EUROPSKA
KOMISIJA

Bruxelles, 27.11.2013.
COM(2013) 847 final

KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU

o funkcioniranju „sigurne luke” iz perspektive građana EU-a i poduzeća s poslovnim nastanom u Europskoj uniji

KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU

o funkcioniranju „sigurne luke" iz perspektive građana EU-a i poduzeća s poslovnim nastanom u Europskoj uniji

UVOD

Direktivom 95/46/EZ od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (dalje u tekstu: Direktiva o zaštiti podataka) utvrđena su pravila za prijenose osobnih podataka iz država članica EU-a u druge države izvan EU-a[1] u mjeri u kojoj su takvi prijenosi obuhvaćeni područjem primjene tog instrumenta[2].

U skladu s Direktivom Komisija može utvrditi da treća zemlja osigurava odgovarajuću razinu zaštite temeljem domaćeg zakonodavstva ili međunarodnih obveza koje je preuzela s ciljem zaštite prava pojedinaca u kojem se slučaju posebna ograničenja prijenosa podataka za tu zemlju ne bi primjenjivala. Takve se odluke uobičajeno navode kao **„odluke o odgovarajućoj zaštiti"**.

Komisija je 26. srpnja 2000. donijela Odluku 520/2000/EZ[3] (dalje u tekstu: **Odluka o „sigurnoj luci"**) kojom načela privatnosti „sigurne luke" i često postavljana pitanja („načela" odnosno „često postavljana pitanja"), koja je izdalo Ministarstvo trgovine Sjedinjenih Američkih Država, priznaje kao odgovarajuću zaštitu u smislu prijenosa osobnih podataka iz EU-a. Odluka o „sigurnoj luci" donijeta je nakon mišljenja Radne skupine iz članka 29. i mišljenja Odbora iz članka 31. koje je donijela kvalificirana većina država članica. U skladu s Odlukom Vijeća 1999/468 Odluka o „sigurnoj luci" bila je predmet prethodnog nadzora Europskog parlamenta.

Kao rezultat toga sadašnjom je Odlukom o „sigurnoj luci" dopušten slobodan prijenos[4] osobnih podataka iz država članica EU-a[5] poduzećima u SAD-u koja su prihvatila načela u okolnostima u kojima prijenos drugačije ne bi ispunio standarde EU-a za odgovarajuću razinu zaštite podataka s obzirom na značajne razlike režima zaštite privatnosti između dviju strana Atlantika.

Funkcioniranje sadašnjeg sporazuma o „sigurnoj luci" oslanja se na preuzimanje obveza i samocertificiranje poduzeća koja se pridržavaju načela. Prihvaćanje je tih aranžmana dobrovoljno, ali su pravila obvezujuća za one koji ih prihvate. Osnovna su načela takvog aranžmana sljedeća:

transparentnost politika zaštite privatnosti poduzeća koja se pridržavaju načela;

uključivanje načela „sigurne luke" u politike zaštite privatnosti poduzeća; i

---

1 Člancima 25. i 26. Direktive o zaštiti podataka utvrđen je pravni okvir za prijenose osobnih podataka iz EU-a u treće zemlje izvan EGP-a.

2 Dodatna su pravila utvrđena u članku 13. Okvirne odluke 2008/977/PUP od 27. studenoga 2008. o zaštiti osobnih podataka obrađenih u okviru policijske i pravosudne suradnje u kaznenim stvarima u mjeri u kojoj se takvi prijenosi odnose na osobne podatke koji su preneseni ili stavljeni na raspolaganje od jedne države članice drugoj državi članici, koja nakon toga namjerava te podatke poslati trećoj zemlji ili međunarodnom tijelu u svrhu sprečavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršenja kaznenopravnih sankcija.

3 Odluka Komisije 520/2000/EZ od 26 srpnja 2000. sukladno s Direktivom 95/46/EZ Europskog parlamenta i Vijeća o primjerenosti zaštite koju pružaju načela privatnosti „sigurne luke" i uz njih vezana često postavljana pitanja koje je izdalo Ministarstvo trgovine SAD-a u SL 215 od 28. kolovoza 2000., str. 7.

4 To ne isključuje primjenu na obradu podataka drugih zahtjeva koji mogu postojati na temelju nacionalnog zakonodavstva kojim se provodi direktiva EU-a o zaštiti podataka.

5 To se odnosi i na prijenose podataka iz država članica EGP-a nakon proširenja Direktive 95/46/EZ na Sporazum o EGP-u, Odluka 38/1999 od 25. lipnja 1999., SL L 296/41, 23.11.2000.

provedba, uključujući od strane tijela javne vlasti.

Tu temeljnu osnovu „sigurne luke” treba preispitati u **novom kontekstu**:

eksponencijalnog rasta protoka podataka koji su bili sporedni, a sada su ključni za brzi rast digitalnoga gospodarstva i brzog razvoja događaja u prikupljanju, obradi i korištenju podataka;

kritične važnosti protoka podataka, osobito za transatlantsko gospodarstvo,[6]

brzog rasta broja poduzeća iz SAD-a koja se pridržavaju programa „sigurne luke”, pri čemu je od 2004. njihov broj povećan za više od osam puta (od 400 u 2004. do 3 246 u 2013.);

nedavno objavljenih informacija o programima nadzora SAD-a koje su izazvale nova pitanja o razini zaštite koju pruža aranžman „sigurne luke”.

Na temelju toga, u ovoj se Komunikaciji razmatra funkcioniranje programa „sigurne luke”. Ona je **utemeljena na dokazima** koje je prikupila Komisija, radu Kontaktne skupine za zaštitu privatnosti EU-a i SAD-a iz 2009., studiji koju je proveo vanjski ugovorni izvođač 2008.[7] i informacijama dobivenima u okviru *ad hoc* radne skupine EU-a i SAD-a („Radna skupina”) koja je osnovana nakon otkrića u vezi s programima nadzora SAD-a *(vidi paralelni dokument)*. Ova se Komunikacija nastavlja na dva **izvješća Komisije o ocjeni** u početnom razdoblju aranžmana „sigurne luke” iz 2002.[8] odnosno 2004[9].

2. STRUKTURA I FUNKCIONIRANJE „SIGURNE LUKE”

2.1. Struktura „sigurne luke”

Poduzeće iz SAD-a koje se želi pridržavati načela „sigurne luke” mora: (a) u svojoj javno objavljenoj politici zaštite privatnosti navesti da se pridržava načela i da je stvarno usklađeno s načelima te (b) obaviti samocertificiranje tj. izjaviti Ministarstvu trgovine SAD-a da poštuje načela. Samocertificiranje se mora obnoviti svake godine. Načela zaštite privatnosti „sigurne luke” navedene u Prilogu I. Odluci o „sigurnoj luci” uključuju zahtjeve za temeljitu zaštitu osobnih podataka (načela nepovredivosti podataka, sigurnosti, mogućnosti izbora i daljnjeg prijenosa) te postupovnih prava osoba čiji se podaci obrađuju (načela obavijesti, pristupa i provedbe).

U pogledu provedbe programa „sigurne luke” u SAD-u, dvije institucije SAD-a imaju glavnu ulogu: Ministarstvo trgovine SAD-a i Savezna trgovinska komisija SAD-a.

Ministarstvo trgovine provjerava svako samocertificiranje „sigurne luke” i svako podnošenje ponovne godišnje certifikacije koje primi od poduzeća kako bi osiguralo da uključuju elemente koji su potrebni za članstvo u programu[10]. Ono ažurira popis poduzeća koja su

---

6 Prema nekim studijama, ako bi došlo do poremećaja protoka podataka kao posljedice diskontinuiteta obvezujućih pravila koja se odnose na poduzeća, standardnih ugovornih klauzula i „sigurne luke”, negativan bi učinak na BDP Europske unije mogao doseći -0,8 % do -1,3 %, a izvoz usluga EU-a u SAD pao bi za -6,7 % zbog gubitka konkurentnosti. Vidi: „Gospodarska važnost ispravnog uređivanja zaštite podataka”, studija Europskog centra za međunarodnu političku ekonomiju za Gospodarsku komoru SAD-a, ožujak 2013.

7 Studija ocjene utjecaja koju je za Europsku komisiju 2008. proveo *Centre de Recherche Informatique et Droit* („CRID”) Sveučilišta u Namuru.

8 Radni dokument osoblja Komisije „Primjena Odluke Komisije 520/2000/EZ od 26 srpnja 2000. sukladno s Direktivom 95/46/EZ Europskog parlamenta i Vijeća o odgovarajućoj zaštiti osobnih podataka koju pružaju načela privatnosti „sigurne luke” i uz njih vezana često postavljana pitanja koje je izdalo Ministarstvo trgovine SAD-a” SEC (2002.) 196, 13.12.2002.

9 Radni dokument osoblja Komisije „Provedba Odluke Komisije 520/2000/EZ o odgovarajućoj zaštiti osobnih podataka koju pružaju načela privatnosti „sigurne luke” i uz njih vezana često postavljana pitanja koje je izdalo Ministarstvo trgovine SAD-a” SEC (2004.) 1323, 20.10.2004.

