti Združenimi državami Amerike.

Ker bosta ti novi dodatni orodji izrecno namenjeni pošiljanju e-dokazov in dostopu do njih, bo EOVP ocenil dodano vrednost instrumentov glede na direktivo o EPN in pogodbo o medsebojni pravni pomoči.

a) Nujnost e-dokazov v primerjavi z zaščitnimi ukrepi, ki jih zagotavljajo EPN in pogodbe o medsebojni pravni pomoči

Glavni argument Komisije v korist predlogov o e-dokazih je pospešitev postopka zavarovanja in pridobivanja e-dokazov, ki jih shranjujejo in/ali imajo ponudniki storitev s poslovno enoto v drugi jurisdikciji.

Vendar EOVP obžaluje, da potreba po novem instrumentu za organizacijo dostopa do e-dokazov ni bila dokazana v oceni učinka. Dejansko v predlogih ni dokazano, da se za dosego cilja predloga o e-dokazih ne bi moglo uporabiti nobeno drugo manj vsiljivo sredstvo, predvidene pa bi lahko bile tudi druge rešitve. Proučila bi se lahko na primer možnost spremembe in izboljšanja direktive o EPN, s čimer bi se izpolnila tudi posebna zahteva iz navedene direktive, da je treba potrebo po spremembi besedila oceniti do 21. maja 2019[3]. Druga možnost bi lahko bila, da bi se uporaba nalogov za zavarovanje dokazov predvidela za zamrznitev podatkov do izdaje formalne zahteve na podlagi pogodbe o medsebojni pravni pomoči. S tema možnostma bi se omogočila ohranitev zaščitnih ukrepov, zagotovljenih v teh instrumentih, hkrati pa bi se zagotovilo, da zahtevani osebni podatki niso izbrisani.

EOVP opozarja, da so roki, določeni v direktivi o EPN, daljši kot v predlogu o e-dokazih. Dejansko ima izvršitveni organ na voljo 30 dni za sprejetje odločitve o priznanju zahteve[4], nalog pa bi moral nato izvršiti v 90 dneh[5]. Po mnenju EOVP je 30 dni za premislek, ki jih imajo izvršitveni organi na voljo v direktivi o EPN, ključni zaščitni ukrep, ki jim omogoči oceno, ali je zahteva za izvršitev dobro utemeljena ter v skladu z vsemi pogoji za izdajo in posredovanje EPN[6].

[3] Glej člen 37 direktive o EPN.
[4] Člen 12(3) direktive o EPN.
[5] Člen 12(4) direktive o EPN.
[6] Člen 6 direktive o EPN.

EOVP skrbi, da zaradi 10-dnevnega roka iz predlogov o e-dokazih za izvršitev potrdila o evropskem nalogu za predložitev dokazov, ki ne omogoča časa za premislek, ne bo mogoče ustrezno oceniti, ali navedeno potrdilo izpolnjuje vsa merila in je pravilno izpolnjeno.

EOVP zato priporoča, naj se prejemniku potrdila o evropskem nalogu za predložitev dokazov da na voljo več časa za odločitev, ali bi bilo treba nalog izvršiti ali ne.

EOVP opozarja, da v primeru evropskega naloga za zavarovanje dokazov (potrdila o evropskem nalogu za zavarovanje dokazov) ni jamstva, da bo zavarovanje podatkov omejeno na tiste podatke, ki jih je treba predložiti. Dejansko so lahko podatki zavarovani več kot 60 dni, ker organu izdajatelju ni določen rok, v katerem mora naslovnika obvestiti, da odstopa od izdaje ali da umika nalog za predložitev dokazov. EOVP zato priporoča vsaj določitev roka, v katerem mora organ izdajatelj odstopiti od izdaje ali umakniti nalog za predložitev dokazov, da se zagotovi skladnost z načelom najmanjšega obsega podatkov iz Splošne uredbe o varstvu podatkov[7].

Nazadnje, EOVP opozarja, da mora v skladu z direktivo o EPN država izdajateljica dokaze vrniti izvršitvenemu organu[8]. Vendar v predlogu uredbe o e-dokazih taka možnost ni predvidena. Ni jasno, kaj se z e-dokazi zgodi po tem, ko se pošljejo organu izdajatelju.

EOVP zato priporoča, da bi moral predlog uredbe vsebovati več informacij o uporabi e-dokazov po njihovem posredovanju organu izdajatelju, da bi se zagotovila skladnost s Splošno uredbo o varstvu podatkov in načelom preglednosti[9], pa tudi načelom specifičnosti, določenim s pogodbami o medsebojni pravni pomoči.

b) Opustitev načela dvojne kaznivosti

EOVP priznava, da je vzajemno priznavanje odvisno od uporabe dvojne kaznivosti, s pomočjo katere države članice ohranjajo suverenost. Vendar se za dvojno kaznivost vse bolj šteje, da ovira dobro pravosodno sodelovanje. Države članice EU so vse bolj pripravljene sodelovati, tudi če se preiskovalni ukrepi nanašajo na dejanja, ki se v njihovem nacionalnem pravu ne štejejo za kaznivo dejanje. Vendar EOVP opozarja, da je namen načela dvojne kaznivosti zagotoviti dodatni zaščitni ukrep za zagotovitev, da se država ne more zanašati na pomoč druge države pri uporabi kazenske sankcije, ki v pravu te druge države ne obstaja. To bi na primer državi preprečilo, da bi od druge države zahtevala pomoč pri odvzemu prostosti osebe zaradi njenega političnega prepričanja, če to prepričanje v zaprošeni državi ni opredeljeno kot kaznivo, ali pri pregonu osebe, ki je splavila, če ta oseba prebiva v drugi državi, kjer to ni kaznivo. Načelo dvojne kaznivosti pogosto spremljajo tudi dodatne omejitve ali zaščitni ukrepi v zvezi s sankcijami, če se te med državo, ki predloži zahtevo, in državo izvršiteljico preveč razlikujejo. Glavni primer je zaveza v nekaterih pogodbah o medsebojni pravni pomoči glede neuporabe smrtne kazni, kadar ta v pravu ene od obeh pogodbenic ne obstaja.

EOVP opozarja, da je načelo dvojne kaznivosti izključeno iz predloga uredbe o e-dokazih. Vendar zaradi tega niso črtane le običajne formalnosti vzajemnega priznavanja, ampak tudi zaščitni ukrepi, povezani s samim načelom dvojne kaznivosti.

EOVP opozarja, da predlog dejansko ne vsebuje nobenega sklicevanja na pravo države, v kateri ima zaprošeni ponudnik storitev poslovno enoto, in da se lahko nalog za zavarovanje katerih koli podatkov,

[7] Člen 5(1)(c) SUVP.
[8] Člen 13(3) in (4) direktive o EPN.
[9] Člen 5(1)(a) SUVP.

pa tudi predložitev podatkov o naročnikih ali dostopu, izda za vsa kazniva dejanja[10], ne glede na to, ali so v drugih državah članicah podobna kazniva dejanja določena ali ne.

Nalog za predložitev se lahko izda in izvrši le, če je v primerljivih nacionalnih primerih v državi izdajateljici za enako kaznivo dejanje na voljo podoben ukrep[11]. Poleg tega je, kot je Komisija pojasnila v obrazložitvenem memorandumu predloga uredbe, določena specifičnost podatkov o transakcijah in vsebini, saj se štejejo za občutljivejše podatke. Dejansko za naloge, ki se nanašajo na podatke o transakcijah ali vsebini, velja prag najvišje zagrožene zaporne kazni vsaj tri leta, da se zagotovi upoštevanje sorazmernosti in pravic prizadetih oseb[12]. Vendar EOVP poudarja, da v EU še niso bila usklajena kazniva dejanja, ki se kaznujejo z najvišjo zagroženo zaporno kaznijo vsaj treh let.

EOVP nasprotuje opustitvi načela dvojne kaznivosti, katerega namen je zagotoviti, da se država ne more zanašati na pomoč drugih, tj. da bo druga država, ki nima enakega pristopa, izvrševala njeno nacionalno kazensko pravo zunaj njenega ozemlja, zlasti glede na črtanje drugih tradicionalnih pomembnih zaščitnih ukrepov na področju kazenskega prava (glej v nadaljevanju točko 3 o merilih glede lokacije in točko 7(g) o morebitnih kolizijah z zakoni tretjih držav).

c) Posledica neposrednega naslavljanja družb

EOVP priznava, da je vse več e-dokazov na voljo na zasebni infrastrukturi in da so lahko zunaj preiskovalne države ter v lasti ponudnikov storitev.