10 Ako certifikacija ili ponovna certifikacija poduzeća ne ispunjava zahtjeve „sigurne luke”, Ministarstvo trgovine obavješćuje poduzeće o koracima koje treba poduzeti (tj. pojašnjenjima, izmjenama u opisu politike) prije nego što postupak certifikacije poduzeća može biti okončan.

dostavila pisma o samocertificiranju i objavljuje popis i pisma na svojem *web*-mjestu. Osim toga, ono prati funkcioniranje „sigurne luke" i s popisa uklanja poduzeća koja ne poštuju načela.

Savezna trgovinska komisija, u okviru svojih ovlasti u području zaštite potrošača, intervenira u slučaju nepoštenih ili prijevarnih praksi u skladu s odjeljkom 5. Zakona o Saveznoj trgovinskoj komisiji. Mjere provedbe od strane Savezne trgovinske komisije uključuju istrage lažnih izjava o poštovanju načela „sigurne luke" ili nepoštovanju tih načela od strane poduzeća koja su članovi programa. U posebnim je slučajevima provedbe načela „sigurne luke" kod zračnih prijevoznika nadležno tijelo Ministarstvo prometa SAD-a[11].

Sadašnja je Odluka o „sigurnoj luci" dio zakonodavstva EU-a koje moraju primjenjivati nadležna tijela država članica. U skladu s Odlukom, **nacionalna tijela za zaštitu podataka** u EU-u u određenim slučajevima imaju pravo suspendirati prijenose podataka certificiranim poduzećima u „sigurnoj luci"[12]. Komisija od osnivanja „sigurne luke" 2000. nije zabilježila slučaj suspenzije od strane nacionalnog tijela za zaštitu podataka. Neovisno o ovlastima koje imaju na temelju Odluke o „sigurnoj luci", nacionalna tijela za zaštitu podataka u EU-u ovlaštena su intervenirati, uključujući u slučaju međunarodnih prijenosa, kako bi osigurala usklađenost s općim načelima zaštite podataka utvrđene u Direktivi o zaštiti podataka iz 1995.

Kako se podsjeća u sadašnjoj Odluci o „sigurnoj luci", **u nadležnosti je Komisije** –djelujući u skladu s postupkom ispitivanja iz Uredbe 182/2011 – da Odluku u bilo koje vrijeme može izmijeniti, suspendirati ili ograničiti njezino područje primjene, uzimajući u obzir iskustva u njezinoj provedbi. To je osobito predviđeno u slučaju sistemskog kvara na strani SAD-a, primjerice ako neko tijelo odgovorno za osiguranje usklađenosti s načelima privatnosti „sigurne luke" u stvarnosti ne izvršava svoju ulogu, ili ako razinu zaštite koju pružaju načela „sigurne luke" usvoji zakonodavstvo SAD-a. Kao i svaka druga odluka Komisije, ona isto tako može biti izmijenjena iz drugih razloga ili čak ukinuta.

2.2. Funkcioniranje „sigurne luke"

Broj od **3 246**[13] **certificiranih poduzeća** uključuje i mala i velika poduzeća[14]. Dok su financijske usluge i telekomunikacijska industrija izvan ovlasti Savezne trgovinske komisije i stoga isključene iz „sigurne luke", među certificiranim poduzećima prisutni su brojni industrijski i uslužni sektori, uključujući poznata internetska poduzeća i industrije u rasponu od informacijskih i računalnih do farmaceutskih poduzeća, usluga putovanja i turizma, zdravstvene skrbi ili kreditnih kartica[15]. To su uglavnom poduzeća iz SAD-a koja pružaju usluge na unutarnjem tržištu EU-a. Isto su tako uključena ovisna društva poduzeća iz EU-a poput Nokije ili Bayera. 51 % su poduzeća koja obrađuju podatke zaposlenika u Europi koji se prenose u SAD za potrebe ljudskih potencijala[16].

---

11 Na temelju glave 49. odjeljka 41712 Zakonika SAD-a.

12 Točnije, suspenzija prijenosa može biti zahtijevana u dvije situacije, ako:
(a) je vladino tijelo u SAD-u utvrdilo da poduzeće krši načela privatnosti „sigurne luke"; ili
(b) postoji stvarna vjerojatnost da se krše načela privatnosti „sigurne luke"; ako postoje opravdani razlozi da se vjeruje da dotični mehanizam provedbe ne poduzima ili neće poduzeti primjerene i pravovremene korake da razriješi dotični slučaj; ako bi nastavak prijenosa stvorio trenutačnu opasnost da ozbiljno našteti osobama čiji se podaci obrađuju; te ako su nadležna tijela država članica poduzela odgovarajuće napore da u tim okolnostima obavijeste poduzeće i dala joj mogućnost da se očituje.

13 Na dan 26. rujna 2013. broj organizacija u „sigurnoj luci" sa statusom „**sadašnji član**" na popisu sudionika u „sigurnoj luci" iznosio je **3 246**, a sa statusom „**bivši član**" **935**.

14 Organizacije u „sigurnoj luci" s 250 ili manje zaposlenika: 60 **%** (1 925 od 3 246). Organizacije u „sigurnoj luci" s 251 ili više zaposlenika: **40 %** (1 295 od 3 246).

15 Na primjer MasterCard posluje s tisućama banaka i to je poduzeće jasan primjer slučaja gdje „sigurna luka" ne može biti zamijenjena drugim pravnim instrumentima za prijenose osobnih podataka poput obvezujućih pravila koja se odnose na poduzeća ili ugovornih odnosa.

16 Organizacije u „sigurnoj luci" čiji su podaci o ljudskim potencijalima obuhvaćeni njihovim certificiranjem „sigurne luke" (i time su pristale na suradnju i usklađenost s tijelima za zaštitu podataka u EU-u): **51%** (1 671 od 3 246).

Među nekim tijelima za zaštitu podataka u EU-u postoji **rastuća zabrinutost** o prijenosima podataka u okviru sadašnjeg programa „sigurne luke”. Neka su tijela država članica za zaštitu podataka kritizirala vrlo općenitu formulaciju načela i visoku razinu oslanjanja na samocertificiranje i samoregulaciju. Istu je zabrinutost izrazila industrija u odnosu na narušavanje tržišnog natjecanja zbog nedostatne provedbe.

Sadašnji aranžman „sigurne luke” temelji se na dobrovoljnom pridržavanju poduzeća, na samocertificiranju tih poduzeća koja se pridržavaju načela i na provedbi obveza preuzetih samocertificiranjem od strane tijela javne vlasti. U tom kontekstu svaki manjak transparentnosti i svi nedostaci u provedbi potkopavaju temelje na kojima je program „sigurne luke” izgrađen.

Bilo kakvi nedostaci u transparentnosti i provedbi od strane SAD-a dovode do prebacivanja odgovornosti na europska tijela za zaštitu podataka i na poduzeća koja koriste program. Njemačka su tijela za zaštitu podataka 29. travnja 2010. objavila odluku kojom od poduzeća koja prenose podatke iz Europe u SAD zahtijevaju da aktivno provjeravaju da poduzeća u SAD-u koja uvoze podatke poštuju načela privatnosti „sigurne luke” i preporučuju da „barem izvozno poduzeće mora utvrditi da li je certifikacija ‚sigurne luke' uvoznika još uvijek valjana”[17].

Na dan 24. srpnja 2013., nakon otkrića u vezi s programima nadzora SAD-a, njemački savjetnici za zaštitu podataka otišli su korak dalje u izražavanju zabrinutosti da „postoji stvarna vjerojatnost da se krše načela iz odluka Komisije”[18]. Postoje slučajevi gdje su neki savjetnici za zaštitu podataka (npr. savjetnik za zaštitu podataka iz Bremena) zahtijevali od poduzeća koje prenosi osobe podatke pružateljima iz SAD-a da obavijesti savjetnika za zaštitu podataka o tome da li i kako dotični pružatelji sprečavaju pristup Nacionalnoj sigurnosnoj agenciji. Irski je savjetnik za zaštitu podataka prijavio nedavni primitak dvije pritužbe koje se odnose na program „sigurne luke” nakon vijesti o programima obavještajnih agencija SAD-a, ali je istraga pritužbi odbačena na temelju toga da je prijenos osobnih podataka u treću zemlju bio u skladu sa zahtjevima irskog zakona o zaštiti podataka. Nakon slične pritužbe luksemburški je savjetnik za zaštitu podataka utvrdio da su Microsoft i Skype pri prijenosu podataka u SAD poštovali luksemburški Zakon o zaštiti podataka[19]. Međutim, od tada je irski Visoki sud odobrio zahtjev za sudsku reviziju na temelju kojeg će preispitati nedjelovanje irskog povjerenika za zaštitu podataka u vezi s programima nadzora SAD-a. Jednu od dvije pritužbe podnijela je studentska skupina Europe v Facebook (EvF) koja je isto tako podnijela sličnu pritužbu protiv Yahooa, koji je u postupku obrade relevantnih tijela za zaštitu podataka.

Ovi različiti odgovori tijela za zaštitu podataka na otkrića o nadziranju ukazuju na stvarni rizik fragmentacije programa „sigurne luke” i postavljaju pitanja o razini njegove provedbe.