EOVP opozarja, da je treba po sodnih odločbah v zadevah Yahoo![13] in Skype[14] v Belgiji ter zaradi terorističnih napadov zagotoviti bolj nemoteno in hitrejše sodelovanje med javnimi in zasebnimi subjekti. Komisija v oceni učinka navaja tri vrste postopkovnih instrumentov, ki vključujejo javne organe in ponudnike storitev. To so pravosodno sodelovanje, neposredno sodelovanje in neposredni dostop. Če pravosodno sodelovanje odgovornosti za izvršitev EPN ne nalaga ponudniku storitev, ampak izvršitvenemu organu[15], drugo, neposredno sodelovanje, temelji na sodelovanju ponudnika storitev. Najbolj vsiljiv z vidika ponudnika storitev je neposredni dostop, saj lahko javni organi do podatkov dostopajo brez pomoči posrednika.

Zato se EOVP boji, da ponudniki storitev, ki bodo naslovljeni neposredno, varstva osebnih podatkov ne bodo zagotovili tako učinkovito, kot to lahko in morajo javni organi, in poudarja, da zaradi tega ne bodo uporabljena nekatera postopkovna jamstva, ki so v okviru pravosodnega sodelovanja predvidena za fizične osebe, pa tudi same družbe[16]. Dejansko bi moral na primer zaprošeni ponudnik storitev za izpodbijanje naloga nastopiti pred sodiščem druge države (članice), v okviru pravosodnega sodelovanja pa bi se soočil z organi svoje države. EOVP priporoča, naj se v predlog uredbe vključijo dodatni razlogi, s katerimi bo zagotovljeno, da bodo ponudniki storitev varovali posamezne temeljne pravice, kot so

[10] Člen 5(3) in člen 6(2) predlagane uredbe o e-dokazih.
[11] Člen 5(2) predlagane uredbe o e-dokazih.
[12] Člen 5(4)(a) predlagane uredbe o e-dokazih.
[13] Hof van Cassatie, Belgija, YAHOO! Inc., št. P.13.2082.N z dne 1. decembra 2015.
[14] Correctionele Rechtbank van Antwerpen, afdeling Mechelen, Belgija, št. ME20.F1.105151-12 z dne 27. oktobra 2016 (družba Skype se je zoper odločbo pritožila).
[15] Členi od 10 do 16 direktive o EPN.
[16] Z vidika mednarodnega varstva podatkov glej tudi „Working paper on Standards for data protection and personal privacy in cross-border data requests for criminal law enforcement purposes“ (Delovni dokument o standardih za varstvo podatkov in zasebnost posameznikov v čezmejnih zahtevah po podatkih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj), Mednarodna delovna skupina za varstvo podatkov v telekomunikacijah, 63. seja, 9. in 10. april 2018, Budimpešta (Madžarska).

varstvo osebnih podatkov ter spoštovanje zasebnega in družinskega življenja, pa tudi informacije pristojnega organa za varstvo podatkov, da se zagotovi, da je mogoč nadzor.

3. Novi razlog za pristojnost in t. i. črtanje meril glede lokacije

EOVP ugotavlja, da Komisija kot eno od pomembnih sprememb, ki jih prinašata ta predloga, poudarja črtanje meril glede lokacije in možnost, da pristojni organi zahtevajo zavarovanje in predložitev podatkov ne glede na to, kje so ti podatki dejansko shranjeni.

Z vidika varstva podatkov ni novost, da pravo EU na področju varstva podatkov velja ne glede na to, kje so podatki zadevnih oseb shranjeni. Dejansko je uporaba SUVP odvisna od tega, ali ima upravljavec ali obdelovalec poslovno enoto v EU, ali pa od tega, ali se podatki posameznika iz EU, na katerega se nanašajo osebni podatki, obdelujejo tudi, kadar upravljavec ali obdelovalec nima poslovne enote na ozemlju EU[17], v tem primeru pa mora tudi imenovati pravnega zastopnika v EU[18]. Z vidika varstva podatkov je treba opozoriti, da je namen razširjene ozemeljske veljavnosti zagotoviti popolnejše varstvo posameznikom iz EU, na katere se nanašajo osebni podatki, ne glede na to, kje ima poslovno enoto družba, ki obdeluje njihove podatke.

Črtanje meril glede lokacije je morda novo na področju kazenskega prava, vendar se to z vidika varstva podatkov ne zdi pomembna sprememba. Poleg tega EOVP opozarja tudi, da je še vedno ohranjena povezava z ozemljem EU, saj na področje uporabe predlogov spadajo le ponudniki storitev, ki ponujajo storitve v Uniji, povezavo z EU pa pomeni tudi dejstvo, da se lahko zahteve naslovijo le v okviru kazenskih preiskav (ker je bilo kaznivo dejanje storjeno na ozemlju države članice ali pa ker je bila žrtev ali storilec kaznivega dejanja državljan države članice).

Če naj bi se črtanje meril glede lokacije zdaj uporabljalo v kazenskem pravu, se po mnenju EOVP najpomembnejše vprašanje nanaša na to, kako zagotoviti, da tak razvoj ne škoduje pravici do varstva podatkov in postopkovnim pravicam v kazenskem postopku, ki jih imajo posamezniki, na katere se nanašajo osebni podatki, in zaprošeni ponudniki storitev. EOVP s tega vidika priznava, da so v EU postopkovni zaščitni ukrepi vsaj delno usklajeni in jih je treba zagotavljati v skladu z Evropsko konvencijo o človekovih pravicah. Zato je mogoče trditi, da bi imelo črtanje meril glede lokacije verjetno bolj omejene posledice, kadar se dokazi zahtevajo znotraj EU, kot pa v obratnem primeru, ko organi iz tretjih držav podatke od družb s poslovno enoto v EU zahtevajo pod enakimi pogoji, kot so določeni v osnutku uredbe o e-dokazih. Dejansko EOVP z zaskrbljenostjo ugotavlja zlasti, da bi to lahko vodilo v bolj problematične situacije. V takem primeru bi lahko imeli organi iz tretje države, v kateri se na področju kazenskega prava uporabljajo drugačni postopkovni zaščitni ukrepi ali morda manj teh ukrepov, dostop do podatkov, ki bi bili v EU zaščiteni z dodatnimi zaščitnimi ukrepi. EOVP s tega vidika znova izraža svoje pomisleke glede dvojnega standarda in oslabitve temeljnih pravic, kadar ponudniki storitev in posamezniki, na katere se nanašajo osebni podatki, ne morejo izkoristiti postopkovnih jamstev v pravu EU, če zahtevo pošlje organ tretje države.

Ker je poleg tega ta novi razlog za pristojnost „ne glede na lokacijo podatkov“ združen s postopkom, ki temelji zlasti na neposrednih zahtevah, ki jih pristojni organi pošljejo ponudnikom storitev, EOVP skrbi, da zasebne družbe, ki prejmejo zahteve in jih ne zavezuje pravni instrument, kot je pogodba o medsebojni pravni pomoči, s katero se običajno ureja izmenjava podatkov med pravosodnimi organi in zagotavljajo zaščitni ukrepi, morda ne bodo uporabljale zaščitnih ukrepov za varstvo podatkov.

[17] Glej člen 3 Splošne uredbe o varstvu podatkov, zlasti odstavek 2.
[18] Glej člen 27 Splošne uredbe o varstvu podatkov.

Minimalni zaščitni ukrepi za varstvo podatkov v okviru pogodb o medsebojni pravni pomoči zlasti pomenijo na primer obveznosti glede zaupnosti in načelo specifičnosti, v skladu s katerim se podatki ne bodo obdelovali v druge namene.

EOVP zato opozarja, da bi bilo treba uporabljati vsaj zaščitne ukrepe iz Direktive 2016/680, tudi kar zadeva prenose podatkov, in zlasti člen 39 v primeru, kadar bi imel ponudnik storitev sedež v tretji državi brez sklepa o ustreznosti na tem področju. EOVP poudarja zlasti, da ta določba pomeni predvsem informacije pristojnega organa za varstvo podatkov v državi članici organa izdajatelja naloga ali nalogov in dokumentacijo o prenosu, tudi kar zadeva utemeljitev neučinkovitosti ali neprimernosti prenosa pristojnemu organu tretje države.