---

17 Vidi odluku Düsseldorfer Kreis od 28./29. travnja 2010. Vidi: *Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover*: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile Međutim, europski nadzornik za zaštitu podataka Peter Hustinx u okviru je istrage Odbora za građanske slobode, pravosuđe i unutarnje poslove Europskog parlamenta 7. listopada 2013. izrazio mišljenje da su „postignuta značajna poboljšanja i većina je pitanja razriješena” u vezi sa „sigurnom lukom”: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_EN.pdf

18 Vidi rezoluciju njemačke konferencije povjerenika za zaštitu podataka u kojoj je naglašeno da obavještajne službe predstavljaju masovnu prijetnju prijenosu podataka između Njemačke i zemalja izvan Europe: http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870

19 Vidi priopćenje za tisak luksemburškog savjetnika za zaštitu podataka od 18. studenoga 2013.

3. TRANSPARENTNOST POLITIKA ZAŠTITE PRIVATNOSTI PODUZEĆA KOJA SE PRIDRŽAVAJU NAČELA

Na temelju često postavljanog pitanja 6. koje je priloženo Odluci o „sigurnoj luci" (Prilog II.) poduzeća koja žele biti certificirana u sklopu „sigurne luke" moraju Ministarstvu trgovine dostaviti svoju politiku zaštite privatnosti te ju javno objaviti. Ta politika mora sadržavati i obvezu poštovanja načela privatnosti. Zahtjev samocertificiranim poduzećima da **javno objave svoje politike zaštite privatnosti** te njihova izjava o poštovanju načela privatnosti ključni su za funkcioniranje programa.

Nedovoljna dostupnost politika zaštite privatnosti takvih poduzeća na štetu je pojedinaca čiji se osobni podaci prikupljaju i obrađuju, te može predstavljati **kršenje načela obavijesti.** U takvim slučajevima pojedinci čiji se podaci prenose iz EU-a mogu biti nesvjesni svojih prava i obveza koje je poduzeće preuzelo samocertificiranjem.

Osim toga, obveza poduzeća na poštovanje načela privatnosti **pokreće ovlasti Savezne trgovinske komisije na provedbu tih načela** u odnosu na poduzeća u slučajevima nepridržavanja kao nepoštene ili prijevarne prakse. Manjak transparentnosti u SAD-u čini nadzor Savezne trgovinske komisije težim i ugrožava učinkovitost provedbe.

Tijekom godina značajan broj samocertificiranih poduzeća nije javno objavio svoju politiku zaštite privatnosti i/ili nije dao javnu izjavu o poštovanju načela privatnosti. U izvješću o „sigurnoj luci" iz 2004. istaknuta je potreba da Ministarstvo trgovine **zauzme aktivniji stav u nadzoru poštovanja** ovog zahtjeva.

Od 2004. Ministarstvo trgovine razvilo je **nove informacijske alate** usmjerene na pomoć poduzećima u poštovanju njihovih obveza transparentnosti. Na *web*-mjestu Ministarstva trgovine posvećenom „sigurnoj luci"[20] dostupne su relevantne informacije, a poduzeća isto tako mogu na njemu postaviti svoje politike zaštite privatnosti. Ministarstvo trgovine izvijestilo je da su poduzeća iskoristila ovu mogućnost i pri prijavi za pridruživanje „sigurnoj luci"[21] postavila svoje politike zaštite privatnosti na *web*-mjestu Ministarstva trgovine. Osim toga, u razdoblju 2009. – 2013. Ministarstvo trgovine objavilo je niz smjernica za poduzeća koja se žele pridružiti „sigurnoj luci", poput „Vodiča za samocertificiranje" i „Korisnih savjeta za uspješno samocertificiranje"[22].

Stupanj usklađenosti s obvezama transparentnosti razlikuje se među poduzećima. Dok se određena poduzeća ograničavaju na dostavljanje opisa svoje politike zaštite privatnosti Ministarstvu trgovine u okviru postupka samocertificiranja, većina poduzeća, uz postavljanje te politike na *web*-mjestu Ministarstva trgovine, istu i javno objavljuje na svojem *web*-mjestu. Međutim, te **politike nisu uvijek predstavljene u lako razumljivom i čitljivom obliku za potrošače**. Hiperpoveznice na politike zaštite privatnosti ne funkcioniraju uvijek pravilno i ne vode uvijek do ispravnih *web*-stranica.

Iz Odluke i njezinih priloga proizlazi da zahtjev da poduzeća trebaju javno objaviti svoje politike zaštite privatnosti **prelazi okvire same dostave obavijesti** o samocertificiranju Ministarstvu trgovine. Zahtjevi za certificiranje utvrđeni u često postavljanim pitanjima uključuju opis politike zaštite privatnosti i transparentne informacije o tome gdje je ona dostupna na uvid javnosti[23]. Izjave o politici zaštite privatnosti moraju biti jasne i lako

---

20 http://www.export.gov/SafeHarbour/

21 https://SafeHarbour.export.gov/list.aspx

22 Vodič je dostupan na *web*-mjestu programa na adresi: http://export.gov/SafeHarbour/ Korisni savjeti: http://export.gov/SafeHarbour/eu/eg_main_018495.asp

23 Ministarstvo trgovine je 12. studenoga 2013. potvrdilo da „danas poduzeća koja imaju javno dostupna *web*-mjesta i obuhvaćaju podatke o potrošačima/klijentima/posjetiteljima moraju objaviti politiku zaštite privatnosti koja je u skladu s načelima ‚sigurne

dostupne javnosti. One moraju sadržavati hiperpoveznicu na *web*-mjesto Ministarstva trgovine o „sigurnoj luci" na kojem se navode svi „sadašnji" članovi programa kao i poveznicu na pružatelja usluga alternativnog rješavanja sporova. Međutim, u razdoblju 2000. – 2013. određeni broj poduzeća u programu nije poštovao ove zahtjeve. Tijekom radnih kontakata s Komisijom u veljači 2013. Ministarstvo je trgovine potvrdilo da približno 10 % certificiranih poduzeća zapravo nije na svojem javnom *web*-mjestu objavilo politiku zaštite privatnosti koja sadrži izjavu o poštovanju načela „sigurne luke".

Nedavni statistički podaci isto tako ukazuju na trajni problem **lažnih tvrdnji o poštovanju načela „sigurne luke"**. Približno 10 % poduzeća koja tvrde da su članovi „sigurne luke" nije navedeno na popisu Ministarstva trgovine kao sadašnji članovi programa[24]. Takve lažne tvrdnje potječu iz poduzeća koja nisu nikada sudjelovala u „sigurnoj luci" i poduzeća koja su sudjelovala u programu, ali nisu Ministarstvu trgovine svake godine dostavile obnovu samocertifikacije. U tom slučaju ona ostaju na popisu „sigurne luke", ali sa statusom „bivši član", što znači da je poduzeće bilo član programa i time ima obvezu nastaviti pružati zaštitu već obrađenim podacima. Savezna trgovinska komisija nadležna je intervenirati u slučajevima prijevarnih praksi i nepoštovanja načela „sigurne luke" (vidi odjeljak 5.1.). Nejasnoće oko „lažnih tvrdnji" utječu na vjerodostojnost programa.

Europska je komisija tijekom redovitih kontakata u 2012. i 2013. upozorila Ministarstvo trgovine da za poštovanje obveza transparentnosti nije dovoljno da poduzeća samo dostave opis svoje politike zaštite privatnosti Ministarstvu trgovine. Izjave o politici zaštite privatnosti moraju biti stavljene na raspolaganje javnosti. Od Ministarstva je trgovine isto tako zatraženo da **pojača svoje periodične kontrole *web*-mjesta poduzeća** nakon postupka provjere provedenog u okviru prvog postupka ili godišnje obnove samocertificiranja te da poduzme mjere protiv onih poduzeća koja ne ispunjavaju zahtjeve transparentnosti.

Kao prvi odgovor na zabrinutost EU-a, Ministarstvo trgovine je od ožujka 2013. uvelo obvezu da poduzeće u „sigurnoj luci" koje ima *web*-mjesto s javnim pristupom mora na njemu objaviti svoju politiku zaštite privatnosti za podatke potrošača/korisnika. Istovremeno je Ministarstvo trgovine počelo obavješćivati sva poduzeća čija politika zaštite privatnosti nije već sadržavala poveznicu na *web*-mjesto Ministarstva trgovine o „sigurnoj luci" da trebaju dodati takvu poveznicu, čineći službeni popis „sigurne luke" i *web*-mjesto izravno dostupnim potrošačima koji posjećuju *web*-mjesto poduzeća. Time će se osobama iz Europe čiji se podaci obrađuju omogućiti da odmah, bez dodatnog pretraživanja interneta, provjere preuzete obveze poduzeća dostavljene Ministarstvu trgovine. Osim toga, Ministarstvo trgovine počelo je obavješćivati poduzeća da u svoje objavljene politike zaštite privatnosti trebaju uključiti podatke za kontakt njihova neovisnog pružatelja usluga rješavanja sporova[25]

Taj je proces potrebno ubrzati kako bi se osiguralo da sva certificirana poduzeća u potpunosti zadovoljavaju zahtjeve „sigurne luke" najkasnije do ožujka 2014. (tj. do roka za ponovnu certifikaciju poduzeća koji teče od uvođenja novih zahtjeva u ožujku 2013.).

---

luke' na svojem *web*-mjestu" (dokument: „Suradnja SAD-a i EU-a u svrhu provedbe okvira ‚sigurne luke'" od 12.studenoga 2013.).

24 U rujnu 2013. australska je konzultantska kuća Galexia usporedila „lažne tvrdnje" o članstvu u „sigurnoj luci" iz 2008. i 2013. Glavni nalaz konzultanata odnosi se na činjenicu da je porastom broja članova u „sigurnoj luci" između 2008. i 2013. (s 1 109 na 3 246) povećan i broj lažnih tvrdnji s 206 na 427 http://www.galexia.com/public/about/news/about_news-id225.html

25 Između ožujka i rujna 2013. Ministarstvo trgovine je:

• obavijestilo 101 poduzeće koje je već postavilo svoju politiku zaštite privatnosti koja je u skladu s načelima „sigurne luke" na web-mjestu „sigurne luke" da isto tako mora objaviti svoju politiku zaštite privatnosti na web-mjestu svojeg poduzeća,

• obavijestilo 154 poduzeća koja to još nisu učinila da u svoju politiku zaštite privatnosti trebaju dodati poveznicu na *web*-mjesto „sigurne luke",

• obavijestilo više od 600 poduzeća da u svoju politiku zaštite privatnosti trebaju uključiti podatke za kontakt njihova neovisnog pružatelja usluga rješavanja sporova

Unatoč tome i dalje postoje zabrinutosti u vezi s time da li samocertificirana poduzeća u potpunosti poštuju zahtjeve transparentnosti. Ministarstvo trgovine trebalo bi strože pratiti i istraživati poštovanje obveza preuzetih u trenutku prvog samocertificiranja i godišnje obnove istog.

4. UKLJUČIVANJE NAČELA PRIVATNOSTI „SIGURNE LUKE" U POLITIKE ZAŠTITE PRIVATNOSTI PODUZEĆA

Samocertificirana poduzeća moraju poštovati načela privatnosti iz Priloga I. kako bi dobile i zadržale pogodnosti „sigurne luke".

U izvješću iz 2004. Komisija je utvrdila da značajan broj **poduzeća nije pravilno uključio načela privatnosti „sigurne luke"** u svoju politiku obrade podataka. Na primjer, pojedinci nisu uvijek dobili jasne i transparentne informacije o svrsi obrade njihovih podataka ili im nije ponuđena mogućnost odustajanja ako će ti podaci biti otkriveni trećoj osobi ili korišteni u svrhu koja nije sukladna svrsi za koju su izvorno prikupljeni. U izvješću Komisije iz 2004. navedeno je da bi Ministarstvo trgovine *„trebalo biti proaktivnije s obzirom na pristupanje ‚sigurnoj luci' i svijest o načelima"*[26].

U tom je pitanju ostvaren ograničeni napredak. Od 1. siječnja 2009. svako poduzeće koje želi obnoviti status svoje certifikacije u „sigurnoj luci" – koja se mora obnavljati jednom godišnje – podvrgnuto je postupku ocjene svoje politike zaštite privatnosti od Ministarstva trgovine prije obnove statusa. Međutim, ta je ocjena ograničenog opsega. Nema **potpune ocjene stvarne prakse** samocertificiranih poduzeća kojom bi se značajno povećala vjerodostojnost postupka samocertificiranja.

Nastavno na zahtjeve Komisije za strožim i sustavnijim nadzorom samocertificiranih poduzeća od strane Ministarstva trgovine, **više se pažnje trenutačno posvećuje novim zahtjevima za članstvo**. Broj novih zahtjeva koji nisu prihvaćeni, već su vraćeni poduzećima u svrhu poboljšanja politike zaštite privatnosti, značajno se povećao između 2010. i 2013.: udvostručio se za poduzeća koja obnavljaju članstvo i utrostručio za nove članove „sigurne luke"[27]. Ministarstvo trgovine uvjerava Komisiju da svaki postupak certifikacije ili ponovne certifikacije može biti zaključen samo ako politika zaštite privatnosti poduzeća ispunjava sve zahtjeve, a osobito da uključuje izjavu o poštovanju relevantnog skupa načela privatnosti „sigurne luke" te je politika zaštite privatnosti dostupna javnosti. Od poduzeća se zahtijeva da na popisu „sigurne luke" navede lokaciju odgovarajuće politike. Isto se tako zahtijeva da poduzeće na svojem *web*-mjestu jasno utvrdi pružatelja usluga alternativnog rješavanja sporova i navede poveznicu na *web*-mjesto Ministarstva trgovine o samocertificiranju „sigurne luke"**.** Međutim, procijenjeno je da više od 30 % članova „sigurne luke" u politikama zaštite privatnosti na svojim *web*-mjestima ne navodi informacije o rješavanju sporova[28].

Većina poduzeća koje je Ministarstvo trgovine uklonilo s popisa „sigurne luke" uklonjena je na izričit zahtjev odgovarajućih poduzeća (npr. poduzeća koja su spojena ili preuzeta, promijenila svoju poslovnu djelatnost ili prestala poslovati). Manji je broj evidencija neaktivnih poduzeća uklonjen kada je utvrđeno da *web*-mjesta navedena u evidenciji više nisu

---

26 Vidi str. 8. Izvješća SEC (2004) 1323 iz 2004.

27 Prema statističkim podacima Ministarstva trgovine iz rujna 2013., Ministarstvo je 2010. obavijestilo 18 % (93) od 512 novih članova i 16 % (231) od 1 417 poduzeća koja su obnovila članstvo o potrebnim poboljšanjima u njihovim politikama zaštite privatnosti i/ili zahtjevima za članstvo u „sigurnoj luci". Međutim, nastavno na zahtjeve Komisije za strožim i sustavnijim nadzorom svih zahtjeva za članstvo, do sredine rujna 2013. Ministarstvo trgovine obavijestilo je 56 % (340) od 602 nova člana i 27 % (493) od 1 809 poduzeća koja su obnovila članstvo o potrebi poboljšanja njihovih politika zaštite privatnosti.

28 Izjava Chrisa Connollya (Galexia) u sklopu istrage Odbora za građanske slobode, pravosuđe i unutarnje poslove Europskog parlamenta od 7. listopada 2013.

u funkciji, a njihov je status već nekoliko godina „bivši član”[29]. Važno je naglasiti kako izgleda da nijedno od tih uklanjanja nije provedeno zato što su provjerom Ministarstva trgovine otkriveni problemi s poštovanjem načela.

Popis „sigurne luke” služi kao javna obavijest i evidencija preuzetih obveza poduzeća povezanih sa „sigurnom lukom”. **Preuzeta obveza poštovanja načela „sigurne luke” nije vremenski ograničena** s obzirom na podatke koje poduzeće primi tijekom razdoblja u kojem koristi pogodnosti „sigurne luke” te poduzeće mora nastaviti primjenjivati načela na takve podatke sve dok ih pohranjuje, koristi ili otkriva, čak i ako napusti „sigurnu luku” iz bilo kojeg razloga.

Broj **podnositelja zahtjeva za članstvo u „sigurnoj luci” koji nisu prošli administrativni pregled** Ministarstva trgovine i stoga nisu uvršteni na popis „sigurne luke” je sljedeći: U **2010**., samo **6 %** (33) od 513 novih članova nije uvršteno na popis „sigurne luke” jer nisu ispunili norme Ministarstva trgovine za samocertificiranje. U **2013**., **12%** (75) od 605 novih članova nije uvršteno na popis „sigurne luke” jer nisu ispunili norme Ministarstva trgovine za samocertificiranje.

Kao najmanji uvjet za povećanje transparentnosti nadzora, Ministarstvo trgovine trebalo bi na svojem *web*-mjestu navesti sva poduzeća koja su uklonjena s popisa „sigurne luke” i navesti razloge zašto certifikacija nije obnovljena. Oznaku „bivši član” na popisu poduzeća članova „sigurne luke” Ministarstva trgovine ne bi trebalo navoditi samo kao informaciju, već bi ona trebala biti popraćena **jasnim upozorenjem** – riječima i slikom – da poduzeće trenutačno ne ispunjava zahtjeve „sigurne luke”.

Nadalje, neka poduzeća još uvijek nisu potpuno usvojila sva načela „sigurne luke”. Uz pitanje transparentnosti iz prethodnog odjeljka 3., politike zaštite privatnosti samocertificiranih poduzeća često su nejasne u vezi sa svrhom prikupljanja podataka i pravom izbora hoće li ti podaci biti otkriveni trećim osobama ili ne; time se u pitanje dovodi poštovanje načela privatnosti „obavijesti” i „mogućnosti izbora”. Obavijest i mogućnost izbora ključni su za osiguranje kontrole osoba čiji se podaci obrađuju nad onime što se događa s njihovim osobnim podacima.