4. Pojem „ponudniki storitev“ bi moral biti omejen ali dopolnjen z dodatnimi zaščitnimi ukrepi za pravice posameznikov, na katere se nanašajo osebni podatki

Kar zadeva ponudnike storitev, EOVP pozdravlja široko opredelitev, ki omogoča vključitev tako komunikacijskih storitev kot povrhnjih storitev (OTT), saj so vse te storitve funkcionalno enakovredne in bi zato lahko predvideni ukrepi podobno vplivali na pravico do zasebnosti in pravico do zaupnih komunikacij, kot je poudarjeno v izjavi Delovne skupine iz člena 29 in pred tem v Mnenju št. 1/2017 o predlogu uredbe o e-zasebnosti. Dejansko predlog uredbe o e-dokazih zajema ponudnike storitev, ki ponujajo elektronske komunikacijske storitve, kakor so opredeljene v členu 2(4) direktive o Evropskem zakoniku o elektronskih komunikacijah, storitve informacijske družbe, kakor so opredeljene v členu 1(1)(b) Direktive (EU) 2015/1535 Evropskega parlamenta in Sveta, „pri katerih je shranjevanje podatkov odločilni element storitve, ki se zagotavlja uporabniku, vključno z družbenimi omrežji, spletnimi tržnicami, ki olajšajo transakcije med svojimi uporabniki, in drugimi ponudniki storitev gostovanja“, ali storitve dodeljevanja internetnih domenskih imen in številk IP, „kot so ponudniki naslovov IP, registri domenskih imen, registratorji domenskih imen ter povezane zasebne in posredniške storitve“[19].

Vendar ponudnik storitev v smislu osnutka uredbe pomeni „vsako fizično ali pravno osebo, ki zagotavlja eno ali več naslednjih kategorij storitev“, zato EOVP skrbi, da bi lahko ta instrument zajemal tako upravljavce kot obdelovalce v smislu SUVP. Ker „ponujanje storitev“, kot je opredeljeno v členu 2(4) osnutka uredbe, dejansko vključuje omogočanje pravnim ali fizičnim osebam v eni ali več državah članicah, da uporabijo navedene storitve, in obstoj pomembne povezave z zadevno državo članico ali zadevnimi državami članicami, te dejavnosti vključujejo dejavnosti, ki jih obdelovalec izvaja za upravljavca, kot je shranjevanje podatkov.

Zato se EOVP boji, da se brez omejitev za ponudnike storitev, ki delujejo kot upravljavci v smislu SUVP, in brez kakršne koli posebne obveznosti za obdelovalca, da mora, kadar je nanj naslovljen nalog za predložitev ali zavarovanje podatkov, o tem obvestiti upravljavca podatkov, pravice posameznikov, na katere se nanašajo osebni podatki, morda ne bi upoštevale. To velja zlasti, ker so v primeru morebitnih nasprotujočih si obveznosti, ki naslovniku preprečujejo izpolnitev prejetih nalogov, v samem osnutku uredbe pravosodni organi spodbujeni tudi, naj nalog naslovijo na najustreznejšega akterja ne glede na

[19] Člen 2(3)(c) predlagane uredbe o e-dokazih.

veljavna pravila o varstvu podatkov, zlasti glede na to, da se lahko zahtevajo kateri koli podatki, ne le osebni podatki, za katere se uporablja SUVP[20].

V skladu s SUVP obdelovalec podatke obdela le, če prejme taka navodila od upravljavca. Zato je upravljavec tisti, ki mora zagotoviti spoštovanje pravic posameznikov, na katere se nanašajo osebni podatki, in jim zagotoviti ustrezne informacije, tudi glede prejemnikov njihovih podatkov, na primer v okviru izvajanja njihove pravice do dostopa. Obdelovalec teh zahtev ne bo prejel od posameznikov, na katere se nanašajo osebni podatki, in nanje ne bo mogel odgovoriti, razen če bo to od njega izrecno zahteval upravljavec.

Zato EOVP poudarja, da posamezniki, na katere se nanašajo osebni podatki in ki imajo korist od uporabe SUVP, razen če so njihove pravice omejene pri uporabi navedene splošne uredbe, morda ne bodo mogli učinkovito uveljavljati svojih pravic, če upravljavec ne bo mogel predložiti popolnih informacij. EOVP opozarja tudi, da je verjetnost odsotnosti informacij še večja, če obdelovalcu ni naložena nobena posebna obveznost, da mora obvestiti upravljavca, kadar se zahtevani podatki nanašajo na posameznike, ki nimajo koristi od zaščite, dodeljene s SUVP. Dejansko za pravosodne organe, ki bodo zahtevali podatke, v tem primeru ne bo nujno veljalo, da morajo posameznike, na katere se nanašajo osebni podatki, obvestiti, da bodo nadalje obdelovali njihove podatke. EOVP zato poziva k omejitvi področja uporabe na upravljavce v smislu SUVP ali uvedbi določbe, v kateri je pojasnjeno, da kadar ponudnik storitev, ki je naslovnik, ni upravljavec podatkov, o tem obvesti upravljavca.

5. Pojma „poslovna enota“ in „pravni zastopnik“ v okviru teh predlogov bi bilo treba jasno razlikovati od teh pojmov v okviru SUVP

Zaradi neuporabe meril glede lokacije, kar zadeva podatke, so naslovniki nalogov za predložitev in zavarovanje dokazov, ki spadajo na področje uporabe predlagane uredbe, omejeni na ponudnike storitev, ki ponujajo storitve v Uniji, ne glede na to, ali imajo v EU poslovno enoto ali ne, in za katere velja obveznost imenovanja pravnega zastopnika v skladu s pravili, predlaganimi v osnutku direktive. Ta pojma „poslovna enota“ in „pravni zastopnik“ sta torej opredeljena v osnutkih instrumentov.

EOVP opozarja, da se ta pojma pojavljata tudi v okviru drugih instrumentov EU in zlasti v okviru SUVP. Zato bi bilo treba pojasniti opredelitev in zagotoviti razmejitev teh pojmov v okviru osnutkov predlogov in v okviru SUVP.

a) Poslovna enota

EOVP opozarja tudi, da se pojem „poslovna enota“ v okviru osnutka uredbe ne sme zamenjati s tem pojmom v okviru SUVP. Dejansko je pojem „poslovna enota“ za namene osnutka uredbe, kakor je opredeljen v njegovem členu 2(5), širši kot v splošni uredbi o varstvu podatkov, saj vključuje „dejansko izvajanje gospodarske dejavnosti za nedoločen čas prek stalne infrastrukture, od koder se dejavnost opravljanja storitev izvaja, ali stalne infrastrukture, od koder se dejavnost upravlja“, ne glede na to, ali se v okviru dejavnosti te poslovne enote osebni podatki obdelujejo ali ne. Če bi bila torej „ustanovitev“

[20] Glej člen 7(3) in (4) predloga uredbe o e-dokazih.

v smislu splošne uredbe o varstvu podatkov nedvomno vključena v „poslovno enoto“, opredeljeno v osnutku uredbe, nasprotno morda ne bi veljalo.

EOVP zato opozarja, da poslovne enote ponudnikov storitev v smislu osnutka uredbe morda ne pomenijo nujno, da so izpolnjeni pogoji za uporabo SUVP v skladu z njenim členom 3(1). Zato so v zvezi s tem upravljavci in obdelovalci pozvani, naj preverijo, ali uporaba splošne uredbe o varstvu podatkov morda ne izhaja iz člena 3(2), kar bi pomenilo imenovanje pravnega zastopnika v EU in odsotnost mehanizma enotne kontaktne točke.

b) Pravni zastopnik

Delovna skupina iz člena 29 je v izjavi poudarila, da bi se bilo treba izogniti vsakršni zamenjavi obveznosti imenovanja predstavnika na podlagi člena 27 SUVP in obveznosti imenovanja pravnega zastopnika, predvideni na podlagi osnutka uredbe o e-dokazih.

Glede zadevnega osnutka predloga želi EOVP znova opozoriti na ta priporočila in zlasti poudariti, da se v skladu z njegovim razumevanjem pravni zastopnik v smislu osnutka direktive o imenovanju pravnega zastopnika v okviru predlogov o e-dokazih imenuje v vsakem primeru, ima posebne naloge, neodvisno od mandata, ki mu ga podeli ponudnik storitev, je pooblaščen za odgovarjanje na zahteve in delovanje v imenu ponudnika storitev ter ima večjo odgovornost od predstavnika iz SUVP.

Poleg tega EOVP poudarja, da se obveznost imenovanja pravnega zastopnika na podlagi osnutkov predlogov o e-dokazih v vsakem primeru, ne glede na to, ali ima ponudnik storitev poslovno enoto v EU ali ne, možnost imenovanja tudi več pravnih zastopnikov za istega ponudnika storitev na podlagi osnutka direktive o e-dokazih in obveznost, da se o imenovanju pravnega zastopnika obvestijo organi države članice, razlikujejo od SUVP, ki ne določa take obveznosti obveščanja o imenovanem pravnem zastopniku, izjem od imenovanja in omejenih odgovornosti pravnega zastopnika.

Zato EOVP ob upoštevanju pomembnih razlik glede vloge, odgovornosti in povezave z drugimi poslovnimi enotami ponudnika storitev v enem primeru ter upravljavca ali obdelovalca v drugem primeru priporoča, da bi bilo treba v primeru, kadar ponudnik storitev nima poslovne enote v EU, vendar zanj veljata SUVP v skladu z njenim členom 3(2) in uredba o e-dokazih, imenovati tako predstavnika kot pravnega zastopnika, vsakega z jasno ločenimi funkcijami v skladu z instrumentom, na podlagi katerega je imenovan.

6. Nove kategorije podatkov

V predlagani uredbi so v členu 2 opredeljene različne kategorije podatkov: podatki o naročnikih, podatki o dostopu, podatki o transakcijah in podatki o vsebini. V recitalu 20 predloga Komisije je nadalje določeno, da „[k]ategorije podatkov, ki jih zajema ta uredba, vključujejo podatke o naročnikih, dostopu in transakcijah (tri kategorije, ki so skupno imenovane ‚podatki, ki ne zajemajo vsebine‘) ter podatke o vsebini. To razlikovanje, razen podatkov o dostopu, obstaja v pravnih redih številnih držav članic in tudi v trenutnem pravnem okviru ZDA, ki ponudnikom storitev omogoča prostovoljno izmenjavo podatkov, ki ne zajemajo vsebine, s tujimi organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj.“

V zvezi s tem EOVP najprej poudarja, da je treba v skladu s pravom EU na področju varstva podatkov za osebne podatke šteti vse zgoraj navedene štiri kategorije podatkov, saj vsebujejo informacije, ki se nanašajo na določeno ali določljivo fizično osebo, in sicer ne glede na to, ali se posameznik, na katerega

se nanašajo osebni podatki, v predlagani uredbi imenuje „naročnik“ ali „uporabnik“. Podobno je treba opozoriti, da pojem „elektronski dokazi“, kakor je opredeljen v členu 2(6) predloga Komisije, zajema vse štiri kategorije podatkov in se zato nanaša na osebne podatke. Zato predlagana uredba določa nove vsebinske in postopkovne pogoje v zvezi z dostopom do osebnih podatkov, namesto da bi določala pravila za dostop do dokazov, opredeljena in določena v skladu z nacionalnim pravom in pravosodnimi postopki.

Medtem ko predlagana uredba določa nove podkategorije osebnih podatkov, za katere se uporabljajo različni postopkovni pogoji za dostop, EOVP opozarja, da v skladu z ustrezno sodno prakso Sodišča Evropske unije za obstoj poseganja v temeljno pravico do spoštovanja zasebnega življenja ni pomembno, ali so zadevni podatki o zasebnem življenju občutljivi, niti to, ali so bile zadevne osebe zaradi tega posega oškodovane ali ne.

Poleg tega EOVP opozarja, da je Sodišče Evropske unije v zvezi s „podatki, ki ne zajemajo vsebine“, ki zajemajo podatke o naročnikih, dostopu in transakcijah, kot pri predlogu Komisije, v sodbi v združenih zadevah C-203/15 in C-698/15, Tele*2 Sverige AB*, odločilo, da so metapodatki, kot so podatki o prometu in lokaciji, sredstva za ugotavljanje profila zadevnih oseb, kar so zelo občutljive informacije glede pravice do spoštovanja zasebnega življenja ter same vsebine komunikacij[21].

Kot je navedeno že v izjavi Delovne skupine iz člena 29 z naslovom „Data protection and privacy aspects of cross-border access to electronic evidence“ (Vidiki varstva podatkov in zasebnosti pri čezmejnem dostopu do elektronskih dokazov) z dne 29. novembra 2017, EOVP zato ponavlja pomisleke in zaskrbljenost glede trenutne razmejitve med „podatki, ki ne zajemajo vsebine“, in podatki o vsebini, pa tudi glede štirih kategorij osebnih podatkov, določenih v predlagani uredbi. Dejansko se za predlagane štiri kategorije zdi, da niso jasno razmejene, opredelitev „podatkov o dostopu“ pa je v primerjavi z drugimi kategorijami še vedno nejasna. EOVP zato obžaluje, da Komisija v oceni učinka in predlogu ni nadalje utemeljila razlogov za določitev teh novih podkategorij osebnih podatkov, in izraža pomisleke glede različnih ravni jamstva, povezanih z vsebinskimi in postopkovnimi pogoji za dostop do kategorij osebnih podatkov, zlasti zaradi praktičnih težav pri vrednotenju, v katero kategorijo podatkov bodo v nekaterih primerih spadali zahtevani podatki. Naslovi IP bi se lahko na primer razvrstili kot podatki o transakcijah in o naročniku.

EOVP v zvezi s tem opozarja tudi, da Komisija v recitalu 14 predloga uredbe o spoštovanju zasebnega življenja in varstvu osebnih podatkov na področju elektronskih komunikacij (uredba o e-zasebnosti) meni, da bi bilo treba „[e]lektronske komunikacijske podatke [...] opredeliti ustrezno široko in tehnološko nevtralno, da bi zajeli vse informacije, ki se nanašajo na preneseno ali izmenjano vsebino (vsebino elektronskih komunikacij) in informacije v zvezi s končnim uporabnikom storitev elektronskih komunikacij, ki se obdelajo za namene prenosa, razširjanja ali omogočanja izmenjave vsebine elektronskih komunikacij; vključno s podatki za sledenje in določitev vira in cilja komunikacije, geografske lokacije ter datuma, časa, trajanja in vrste komunikacije“. Ker se bodo veljavni in prihodnji okvir o e-zasebnosti, pa tudi povezane omejitve pravice do zasebnosti uporabljali za pravila, s katerimi se ureja dostop organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj do e-dokazov, EOVP priporoča, naj se v predlagano uredbo vključi širša opredelitev elektronskih komunikacijskih podatkov, da se zagotovi, da ustrezni zaščitni ukrepi in pogoji za dostop, ki bodo določeni, dosledno zajemajo „podatke, ki ne zajemajo vsebine“, in „podatke o vsebini“.

[21] Sodba Sodišča Evropske unije z dne 21. decembra 2016, točka 99.

7. Analiza postopkov za nalog za predložitev in nalog za zavarovanje dokazov

Na splošno se zdi, da je postopek za naslovitev naloga za predložitev ali zavarovanje dokazov tak, kot je opisan v nadaljevanju.