Ključni prvi korak u procesu potvrđivanja, uključivanje načela privatnosti „sigurne luke” u politike poduzeća za zaštitu privatnosti, nije osiguran na zadovoljavajući način. Ministarstvo trgovine trebalo bi dati prednost rješavanju tog problema razvojem metodologije za usklađenost poslovne prakse poduzeća i njihove interakcije s klijentima. **Ministarstvo trgovine mora aktivno pratiti stvarno uključivanje načela privatnosti „sigurne luke” u politike poduzeća za zaštitu privatnosti** umjesto da provedbu obveza pokreću samo pritužbe pojedinaca.

5. PROVEDBA OD STRANE TIJELA JAVNE VLASTI

Dostupan je niz mehanizama kojima se osigurava provedba programa „sigurne luke” i pravna zaštita pojedinaca u slučajevima kada nepoštovanje načela privatnosti utječe na zaštitu njihovih osobnih podataka.

Prema načelu „provedbe”, politike zaštite privatnosti samocertificiranih poduzeća moraju uključivati mehanizme kojima se osigurava poštovanje načela. U skladu s načelom „provedbe”, kako je dodatno razjašnjeno u često postavljanim pitanjima 11., 5. i 6., taj zahtjev može biti ispunjen primjenom **neovisnih mehanizama pravne zaštite** tijela koja su javno

[29] Od prosinca 2011. Ministarstvo trgovine SAD-a uklonilo je 323 poduzeća s popisa „sigurne luke”: 94 poduzeća je uklonjeno s popisa zbog stečaja; 88 poduzeća zbog spajanja ili preuzimanja; 95 poduzeća na zahtjev matičnog društva; 41 poduzeće zbog propusta obnove članstva i 5 poduzeća iz ostalih razloga.

potvrdila svoju nadležnost za primanje pritužbi pojedinaca u slučaju nepoštovanja načela. Alternativno, to se može postići kroz preuzimanje obveze organizacije na suradnju s **Europskim odborom za zaštitu podataka**[30]**.** Osim toga, samocertificirana poduzeća podliježu nadležnosti Savezne trgovinske komisije na temelju odjeljka 5. Zakona o Saveznoj trgovinskoj komisiji kojim su zabranjena nepoštena ili prijevarna djela ili postupci u trgovini ili koji utječu na trgovinu[31].

U izvješću iz 2004. izražena je zabrinutost u vezi provedbe programa „sigurne luke", odnosno u vezi s time da bi Savezna trgovinska komisija trebala biti proaktivnija u pokretanju istraga i podizanja svijesti pojedinaca o njihovim pravima. Drugo područje zabrinutosti odnosi se na manjak jasnoće u vezi s nadležnošću Savezne trgovinske komisije da provodi načela u pogledu podataka o ljudskim potencijalima.

Tijelo nadležno za pravnu zaštitu u slučaju pritužbi na korištenje podataka o ljudskim potencijalima – Europski odbor za zaštitu podataka – primilo je jednu pritužbu povezanu s podacima o ljudskim potencijalima[32]. Međutim, nedostatak pritužbi ne omogućava donošenje zaključka o potpunom funkcioniranju programa. Treba uvesti službene provjere poduzeća u smislu poštovanja načela radi potvrđivanja stvarne primjene preuzetih obveza zaštite podataka. Europska tijela za zaštitu podataka isto bi tako trebala poduzeti mjere za podizanje svijesti o postojanju Odbora.

Naglašeni su i problemi u vezi s načinom na koji alternativni mehanizmi pravne zaštite funkcioniraju kao tijela za provedbu obveza. Određeni broj tih tijela ne raspolaže odgovarajućim sredstvima za pružanje pravne zaštite u slučajevima nepoštovanja načela. Taj je nedostatak potrebno riješiti.

5.1. Savezna trgovinska komisija

Savezna trgovinska komisija može poduzeti mjere provedbe u slučaju kada poduzeća krše obveze „sigurne luke". Kada je „sigurna luka" uspostavljena, Savezna trgovinska komisija preuzela je obvezu prioritetnog razmatranja svih obavijesti o nepoštovanju načela upućenih od tijela država članica EU-a[33]. Budući da prvih deset godina sporazuma nije primljena nijedna pritužba, Savezna trgovinska komisija odlučila je pokušati utvrditi kršenja načela „sigurne luke" u svakoj istrazi o zaštiti privatnosti i sigurnosti podataka koju provodi. Od 2009. Savezna trgovinska komisija provela je 10 postupaka protiv poduzeća na temelju kršenja načela „sigurne luke". Ti su postupci uglavnom riješeni nagodbama – uz značajne kazne – kojima se zabranjuje lažno prikazivanje, uključujući poštovanje načela „sigurne luke", i kojima se poduzećima određuje provođenje sveobuhvatnih programa zaštite privatnosti i prihvaćanje revizija u razdoblju od 20 godina. Poduzeća na zahtjev Savezne trgovinske komisije moraju prihvatiti neovisno ocjenjivanje njihovih programa zaštite privatnosti. O tim se ocjenama redovito obavješćuje Saveznu trgovinsku komisiju. Nalozima Savezne

---

30 Europski odbor za zaštitu podataka je tijelo nadležno za istraživanje i rješavanje pritužbi koje su podnijeli pojedinci u slučaju navodnog nepoštovanja načela „sigurne luke" od strane poduzeća iz SAD-a koje je član „sigurne luke". Poduzeća koja certificiraju načela „sigurne luke" moraju odabrati neovisni mehanizam pravne zaštite ili suradnju s Europskim odborom za zaštitu podataka kako bi riješile probleme koji proizlaze iz nepoštovanja načela „sigurne luke". Međutim, suradnja s Europskim odborom za zaštitu podataka obvezna je u slučaju kada poduzeće iz SAD-a obrađuje osobne podatke o ljudskim potencijalima koje se prenose iz EU-a u kontekstu radnog odnosa. Ako se poduzeće obveže na suradnju s Odborom, ono se isto tako mora obvezati da će postupati u skladu s bilo kojim savjetom Odbora ako Odbor smatra da poduzeće treba izvršiti određenu radnju da bi poštovalo načela „sigurne luke", uključujući mjere za zaštitu prava ili naknadu štete.

31 Ministarstvo prometa SAD-a na temelju glave 49. odjeljka 41712 Zakonika Sjedinjenih Američkih Država ima sličnu nadležnost nad zračnim prijevoznicima.

32 Pritužbu je podnio švicarski državljanin te ju je zato Europski odbor za zaštitu podataka uputio švicarskom tijelu za zaštitu podataka (SAD ima odvojeni program „sigurne luke" za Švicarsku).

33 Vidi Prilog V. Odluci Komisije 2000/520/EZ od 26. srpnja 2000.

trgovinske komisije isto je tako tim poduzećima zabranjeno lažno prikazivanje njihove politike zaštite okoliša i njihova sudjelovanja u „sigurnoj luci" ili sličnim programima zaštite privatnosti. To je na primjer bio slučaj u istragama Savezne trgovinske komisije protiv Googlea, Facebooka i Myspacea.[34] Google je 2012. pristao platiti novčanu kaznu u iznosu od 22,5 milijuna USD kako bi riješio pritužbe da je prekršio odredbe o zaštiti privatnosti korisnika. Savezna trgovinska komisija u svim istragama u pogledu zaštite privatnosti službeno provjerava postoji li kršenje načela „sigurne luke".

Savezna trgovinska komisija nedavno je ponovila svoje izjave i preuzimanje obveze prioritetnog razmatranja svih proslijeđenih obavijesti primljenih od poduzeća koja sama reguliraju privatnost i država članica EU-a o navodnom nepoštovanju načela „sigurne luke".[35] U zadnje tri godine Savezna trgovinska komisija primila je samo nekoliko takvih obavijesti od europskih tijela za zaštitu podataka.

Transatlantska se suradnja tijela za zaštitu podataka u zadnjim mjesecima počela razvijati. Na primjer, 26. lipnja 2013. Savezna trgovinska komisija i Ured povjerenika za zaštitu podataka Irske potpisali su Memorandum o razumijevanju o uzajamnoj pomoći u provedbi zakonodavstva o zaštiti osobnih podataka u privatnom sektoru. Tim se memorandumom uspostavlja okvir za povećanu, unaprijeđenu i učinkovitiju suradnju u području provedbe zakonodavstva o privatnosti[36].

U kolovozu 2013. Savezna trgovinska komisija najavila je daljnje jačanje provjera poduzeća koja kontroliraju velike baze osobnih podataka. Isto je tako pokrenula portal na kojem potrošači mogu podnijeti pritužbu u vezi s nekim poduzećem iz SAD-a[37].