- Pristojni pravosodni organ – organ izdajatelj – odvisno od vrste zahtevanih podatkov in vrste naloga izda nalog v skladu z (malоštevilnimi) pogoji, navedenimi v členih 5 in 6, in ga prek usklajenega potrdila pošlje pravnemu zastopniku ponudnika storitev ali kateri koli njegovi poslovni enoti v EU – naslovniku.
- Naslovnik po prejetju potrdila izvrši nalog, kar pomeni, da pošlje podatke v desetih dneh ali šestih urah v nujnem primeru ali jih zavaruje za največ 60 dni, razen če tega ne more storiti, ker je potrdilo nepopolno, ali zaradi višje sile, ali ker je bilo to za naslovnika dejansko nemogoče storiti, ali ker naslovnik izvršitev zavrne zaradi nasprotujočih si obveznosti, ki se nanašajo na temeljne pravice ali temeljne interese tretje države, ali iz drugih razlogov.
- Če naslovnik ne izvrši prejetega naloga in za to ne navede razlogov, ki jih organ izdajatelj sprejme, so predvideni postopki, v skladu s katerimi naloge izvrši organ izvršitelj, pristojen v državi članici, kjer ima ponudnik storitev zastopnika ali poslovno enoto, razen če obstajajo omejeni razlogi za zavrnitev in organ izvršitelj nasprotuje priznanju ali izvršitvi naloga.
- Če je naslovnik podal obrazložen ugovor zoper nalog na podlagi nasprotujočih si obveznosti, organ izdajatelj zadevo predloži pristojnemu sodišču v svoji državi članici, to pa je nato pristojno za presojo o morebitnem nasprotovanju in potrditev naloga v primeru neobstoja nasprotovanja. Pristojno sodišče v primeru obstoja nasprotovanja stopi v stik z osrednjimi organi v tretji državi prek svojih nacionalnih osrednjih organov ter določi 15-dnevni rok za odgovor, ki se lahko na obrazloženo zahtevo podaljša za 30 dni v primeru nasprotujočih si obveznosti na podlagi temeljnih pravic ali temeljnih interesov tretje države, ali pa odloči o potrditvi ali umiku naloga na podlagi drugih razlogov za zavrnitev, na katere se sklicuje naslovnik.
- Brez poseganja v pravna sredstva, ki so na voljo na podlagi SUVP in direktive o preprečevanju, odkrivanju in preiskovanju kaznivih dejanj, imajo osebe, katerih podatki so bili pridobljeni na podlagi naloga za predložitev dokazov, tudi pravico do učinkovitega pravnega sredstva zoper ta nalog.

EOVP je ocenil postopke, predvidene v osnutku uredbe, in v njem zagotovljene zaščitne ukrepe, povezane z različnimi koraki, ter za vsak vidik, predstavljen v nadaljevanju, priporoča naslednje zaščitne ukrepe in spremembe.

a) Prage za izdajo nalogov bi bilo treba povišati, naloge pa naj izdajo ali odobrijo sodišča

Kar zadeva pogoje za izdajo nalogov, EOVP pozdravlja načelo višjih zaščitnih ukrepov za dostop do podatkov o transakcijah ali vsebini. Vendar opozarja, da glede na neusklajenost kazenskih sankcij med državami članicami sklicevanje na „kazniva dejanja, za katera je v državi izdajateljici najvišja zagrožena

zaporna kazen vsaj tri leta“[22], za posameznike, na katere se nanašajo osebni podatki, še vedno pomeni različne prage in neskladja pri varstvu njihovih podatkov v EU.

EOVP poleg tega poudarja, da se zdi določeni prag zlasti glede na široko opredelitev podatkov o naročnikih razmeroma nizek za naloge za zavarovanje in predložitev dokazov, ki se nanašajo na podatke o naročnikih ali dostopu, saj se lahko taki nalogi načeloma utemeljeno izdajo za vsa kazniva dejanja. Podobno so organi, ki lahko izdajo take naloge, bolj omejeni v okviru nalogov za predložitev dokazov, ki se nanašajo na podatke o transakcijah ali vsebini, kot pri izdaji nalogov za zavarovanje ali predložitev podatkov o naročnikih ali dostopu, saj lahko tožilec izda ali odobri le zadnje navedene naloge, vsak sodnik, sodišče ali preiskovalni sodnik pa lahko izda ali odobri kateri koli nalog.

EOVP obžaluje zlasti, da najnižji prag, ki organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj omogoča, da zahtevajo dostop do podatkov o naročnikih in dostopu za katero koli kaznivo dejanje, za razlikovanje med zaščitnimi ukrepi, ki jih je treba zagotoviti, temelji na sklepanju po nasprotnem razlogovanju na podlagi sodne prakse Sodišča Evropske unije (ki se osredotoča na druge podatke). Dejansko je Sodišče Evropske unije posebej poudarilo, da je dostop pristojnih organov do podatkov o prometu in lokaciji omejen izključno na boj proti hudim kaznivim dejanjem[23]. EOVP bi lahko razumel, da bi predlog zagotovil možnost zahtevanja dostopa do zelo osnovnih informacij, ki bi omogočile le identifikacijo osebe, ne bi pa razkrile nobenih komunikacijskih podatkov brez predhodne odobritve sodišča. Vendar obžaluje široko sklepanje Komisije po nasprotnem razlogovanju na podlagi te sodbe in poziva k uvedbi višjih zaščitnih ukrepov, da se omejijo razlogi za dostop do drugih podatkov o naročnikih in podatkov o dostopu. EOVP predlaga, naj se dostop do teh podatkov omeji na seznam kaznivih dejanj iz osnutka uredbe ali vsaj na „huda kazniva dejanja“, zlasti glede na nižji prag za predhodno odobritev, ki je predviden za te podatke.

EOVP poleg tega poudarja, da to sklepanje po nasprotnem razlogovanju vodi tudi v dejstvo, da predlog tožilcem omogoča izdajo ali odobritev izdaje nalogov. Po njegovem mnenju to razen v primerih zahtev v zvezi z zelo osnovnimi informacijami, ki bi omogočile le identifikacijo osebe, ne bi pa razkrile nobenih komunikacijskih podatkov, pomeni korak nazaj v primerjavi s sodno prakso Sodišča Evropske unije v zvezi z dostopom do komunikacijskih podatkov. Dejansko je Sodišče Evropske unije v sodni praksi, ki se nanaša na dostop do komunikacijskih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, možnost zagotovitve takega dostopa, med drugim in „*razen v nujnih primerih, ki so ustrezno utemeljeni*“[24], omejilo na predhodni nadzor, „*ki ga opravi sodišče ali neodvisen upravni subjekt*“ „*na podlagi obrazloženega predloga, ki ga [pristojni nacionalni organi] vložijo v postopkih preprečevanja, odkrivanja ali pregona kaznivih dejanj*“. [25]

EOVP opozarja, da je pojem „sodišče“ avtonomni pojem prava EU in da Sodišče Evropske unije stalno poudarja in opozarja na merila, ki morajo biti izpolnjena, da se organ šteje za sodišče, vključno z merilom neodvisnosti[26], kar pa očitno ne velja za tožilce, kot je v sodni praksi opozorilo tudi Evropsko sodišče za človekove pravice[27].

Zato se bo na podlagi člena 4(1)(a) in (b) ter 4(3)(a) in (b) predloga uredbe v postopkih za podatke o naročnikih in dostopu uporabljalo precej manj zaščitnih ukrepov, saj bo lahko podatke zahteval le tožilec, in sicer brez nadaljnjega nadzora s strani organa države, v kateri so zahtevani podatki, ali organa

[22] Glej člen 5(3)(a) predloga uredbe o e-dokazih.
[23] Glej zadevo C-203/15, točka 125.
[24] Glej zadevo C-203/15, točka 120.
[25] Glej združeni zadevi C-293/12 in C-594/12, točka 62.
[26] Glej na primer zadevo C-203/14.
[27] Glej na primer sodbo v zadevi Moulin proti Franciji z dne 23. novembra 2010.

države, v kateri bo pravni zastopnik družbe, od katere se bodo zahtevali podatki, ali nadzora s strani neodvisnega upravnega organa.

EOVP poleg tega opozarja na t. i. dodatni zaščitni ukrep iz člena 5(2) predloga uredbe, v skladu s katerim je izdaja naloga za predložitev mogoča le, če je v primerljivih nacionalnih primerih za enako kaznivo dejanje na voljo podoben ukrep. Vendar opozarja na nasprotni neželeni učinek take določbe: namesto da bi zagotovila dodatne zaščitne ukrepe, se zdi, da države članice spodbuja, naj razširijo svoje nacionalne možnosti za zahtevanje predložitve podatkov o naročnikih ali dostopu ter tako zagotovijo, da se nalogi za predložitev na podlagi te uredbe lahko izdajo.

b) Roki za predložitev podatkov bi morali biti utemeljeni

EOVP opozarja, da je treba na evropske naloge za predložitev dokazov odgovoriti najpozneje v desetih dneh po prejemu potrdila, razen če organ izdajatelj navede razloge za predčasno razkritje, in najpozneje v šestih urah v nujnih primerih, kot je določeno v členu 9(1) in (2).

Vendar EOVP ni ugotovil nobenih meril, na podlagi katerih bi morali organi dokazati nujnost predložitve podatkov, tudi naknadno, da bi se omogočil morebiten nadzor nad uporabo tega zelo hitrega postopka, medtem ko šesturni rok verjetno pomeni, da bo ponudnik storitev lahko izvedel zelo omejen nadzor pred predložitvijo podatkov ali pa ga sploh ne bo mogel izvesti. Dejansko je v oceni učinka poudarjena nujnost pravočasnega dostopa pristojnih organov do podatkov. Vendar se vsi primeri, navedeni v oceni učinka, nanašajo na dokaze, potrebne v primeru storitve hudih kaznivih dejanj (teroristična kazniva dejanja s talci, primeri spolne zlorabe otrok, ki se še dogaja), utemeljitev, ki temelji na minljivosti dokazov, pa se ne zdi dobra, kadar ni posebne nujnosti razen te morebitne minljivosti podatkov. Minljivost podatkov tudi ne zagotavlja dodatne utemeljitve glede sorazmernosti dostopa do podatkov z manj zaščitnimi ukrepi v teh primerih, kadar razen minljivosti podatkov ni druge nujnosti.

Poleg tega EOVP dvomi o potrebi po zagotovitvi šesturnega roka, ko je obenem določeno, da se ta rok ne uporablja, dokler organ izdajatelj ne zagotovi dodatnih pojasnil „v petih dneh“, če ponudnik storitev ne more izpolniti svoje obveznosti.

EOVP zato poziva, naj se v oceno učinka vključijo dodatni elementi za utemeljitev potrebe po teh rokih, kadar storjeno ali preganjano kaznivo dejanje ni hudo kaznivo dejanje, če so taki podrobni elementi že določeni, pa izrecna merila za utemeljitev nujnosti v primeru izdaje potrdil o evropskem nalogu za predložitev dokazov. Predviden bi lahko bil na primer enak model kot v direktivi o EPN. Direktiva o EPN določa krajši rok, kadar je to utemeljeno zaradi „postopkovnih rokov, teže kaznivega dejanja ali drugih zelo nujnih okoliščin“ (glej člen 12(2) direktive o EPN), ali 24-urni rok za sprejetje odločitve o začasnih ukrepih (glej člen 32(2) direktive o EPN). Dejansko ocena učinka osnutka uredbe ne vsebuje podrobnih elementov, s katerimi bi se utemeljilo, zakaj ti roki niso učinkoviti, saj je poudarjeno le, da so pravosodni organi prejemniki zaradi števila poslanih zahtev preobremenjeni in ne morejo upoštevati rokov.

c) Evropski nalog za predložitev in evropski nalog za zavarovanje e-dokazov se ne uporabljata za zahtevanje podatkov o posamezniku iz druge države članice, na katerega se nanašajo podatki, ne da bi bili o tem vsaj obveščeni pristojni organi navedene države članice, zlasti v primeru podatkov o vsebini

EOVP opozarja, da je v veljavnih instrumentih zagotovljeno pravosodno sodelovanje in s tem dodatni zaščitni ukrepi, zlasti za nadzor nad nujnostjo in sorazmernostjo zahtev, ter poudarja, da so ti zaščitni ukrepi toliko bolj utemeljeni, kadar se zahtevajo podatki o vsebini, ki vključujejo več omejitev pravic

posameznikov, na katere se osebni podatki nanašajo, do zaščite njihovih osebnih podatkov in zasebnosti. V zvezi s tem EOVP opozarja, da direktiva o EPN zagotavlja tudi možnost prestrezanja telekomunikacij s tehnično pomočjo druge države članice (glej člen 30 direktive o EPN) in določa obveznost, da se v primerih, kadar pomoč ni potrebna, o vsakem prestrezanju podatkov uradno obvesti pristojni organ druge države članice, kadar zadevni posameznik, na katerega se podatki nanašajo, je ali bo na ozemlju navedene države članice (glej člen 31 direktive o EPN).

Po mnenju EOVP je postopek, ki je predviden v osnutku uredbe o e-dokazih, tj. da se omogoči predložitev podatkov o vsebini brez kakršne koli vključitve vsaj pristojnih organov države članice, v kateri je posameznik, na katerega se nanašajo osebni podatki, popolnoma neutemeljen.

d) Evropski nalogi za zavarovanje e-dokazov se ne uporabijo za izogibanje obveznostim ponudnikov storitev glede hrambe podatkov

EOVP ugotavlja, da je glavni namen evropskih nalogov za zavarovanje e-dokazov preprečiti izbris podatkov.

Čeprav EOVP priznava, da je to v nekaterih primerih morda nujno in sorazmerno, obžaluje pomanjkanje zaščitnih ukrepov, povezanih z izdajo takih nalogov. Zlasti priporoča, da nalog za zavarovanje dokazov, kadar taki nalogi zajemajo le določene podatke, kadar se za osnutek zdi, da omogoča široke zahteve, in se taki nalogi izdajo za podatke, za katere je načrtovan izbris v skladu z načelom hrambe podatkov, ponudniku storitev nikoli ne služi kot podlaga za obdelavo podatkov po prvotnem datumu za izbris. Povedano drugače, podatki bi morali biti „zamrznjeni“.

Poleg tega bi bilo treba okrepiti povezavo med nalogom za zavarovanje in naknadno zahtevo po predložitvi podatkov, in sicer prek evropskega naloga za predložitev e-dokazov, zahteve na podlagi EPN ali zahteve za medsebojno pravno pomoč, da bi se zagotovilo, da se evropski nalogi za zavarovanje e-dokazov izdajo le, kadar je druga zahteva nesporna (in ne le predvidena kot možnost), in da se ob zavrnitvi druge zahteve izteče tudi nalog za zavarovanje dokazov, ne da bi bilo treba čakati 60 dni[28], če je naknadna zahteva zavrnjena prej.

e) Zaupnost in podatki o uporabnikih

EOVP ugotavlja, da je v osnutek uredbe uveden poseben člen[29] v zvezi z zaupnostjo naslovljenih nalogov. Da bi se preprečili zamenjava s pravico do varstva podatkov in napačno razumevanje, EOVP opozarja, da splošna uredba o varstvu podatkov sicer določa, da bi morale biti omejitve pravic posameznikov, na katere se nanašajo osebni podatki, zaradi zaščite preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj določene z zakonom in s tem javno dostopne[30] ter da ti zakonodajni ukrepi vsebujejo posebne določbe glede pravice posameznikov, na katere se nanašajo osebni podatki, da so obveščeni o omejitvi, razen če bi to posegalo v namen omejitve[31], vendar ne določa obveznosti, da je treba posameznike, na katere se nanašajo osebni podatki, posebej obvestiti o vsaki zahtevi za dostop, ki jo podajo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj.

Vendar EOVP opozarja tudi, da direktiva o varstvu podatkov to pravico posameznikov, na katere se nanašajo osebni podatki, da jih obvestijo sami pristojni organi, razen če je bila ta pravica omejena,

[28] Glej člen 10(1) predloga uredbe o e-dokazih.
[29] Glej člen 11 predloga uredbe o e-dokazih.
[30] Glej člen 23(1)(d) Splošne uredbe o varstvu podatkov.
[31] Glej člen 23(2)(h) Splošne uredbe o varstvu podatkov.

zagotavlja vsem posameznikom, na katere se nanašajo osebni podatki, in je ne omejuje le na navedene posameznike, ki prebivajo na ozemlju EU.

f) Postopek za izvršitev naloga, kadar ponudnik storitev zavrne njegovo izvršitev

EOVP ugotavlja, da je v členu 14 osnutka uredbe določen postopek za zagotovitev izvršitve naloga, kadar ga naslovnik ne upošteva, opira pa se na pravosodno sodelovanje med organom izdajateljem in pristojnim organom v državi izvršiteljici.