Savezna trgovinska komisija bi isto tako trebala povećati napore u istraživanju lažnih tvrdnji o poštovanju načela „sigurne luke". Poduzeće koje na svojem *web*-mjestu tvrdi da ispunjava zahtjeve „sigurne luke", ali ga Ministarstvo trgovine ne navodi kao „sadašnjeg" člana programa, time zavarava potrošače i zloupotrebljava njihovo povjerenje. Lažnim tvrdnjama oslabljuje se vjerodostojnost cijelog sustava i stoga bi trebale biti bez odlaganja uklonjene s *web*-mjesta takvih poduzeća. Poduzeća bi trebala biti obvezana provedivim zahtjevom da ne zavaravaju potrošače. Savezna trgovinska komisija trebala bi nastaviti u naporima da utvrdi lažne tvrdnje o poštovanju načela „sigurne luke" kao u predmetu *Karnani*, kada je Savezna trgovinska komisija zatvorila kalifornijsko *web*-mjesto zbog lažne tvrdnje o članstvu u „sigurnoj luci" te zbog prijevarne prakse u e-trgovanju usmjerene na europske potrošače[38].

Savezna trgovinska komisija je 29. listopada 2013. objavila otvaranje „brojnih istraga o poštovanju načela ‚sigurne luke' tijekom prošlih mjeseci" i da se po ovom pitanju može očekivati još mjera provedbe obveza „u nadolazećim mjesecima". Savezna trgovinska komisija isto je tako potvrdila da je „posvećena traženju načina da unaprijedi svoju učinkovitost" te želi „nastaviti s prihvaćanjem svih značajnih tragova, poput nedavne pritužbe odvjetnika za prava potrošača iz Europe o velikom broju navodnih prekršaja povezanih sa

---

34 Tijekom razdoblja 2009. – 2012. Savezna je trgovinska komisija okončala deset postupaka provedbe obveza preuzetih u sklopu „sigurne luke": FTC protiv Javian Karnani, and Balls of Kryptonite, LLC (2009.), World Innovators, Inc. (2009.), Expat Edge Partners, LLC (2009.), Onyx Graphics, Inc. (2009.), Directors Desk LLC (2009.), Progressive Gaitways LLC (2009.), Collectify LLC (2009.), Google Inc. (2011.), Facebook, Inc. (2011.), Myspace LLC (2012.). Vidi: „Federal Trade Commission of Safe Harbour Commitments": http://export.gov/build/groups/public/@eg_main/@SafeHarbour/documents/webcontent/eg_main_052211.pdf Vidi i: „Case Highlights": http://business.ftc.gov/us-eu-Safe-Harbour-framework. Većina tih predmeta uključivala je probleme s poduzećima koja su se pridružila „sigurnoj luci" i onda se nastavila predstavljati kao članovi bez obnove godišnje certifikacije.

35 Preuzimanje je te obveze ponovljeno na sastanku članice Savezne trgovinske komisije Julie Brill s europskim tijelima za zaštitu podataka (Radna skupina iz članka 29.) u Bruxellesu 17. travnja 2013.

36 http://www.dataprotection.ie/viewdoc.asp?Docid=1317&Catid=66&StartDate=1+January+2013&m=n

37 Potrošači mogu podnijeti pritužbu koristeći Federal Trade Commission Complaint Assistant (https://www.ftccomplaintassistant.gov/), a međunarodni potrošači mogu podnijeti pritužbu na econsumer.gov (http://www.econsumer.gov).

38 http://www.ftc.gov/os/caselist/0923081/090806karnanicmpt.pdf

‚sigurnom lukom'".[39] Agencija se isto tako obvezala na „sustavno praćenje sukladnosti s nalozima ‚sigurne luke', kao što to činimo sa svim našim nalozima"[40].

Savezna trgovinska komisija je 12. studenoga 2013. obavijestila Europsku komisiju da „**ako je politikom zaštite privatnosti nekog poduzeća obećana zaštita prema načelima ‚sigurne luke', tada propust tog poduzeća da se registrira ili obnovi registraciju ne može, sam po sebi, biti razlogom za izuzimanje tog poduzeća od mjera Savezne trgovinske komisije u pogledu provedbe tih obveza preuzetih u okviru ‚sigurne luke'"[41].**

U studenome 2013. Ministarstvo trgovine obavijestilo je Europsku komisiju da „kako bi pomoglo u osiguravanju da poduzeća ne daju ‚lažne tvrdnje' o sudjelovanju u ‚sigurnoj luci', Ministarstvo trgovine odlučilo je pokrenuti postupak kontaktiranja sudionika u ‚sigurnoj luci' mjesec dana prije njihova datuma za ponovnu certifikaciju u svrhu opisivanja koraka koje moraju slijediti ako se ne žele ponovno certificirati". **Ministarstvo trgovine** „**upozorit će poduzeća** u ovoj kategoriji da uklone sve navode i upućivanja na sudjelovanje u ‚sigurnoj luci', uključujući korištenje certifikacijske oznake ‚sigurne luke', iz politika zaštite privatnosti i *web*-mjesta poduzeća, **i jasno ih obavijestiti da svaki propust u postupanju prema tom nalogu može poduzeća podvrgnuti mjerama Savezne trgovinske komisije u pogledu provedbe tih obveza**"[42].

Kako bi spriječili lažne tvrdnje o poštovanju načela „sigurne luke", *web*-mjesta s politikama zaštite privatnosti samocertificiranih poduzeća trebala bi uvijek sadržavati poveznicu na *web*-mjesto Ministarstva trgovine o „sigurnoj luci" gdje su navedeni svi „sadašnji" članovi programa. Time će se osobama iz Europe čiji se podaci obrađuju omogućiti da odmah, bez dodatnog pretraživanja, provjere je li poduzeće trenutačno član „sigurne luke". Ministarstvo trgovine je u ožujku 2013. počelo slati takve zahtjeve poduzećima, ali je taj postupak potrebno pojačati.

Kontinuirano praćenje i posljedična provedba stvarnog pridržavanja načela „sigurne luke" od strane Savezne trgovinske komisije – uz prethodno navedene mjere koje je poduzelo Ministarstvo trgovine – ostaje glavni prioritet za osiguravanje pravilnog i učinkovitog funkcioniranja programa. Osobito je potrebno povećati broj **službenih provjera i istraga poduzeća** u smislu poštovanja načela „sigurne luke". Isto je tako potrebno nastaviti olakšavati upućivanje pritužbi Saveznoj trgovinskoj komisiji u vezi s kršenjem načela.

5.2. Europski odbor za zaštitu podataka

Europski odbor za zaštitu podataka je tijelo osnovano na temelju Odluke o „sigurnoj luci". Ono je ovlašteno istraživati pritužbe pojedinaca koje se odnose na zaštitu osobnih podataka prikupljanih u kontekstu radnog odnosa te predmete povezane s certificiranim poduzećima koja su odabrala tu mogućnost za rješavanje sporova u okviru „sigurne luke" (53% svih poduzeća). Sastoji se od predstavnika raznih tijela za zaštitu podataka iz EU-a.

Do danas je Odbor primio četiri pritužbe (dvije u 2010. i dvije u 2013.). Dvije su pritužbe iz 2010. upućene nacionalnim tijelima za zaštitu podataka (UK i Švicarska). Treća i četvrta pritužba trenutačno su u postupku razmatranja. Mali broj pritužbi može se objasniti činjenicom da su ovlasti Odbora, kako je prethodno navedeno, prvenstveno ograničene na određenu vrstu podataka.

---

39 http://www.ftc.gov/speeches/brill/131029europeaninstituteremarks.pdf i http://www.ftc.gov/speeches/ramirez/131029tacdremarks.pdf

40 Pismo predsjednice Savezne trgovinske komisije Edith Ramirez potpredsjednici Viviane Reding.

41 Pismo predsjednice Savezne trgovinske komisije Edith Ramirez potpredsjednici Viviane Reding.

42 „Suradnja SAD-a i EU-a u svrhu provedbe okvira ‚sigurne luke'" 12.studenoga 2013.

Ograničeni broj predmeta Odbora isto bi se tako mogao objasniti manjkom svijesti o postojanju Odbora.+ Komisija je od 2004. učinila vidljivijima informacije o Odboru na svojem *web*-mjestu[43].

Kako bi poboljšali način korištenja Odbora, poduzeća iz SAD-a koja su odabrala suradnju s Odborom i poštovanje njegovih odluka za neke ili sve kategorije osobnih podataka obuhvaćene njihovom samocertifikacijom trebala bi to jasno i trajno naznačiti u svojim politikama zaštite privatnosti čime Ministarstvu trgovine daju pravo nadzora tog aspekta njihovih preuzetih obveza. Treba kreirati posebnu stranicu na *web*-mjestu svakog tijela za zaštitu podataka iz EU-a posvećenu „sigurnoj luci" s ciljem podizanja svijesti europskih poduzeća i osoba čiji se podaci obrađuju o „sigurnoj luci"**.**

5.3. Poboljšanje provedbe

Prethodno utvrđene slabosti u transparentnosti i slabosti u provedbi izazivaju zabrinutost među europskim poduzećima o negativnom utjecaju programa „sigurne luke" na konkurentnost europskih poduzeća. U slučaju kada se europsko poduzeće natječe s poduzećem iz SAD-a koje djeluje u okviru „sigurne luke", ali u praksi ne primjenjuje njezina načela, europsko je poduzeće u konkurentski nepovoljnom položaju u odnosu na poduzeće iz SAD-a.

Nadalje, nadležnošću Savezne trgovinske komisije obuhvaćene su nepravedne ili prijevarne radnje ili postupci „u trgovini ili koji utječu na trgovinu". U odjeljku 5. Zakona o Saveznoj trgovinskoj komisiji utvrđena su izuzeća iz nadležnosti Savezne trgovinske komisije nad nepoštenim ili prijevarnim radnjama ili postupcima s obzirom na, između ostalog, **telekomunikacije.** Budući da su izvan ovlasti Savezne trgovinske komisije, telekomunikacijskim poduzećima nije dozvoljeno pristupanje „sigurnoj luci". Međutim, rastućim približavanjem tehnologija i usluga brojni su njihovi neposredni konkurenti na tržištu informacijskih i komunikacijskih tehnologija u SAD-u članovi „sigurne luke". Isključivanje telekomunikacijskih poduzeća iz razmjene podataka u okviru programa „sigurne luke" razlog je zabrinutosti nekih europskih telekomunikacijskih operatora. Prema mišljenju Udruženja europskih telekomunikacijskih operatora (*European Telecommunications Network Operators' Association* - ETNO) „to je u izravnom sukobu s najvažnijim zahtjevom telekomunikacijskih operatora o potrebi osiguranja ravnopravnog tržišnog natjecanja"[44].

6. JAČANJE NAČELA PRIVATNOSTI „SIGURNE LUKE"

6.1. Alternativno rješavanje sporova

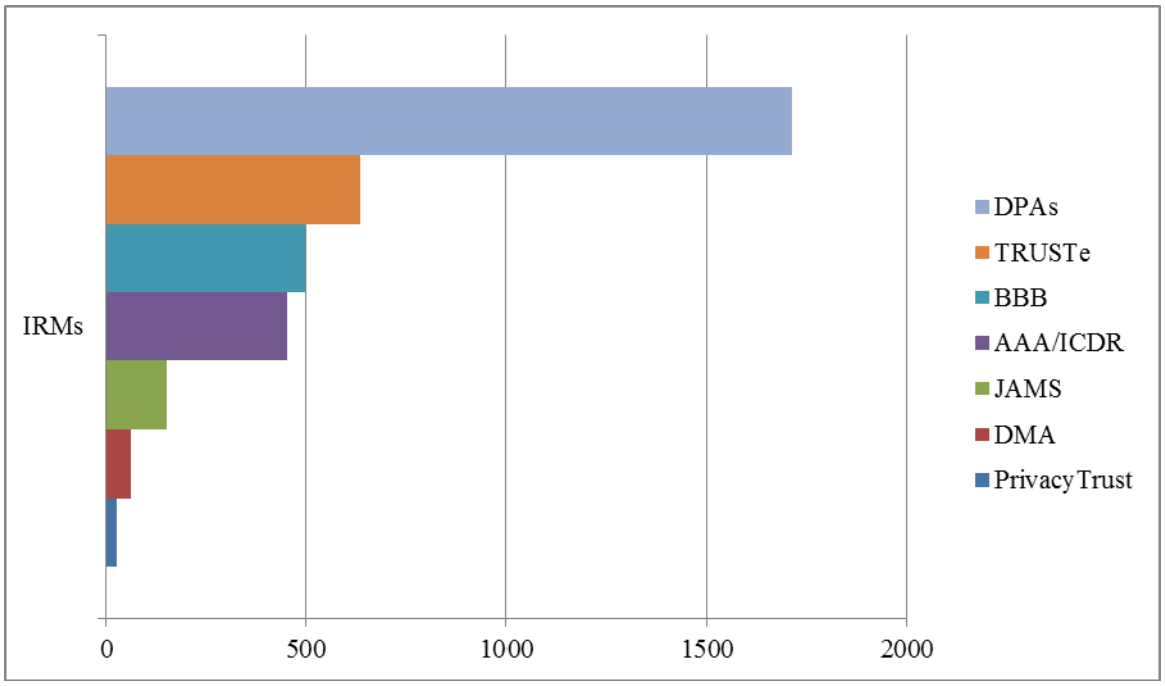
Načelom provedbe utvrđeno je da moraju postojati „**lako dostupni i prihvatljivi mehanizmi pravne zaštite** prema kojima se svaka pritužba pojedinca i spor istražuje". U tu je svrhu u okviru programa „sigurne luke" uspostavljen sustav alternativnog rješavanja sporova (ADR)

---

43 U skladu s izvješćem iz 2004., na *web*-mjestu Komisije (GU Justice) objavljena je Obavijest u obliku pitanja i odgovora o Europskom odboru za zaštitu podataka u svrhu podizanja svijesti pojedinaca i pomoći u podnošenju pritužbe ako smatraju da su njihovi osobni podaci obrađeni uz kršenje načela „sigurne luke": http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_Safe_harbour_en.pdf
Standardni obrazac za pritužbe dostupan je na: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/ complaint_form_en.pdf

44 U dokumentu „Razmatranja ETNO-a" koji su službe Komisije primile 4. listopada 2013. isto se tako raspravlja o 1) definiciji osobnih podataka u „sigurnoj luci", 2) manjku praćenja u okviru „sigurne luke", i 3) činjenici da „poduzeća iz SAD-a mogu prenositi podatke s puno manje ograničenja od njihovih europskih konkurenata" što „predstavlja jasnu diskriminaciju europskih poduzeća i utječe na konkurentnost europskih poduzeća". Prema pravilima „sigurne luke", pri otkrivanju podataka trećoj osobi organizacije moraju primjenjivati načela obavijesti i mogućnosti izbora. Ako organizacija želi prenijeti podatke trećoj osobi koja ima ulogu posrednika, može to učiniti ako se prvo uvjeri da se treća osoba obvezala na načela ili podliježe direktivi ili nekoj drugoj potvrdi o primjerenosti, ili ako sklopi pisani sporazum s tom trećom osobom u kojem se zahtijeva da treća osoba pruži barem istu razinu zaštite privatnosti koju traže relevantna načela.

od neovisne treće strane[45] s ciljem pružanja brzih rješenja sporova pojedincima. Najvažnija tri tijela u okviru mehanizama pravne zaštite su Europski odbor za zaštitu podataka, BBB (Better Business Bureaus) i TRUSTe.



Korištenje alternativnog rješavanja sporova povećava se od 2004., a Ministarstvo trgovine ojačalo je praćenje američkih pružatelja usluga alternativnog rješavanja sporova kako bi osiguralo da su informacije koje navode o postupku pritužbe jasne, dostupne i razumljive. Međutim, učinkovitost ovog sustava tek treba biti dokazana zbog do sada ograničenog broja riješenih predmeta[46].

Unatoč tome što je Ministarstvo trgovine bilo uspješno u smanjivanju naknada koju naplaćuju pružatelji usluga alternativnog rješavanja sporova, dva od sedam glavnih pružatelja usluga alternativnog rješavanja sporova još uvijek naplaćuju naknadu pojedincima za podnošenje pritužbe[47]. To predstavlja približno 20 % pružatelja usluga alternativnog rješavanja sporova koje koriste poduzeća u „sigurnoj luci". Ta su poduzeća odabrala pružatelja usluga alternativnog rješavanja sporova koji potrošačima naplaćuju naknadu za podnošenje pritužbe. Takve prakse nisu u skladu s načelom provedbe „sigurne luke" kojim se pojedincima daje

45 U Direktivi 2013/11/EU o alternativnom rješavanju sporova za potrošačke sporove naglašena je važnost neovisnih, nepristranih, transparentnih, učinkovitih, brzih i poštenih postupaka alternativnog rješavanja sporova.

46 Na primjer, jedan od glavnih pružatelja usluga („TRUSTe") izjavio je da su u 2010. primili 881 zahtjev, ali samo su tri zahtjeva ocijenjeni kao prihvatljivi i utemeljeni te su doveli do toga da je predmetno poduzeće moralo izmijeniti svoju politiku zaštite privatnosti i *web*-mjesto. U 2011. broj je pritužbi bio 879, a u jednom je predmetu poduzeću bilo naloženo da izmjeni svoju politiku zaštite privatnosti. Prema Ministarstvu trgovine velika većina tih pritužbi tijelima za ADR odnosi se na zahtjeve potrošača, primjerice korisnika koji su zaboravili svoju zaporku te je nisu mogli dobiti od pružatelja internetskih usluga. Nakon zahtjeva Komisije Ministarstvo trgovine pripremilo je nove statističke podatke o kriterijima koje trebaju koristiti sva tijela za alternativnog rješavanja sporova. Njima se razdvajaju obični zahtjevi i pritužbe te daju daljnja pojašnjenja o vrstama zaprimljenih pritužbi. Međutim, o tim je kriterijima potrebna daljnja rasprava kako bi se osiguralo da novi statistički podaci u 2014. obuhvaćaju sve pružatelje usluga alternativnog rješavanja sporova, usporedivi su i pružaju ključne informacije za procjenu učinkovitosti mehanizma pravne zaštite.