Vendar se zdi, da lahko organ izvršitelj v skladu s tem postopkom izvršitev poslanega naloga zavrne le iz strogo postopkovnih razlogov (ki se tako kot pri naslovniku nanašajo zlasti na pomanjkanje informacij ali dejansko nezmožnost predložitve podatkov), ker so zadevni podatki zaščiteni z imuniteto ali privilegijem na podlagi njegovega nacionalnega prava ali ker bi lahko njihovo razkritje vplivalo na temeljne interese, kot sta nacionalna varnost in obramba[32].

EOVP zato ponavlja svoje pomisleke glede odprave kakršnega koli dvojnega preverjanja poslanega naloga, ki ga izvede pristojni organ prejemnik, v primerjavi z drugimi instrumenti. Tudi razlog, da se zavrne izvršitev naloga, ker bi se s tem kršila Listina, se zdi strožji od klasičnega praga, povezanega s kršitvijo temeljnih pravic zadevne osebe. Zato bi moralo biti v osnutku uredbe po zgledu evropskega naloga za prijetje, ki določa obvezne in neobvezne razloge za zavrnitev, ali vsaj direktive o EPN, ki na splošno določa, da se lahko domneva, v skladu s katero „[v]zpostavitev območja svobode, varnosti in pravice v Uniji temelji na medsebojnem zaupanju in domnevi, da druge države članice spoštujejo pravo Unije in zlasti temeljne pravice“, izpodbija[33], predvideno vsaj minimalno običajno odstopanje, da bi bilo treba izvršitev naloga zavrniti, če je mogoče utemeljeno domnevati, da bodo z izvršitvijo naloga kršene temeljne pravice zadevnega posameznika in da država izvršiteljica ne bo upoštevala svojih obveznosti glede varstva temeljnih pravic, priznanih v Listini.

g) Izvršitev nalogov in nasprotujoče si obveznosti na podlagi prava tretje države (člena 15 in 16)

EOVP pozdravlja možnost iz osnutka uredbe, da lahko naslovniki zavrnejo nalog, ker bi bil v nasprotju s temeljnimi pravicami, saj je namenjena zagotavljanju zaščitnih ukrepov v primeru nasprotujočih si pravnih obveznosti. Po njegovem mnenju je bistveno tudi, da je v predlogu zagotovljeno posvetovanje z organi tretjih držav, vsaj kadar pride do nasprotovanja, in tudi obveznost, da se nalog umakne, če mu organ tretje države ugovarja.

Zato bi bilo treba precej izboljšati postopek, predviden za zavrnitev izvršitve naloga zaradi nasprotujočih si obveznosti na podlagi prava tretje države.

EOVP najprej ugotavlja, da je v skladu z osnutkom uredbe za oceno, ali bi bil nalog za predložitev dokazov v nasprotju s pravom tretje države, ki se uporablja in ki prepoveduje razkritje zadevnih podatkov, pooblaščena zasebna družba kot naslovnik navedenega naloga. Družba mora predložiti obrazložen ugovor, ki vsebuje vse zadevne podrobnosti o pravu tretje države, njegovi upoštevnosti v zadevi in naravi nasprotujoče obveznosti.

EOVP je predvsem zaskrbljen, da v primeru vložitve takega ugovora pristojno sodišče države članice organa izdajatelja samo presodi, ali nasprotovanje obstaja ali ne, saj sodišče v stik z organi tretje države

[32] Glej člen 14(2) predloga uredbe o e-dokazih.
[33] Glej uvodno izjavo 19 direktive o EPN.

stopi šele, če ugotovi, da nasprotovanje obstaja. Pristojnemu sodišču EU je torej podeljena pristojnost za dokončno razlago prava tretje države v zvezi s tem, čeprav niti ni dobro strokovno seznanjeno z njegovo vsebino. EOVP meni, da je obveznost posvetovanja s pristojnimi organi tretje države v sedanjem predlogu zato preveč omejena. Na področju varstva podatkov zakonodajalca opozarja na dejstvo, da bi bili v primeru, ko bi pristojno sodišče tretje države razlagalo SUVP, da bi ocenilo, ali je v nasprotju z njegovimi lastnimi zahtevami, organi EU za varstvo podatkov in pristojna sodišča še vedno pristojni za oceno zakonitosti prenosa na podlagi sodbe sodišča ali odločbe upravnega organa tretje države, ki zahteva prenos ali razkritje osebnih podatkov, ki spadajo na področje uporabe SUVP[34].

EOVP poleg tega poudarja, da mora presoja prava tretje države, ki jo izvede pristojno sodišče države EU, ki predloži zahtevo, temeljiti na objektivnih elementih, ter je zaskrbljeno zaradi meril, ki jih mora pristojno sodišče upoštevati pri presoji prava tretje države na podlagi člena 15(4) in člena 16(5)(a) osnutka uredbe. Dejansko bi moralo Sodišče presojati o dejstvu, da je namen prava tretje države namesto „zaščititi druge interese in ne temeljnih pravic posameznikov ali temeljnih interesov tretje države, ki se nanašajo na nacionalno varnost ali obrambo“, „zaščititi nezakonite dejavnosti pred zahtevami organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj v okviru kazenskih preiskav“ ali „interes[e], ki jih ščiti zadevno pravo tretje države, vključno z interesom tretje države glede preprečevanja razkritja podatkov.“ Čeprav bi bilo na primer treba zaradi morebitnega učinka take odločitve načeloma pri tej presoji izvesti oceno na podlagi dokazov ob upoštevanju vseh razpoložljivih informacij, se vsaj besedilo („je njegov namen“) zdi nejasno in bi ga bilo treba spremeniti („je njegov cilj“).

EOVP obžaluje, da bi bil edini primer, v katerem bi se z organi tretje države posvetovalo in bi ti lahko nasprotovali izvršitvi naloga za predložitev dokazov, kadar bi to pristojno sodišče EU menilo, da obstaja pomembno nasprotovanje, in bi poslalo vse elemente osrednjim organom v zadevni tretji državi, osrednji organ navedene tretje države pa bi lahko ugovarjal v kratkih rokih, ki bi skupaj trajali največ 50 dni (15 dni, ki se lahko podaljša za 30 dni, in še dodatnih pet dni po zadnjem možnem opomniku). V vseh drugih primerih bi lahko pristojno sodišče potrdilo nalog za predložitev dokazov in naložilo denarno kazen ponudniku storitev, ki zavrača izvršitev naloga. Zato je EOVP zaskrbljen, da pristojna sodišča EU ne bodo imela širše obveznosti posvetovanja s pristojnimi organi zadevnih tretjih držav, s katero bi se zagotovilo, da se bo pri postopku bolj sistematično zagotavljalo upoštevanje argumentov obeh strani in da se bo pravo tretjih držav še bolj spoštovalo.

Kot je že poudarjeno v izjavi Delovne skupine iz člena 29 in zgoraj, EOVP ponovno poudarja, da bi bilo treba posebno pozornost nameniti sprejetju podobnih instrumentov s strani tretjih držav, ki bi lahko vplivali na pravice posameznikov, na katere se nanašajo osebni podatki, in njihovo pravico do zasebnosti v EU, zlasti tveganju, da sprejmejo podobne instrumente, ki bi neposredno nasprotovali pravu EU na področju varstva podatkov.

EOVP poleg tega poudarja, da pristojno sodišče države članice organa izdajatelja morda niti ni sodišče, pristojno za izvršitev naloga, predvideno v členu 14 osnutka uredbe, kar bi še povečalo tveganje nasprotujočih si postopkov in neobstoj nasprotnih preverjanj v primeru nasprotujočih si zakonov. To izhaja iz dejstva, da bi lahko bile v nekaterih primerih vključene tri države: država organa, ki izda nalog, tretja država ponudnika storitev in država članica, v kateri je pravni zastopnik ponudnika storitev v EU in kjer bi moral biti nalog izvršen. Zato bi lahko v skladu s trenutno predvidenim postopkom sodišče organa, ki predloži zahtevo, v državi članici A po svoje razlagalo pravo tretje države B ponudnika storitev, ne da bi zahtevalo mnenje organov te tretje države (ti pa bi ugovarjali nalogu), in od sodišča

[34] Glej člen 48 SUVP.

v drugi državi članici C zahtevalo izvršitev njegove odločitve, ne da bi to zadnje navedeno sodišče imelo možnost ugovora.

Poleg tega EOVP pozdravlja tudi uvedbo posebnih pravnih sredstev zoper naloge za predložitev dokazov poleg pravnih sredstev, ki so že zagotovljena s SUVP ter direktivo o preprečevanju, odkrivanju in preiskovanju kaznivih dejanj. Delovna skupina iz člena 29 je k uvedbi takih zaščitnih ukrepov pozvala že v prejšnji izjavi. EOVP pa obžaluje, da taka pravna sredstva niso predvidena tudi zoper naloge za zavarovanje dokazov, saj lahko tudi ti nalogi povzročijo omejitve temeljnih pravic posameznikov, katerih podatki so shranjeni. Dejansko lahko nalogi za zavarovanje dokazov privedejo do tega, da so podatki shranjeni dlje, kot bi bili v skladu s pravili o varstvu podatkov. Zato nalog za zavarovanje dokazov sam po sebi povzroči omejitev temeljnih pravic zadevnega posameznika, na katerega se nanašajo osebni podatki, za utemeljitev katere se opravi pregled, zanjo pa veljajo tudi posebna pravna sredstva, zlasti v primerih, ko se bo nalog za zavarovanje dokazov izdal skupaj z nalogom za predložitev dokazov, da bi se pridobili podatki. Kot je Delovna skupina iz člena 29 priporočila v izjavi, bi bilo treba predvideti pravna sredstva, ki so vsaj enakovredna tistim, ki so na voljo v nacionalnem primeru.

h) Varnost prenosa podatkov pri odzivanju na nalog

EOVP opozarja, da morajo biti v skladu z osnutkom uredbe nalogi naslovljeni le na prejemnike v Evropski uniji, zato v njej ni predviden poseben kanal za prenos podatkov med naslovniki in ponudniki storitev, ki so zunaj Evropske unije.

Čeprav EOVP pozdravlja dejstvo, da ni drugih odstopanj od splošnega okvira EU za varstvo podatkov, ponavlja, da bi bilo treba pri vsakem nalogu, poslanem naslovniku, pri katerem bi to pomenilo prenos v države zunaj EU, spoštovati pravni okvir, ki ga določa SUVP. Izogibanje pravnemu okviru pravosodnega sodelovanja, ki zagotavlja spoštovanje zaščitnih ukrepov za varstvo podatkov, dejansko ne bi smelo povzročiti tega, da bi se tudi naslovniki nalogov za predložitev ali zavarovanje dokazov izogibali zahtevam za prenos podatkov za izpolnitev takih nalogov.

Medtem ko EOVP pozdravlja neobstoj določbe, ki bi nalagala obveznost dešifriranja šifriranih podatkov[35], pa z zaskrbljenostjo ugotavlja tudi, da v osnutkih predlogov ni predvidena nobena posebna zahteva, da morajo naslovniki oceniti pristnost predloženih podatkov, poudarja, da je ta ocena tudi dodana vrednost tradicionalnih instrumentov, ki temeljijo na pravosodnem sodelovanju, in opozarja na povečana tveganja, ki jih neobstoj take ocene predstavlja za zadevne posameznike, na katere se nanašajo osebni podatki.

Sklepne ugotovitve

Evropski odbor za varstvo podatkov EOVP želi na podlagi te presoje na sozakonodajalca nasloviti priporočila, navedena v nadaljevanju.

1) Pravna podlaga uredbe ne bi smel biti člen 82(1) PDEU.
2) Bolje bi bilo treba dokazati potrebo po novem instrumentu v primerjavi z veljavno direktivo o EPN ali pogodbo o medsebojni pravni pomoči, tudi s podrobno analizo manj vsiljivih sredstev, kar zadeva temeljne pravice, kot so spremembe teh veljavnih instrumentov ali omejitev področja uporabe tega instrumenta na naloge za zavarovanje dokazov v kombinaciji z drugimi veljavnimi postopki za zahtevanje dostopa do podatkov.

[35] Glej uvodno izjavo 19 in stran 240 ocene učinka.

3) V uredbi bi moral biti predviden daljši rok, ki bi ponudniku storitev izvršitelju omogočil, da zagotovi spoštovanje zaščitnih ukrepov v zvezi z varstvom temeljnih pravic.
4) Načelo dvojne kaznivosti bi bilo treba ohraniti, zlasti če se opustijo merila glede lokacije podatkov, da bi se ohranila obveznost upoštevanja zaščitnih ukrepov, zagotovljenih v obeh zadevnih državah (državi organa, ki predloži zahtevo, in državi, v kateri je ponudnik storitev).
5) Področje uporabe uredbe bi bilo treba omejiti na upravljavce v smislu SUVP ali pa bi morala uredba vsebovati določbo, da mora ponudnik storitev, ki prejme zahtevo in ni upravljavec podatkov, ampak njihov obdelovalec, o tem obvestiti upravljavca.
6) Uredba bi morala vključevati zaščitne ukrepe v zvezi s prenosi podatkov v primeru, kadar bi imel ponudnik storitev poslovno enoto v tretji državi brez sklepa o ustreznosti na tem področju, ali sklicevanje na Direktivo 2016/680, ko se bodo ti zaščitni ukrepi začeli uporabljati.
7) Ker se obvezno imenovanje pravnega zastopnika razlikuje od SUVP, bi moralo biti v uredbi natančno opredeljeno, da bi moral biti pravni zastopnik, imenovan na podlagi uredbe o e-dokazih, drug kot predstavnik, imenovan na podlagi člena 3(2) SUVP.
8) Uredba bi morala vsebovati širšo opredelitev elektronskih komunikacijskih podatkov, da se zagotovi, da ustrezni zaščitni ukrepi in pogoji za dostop, ki se bodo določili, zajemajo podatke, ki ne zajemajo vsebine, in podatke o vsebini.
9) V uredbi bi morali biti določeni višji pragovi za izdajo nalogov, naloge pa izdajo ali odobrijo sodišča, razen nalogov za podatke o naročnikih, če se opredelitev te kategorije podatkov močno omeji na zelo osnovne informacije, ki omogočajo le identifikacijo osebe, ne vključujejo pa dostopa do nobenih komunikacijskih podatkov.
10) Z uredbo bi se moral dostop do podatkov o naročnikih in dostopu omejiti na seznam kaznivih dejanj, ki so strogo določena, ali vsaj na „huda kazniva dejanja“.
11) V uredbi bi bilo treba bolje utemeljiti rok za predložitev podatkov, zlasti v nujnih primerih, možnost uporabe hitrega šesturnega postopka pa bi morala vključevati obveznost, da morajo organi, ki predložijo zahtevo, dokazati nujnost, zaradi katere se uporabi ta postopek, kar se lahko naredi celo naknadno, da se omogoči nadzor nad uporabo takih izjemnih pooblastil.
12) Postopek, ki omogoči predložitev podatkov o vsebini brez kakršne koli vključitve pristojnih organov države članice, v kateri je posameznik, na katerega se nanašajo osebni podatki, bi bilo treba opustiti.
13) V uredbi bi bilo treba izboljšati zaščitne ukrepe, povezane z izdajo evropskih nalogov za zavarovanje e-dokazov.
14) Uredba bi morala vključevati vsaj minimalno običajno odstopanje, da bi bilo treba izvršitev naloga zavrniti, če je mogoče utemeljeno domnevati, da bodo z izvršitvijo naloga kršene temeljne pravice zadevnega posameznika, zaradi česar država izvršiteljica ne bo upoštevala svojih obveznosti glede varstva temeljnih pravic, priznanih v Listini.
15) V uredbi bi morala biti predvidena širša obveznost, da se je treba v primeru kolizije zakonov posvetovati s pristojnimi organi tretje države, v kateri je ponudnik storitev, od katerega se zahteva predložitev podatkov, da bi se izognili subjektivnim razlagam enega samega sodišča.
16) Veljavnost in trajanje nalogov za zavarovanje dokazov bi morala biti bolj povezana z nalogi za predložitev, ki so jim priloženi.
17) Bolj bi bilo treba poskrbeti za varnost prenosa podatkov.
18) Predvideti bi bilo treba preverjanje pristnosti podatkov, zlasti kadar bi se lahko zagotovili šifrirani podatki.

Za Evropski odbor za varstvo podatkov

Predsednica
(Andrea Jelinek)