47 Međunarodni centar za rješavanje sporova / Američko udruženje za arbitražu (*International Centre for Dispute Resolution* - ICDR / *American Arbitration Association* - AAA) naplaćuju 200 USD, a JAMS 250 USD kao „naknadu za podnošenje pritužbe". Ministarstvo trgovine obavijestilo je Komisiju da je s AAA-om, najskupljim pružateljem usluga rješavanja sporova za pojedince, radilo na razvoju posebnog programa za „sigurnu luku" kojim je trošak za potrošače smanjen s nekoliko tisuća dolara na jedinstvenu cijenu od 200 USD.

pravo na pristup „lako dostupnim i prihvatljivim neovisnim mehanizmima pravne zaštite". U Europskoj uniji pristup neovisnoj službi za rješavanje sporova koju osigurava Europski odbor za zaštitu podataka besplatan je za sve osobe čiji se podaci obrađuju.

Ministarstvo trgovine potvrdilo je 12. studenoga 2013. da „će nastaviti zastupati prava na privatnost građana EU-a i raditi s pružateljima usluga alternativnog rješavanja sporova na utvrđivanju je li moguće dodatno smanjiti njihove naknade ".

U pogledu sankcija, određeni broj pružatelja usluga alternativnog rješavanja sporova ne raspolaže potrebnim alatima za pružanje pravne zaštite u slučajevima nepoštovanja načela privatnosti. Nadalje, između niza sankcija i mjera svih pružatelja usluga alternativnog rješavanja sporova ne nalazi se javno objavljivanje nalaza o nepoštovanju načela.

Od pružatelja usluga alternativnog rješavanja sporova isto se tako zahtijeva da predmete u kojima poduzeće ne poštuje ishod postupka usluga alternativnog rješavanja sporova ili odbije odluku pružatelja usluga alternativnog rješavanja sporova proslijedi Saveznoj trgovinskoj komisiji tako da ih ona može preispitati i istražiti te, prema potrebi, poduzeti mjere provedbe. Međutim do danas nije zabilježen niti jedan slučaj upućivanja predmeta od pružatelja usluga alternativnog rješavanja sporova Saveznoj trgovinskoj komisiji zbog nepoštovanja načela[48].

Pružatelji usluga alternativnog rješavanja sporova na svojim *web*-mjestima održavaju popise poduzeća (sudionici u rješavanju sporova) koji koriste njihove usluge. Time se potrošačima omogućava da lagano provjere može li pojedinac – u slučaju spora s poduzećem – pritužbu podnijeti utvrđenom pružatelju usluga rješavanja sporova. Tako na primjer pružatelj usluga rješavanja sporova BBB navodi sva poduzeća koja sudjeluju u sustavu BBB-a za rješavanje sporova. Međutim, postoje brojna poduzeća koja tvrde da sudjeluju u određenom sustavu za rješavanje sporova, ali ih pružatelji usluga alternativnog rješavanja sporova ne navode kao sudionike u svojim programima za rješavanje sporova[49].

Mehanizmi alternativnog rješavanja sporova trebaju biti lako dostupni, neovisni i prihvatljivi za pojedince. Osoba čiji se podaci obrađuju trebala bi moći podnijeti pritužbu bez ikakvih prekomjernih ograničenja. Sva bi tijela za alternativno rješavanje sporova trebala na svojim *web*-mjestima objaviti statističke podatke o broju riješenih pritužbi te posebne informacije o njihovu ishodu. Naposljetku, potreban je daljnji nadzor tijela za alternativno rješavanje sporova kako bi se osiguralo da su informacije koje navode o postupku i načinu podnošenja pritužbe jasne i razumljive, tako da rješavanje sporova postane učinkovit i pouzdan mehanizam koji daje rezultate. Isto je tako potrebno ponoviti da bi javno objavljivanje nalaza o nepoštovanju načela trebalo biti uključeno među obvezne sankcije tijela za alternativno rješavanje sporova.

6.2. Daljnji prijenos

Eksponencijalnim rastom protoka podataka nastaje potreba za daljnjim osiguravanjem zaštite osobnih podataka u svim fazama obrade podataka, osobito ako poduzeće koje poštuje načela „sigurne luke" podatke prenosi nekoj **trećoj osobi koja obrađuje podatke**. Stoga se potreba za boljom provedbom „sigurne luke" ne odnosi samo na članove „sigurne luke" već i na podugovaratelje.

---

48 Vidi često postavljano pitanje 11.

49 Primjeri: Amazon je obavijestio Ministarstvo trgovine da kao svojeg pružatelja usluga rješavanja sporova koristi BBB. Međutim, BBB ne navodi Amazon među svojim sudionicima u rješavanju sporova. Suprotno tome, Arsalon Technologies (www.arsalon.net), pružatelj internetskih usluga u oblaku, pojavljuje se na popisu BBB-a za rješavanje sporova u vezi sa „sigurnom lukom", ali poduzeće nije sadašnji član „sigurne luke" (stanje na dan 1. listopada 2013.). BBB, TRUSTe i drugi pružatelji usluga alternativnog rješavanja sporova trebali bi ukloniti ili ispraviti tvrdnje o certifikaciji poduzeća. Oni bi trebali biti obvezani provedivim zahtjevom da certificiraju samo poduzeća koja su članovi „sigurne luke".

Programom „sigurne luke” omogućavaju se daljnji prijenosi podataka trećim osobama koje imaju ulogu „posrednika” ako se poduzeće – koje je član „sigurne luke” – „uvjeri da se treća osoba obvezala na načela ili podliježe direktivi ili nekoj drugoj potvrdi o primjerenosti, ili ako sklopi pisani sporazum s tom trećom osobom u kojem se zahtijeva da treća osoba pruži barem istu razinu zaštite privatnosti koju traže načela privatnosti”[50]. Na primjer, Ministarstvo trgovine od pružatelja usluga računalstva u oblaku zahtijeva sklapanje ugovora čak i ako je „usklađen sa sigurnom lukom” i prima osobne podatke za obradu[51]. Međutim, ta odredba nije jasna u Prilogu II. Odluci o „sigurnoj luci”.

Kako se pravna zaštita podugovaratelja značajno povećala tijekom proteklih godina, osobito u kontekstu računalstva u oblaku, pri sklapanju takvog ugovora poduzeće u „sigurnoj luci” trebalo bi obavijestiti Ministarstvo trgovine i biti obvezno javno objaviti odredbe o zaštiti privatnosti[52].

Potrebna su daljnja pojašnjenja u odnosu na tri prethodno navedena pitanja: mehanizam alternativnog rješavanja sporova, pojačani nadzor i daljnji prijenos podataka.

7. PRISTUP PODACIMA PRENESENIM U OKVIRU PROGRAMA „SIGURNE LUKE”

Tijekom 2013. informacije o razmjeru i opsegu programa nadzora SAD-a izazvale su pitanja o kontinuitetu zaštite osobnih podataka koji su zakonito preneseni u SAD na temelju programa „sigurne luke”. Na primjer, pokazalo se da su sva poduzeća uključena u program PRISM, koja nadležnim tijelima SAD-a omogućavaju pristup pohranjenim i obrađenim podacima u SAD-u, članovi „sigurne luke”. To je učinilo program „sigurne luke” jednim od kanala kojim je obavještajnim agencijama SAD-a omogućen pristup prikupljanju podataka koji su prvotno obrađeni u EU-u.

U Odluci o „sigurnoj luci”, Prilogu 1., propisano je da pridržavanje načela privatnosti može biti ograničeno ako je to opravdano zahtjevima nacionalne sigurnosti, javnog interesa, ili provedbe zakona; ili zakonom, vladinom uredbom ili sudskom praksom. Kako bi ograničenja i zabrane uživanja temeljnih prava bile valjane, one moraju biti usko definirane, moraju biti navedene u zakonu dostupnom javnosti i moraju biti nužne i razmjerne u demokratskom društvu. U Odluci o „sigurnoj luci” posebno je navedeno da su takva ograničenja dopuštena **„u onoj mjeri koja je potrebna”** da se ispune zahtjevi nacionalne sigurnosti, javnog interesa, ili provedbe zakona[53]. Dok su iznimni slučajevi obrade podataka za potrebe nacionalne sigurnosti, javnog interesa ili provedbe zakona predviđeni programom „sigurne luke”,

---

50 Vidi Odluku Komisije 2000/250/EZ, str. 7. (daljnji prijenos).

51 Vidi: „*Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing*”: http://export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_main_060351.pdf

52 Ove se primjedbe odnose na pružatelje usluga računalstva u oblaku koji nisu članovi „sigurne luke”. Prema konzultantskoj kući Galexia „razina je članstva (i poštovanja načela) u ‚sigurnoj luci’ među pružateljima usluga u oblaku prilično visoka. Pružatelji usluga u oblaku obično imaju višestruke razine zaštite privatnosti, koje često uključuju izravne ugovore s klijentima i ‚krovne’ politike zaštite privatnosti. Uz jednu ili dvije važne iznimke, pružatelji usluga u oblaku u ‚sigurnoj luci’ poštuju ključne odredbe u vezi s rješavanjem sporova i provedbom. Trenutačno na popisu poduzeća s lažnim članstvom nema velikih pružatelja usluga *u oblaku*.” (izjava Chrisa Connollya iz Galexije u sklopu istrage Odbora za građanske slobode, pravosuđe i unutarnje poslove o „elektroničkom masovnom nadzoru građana EU-a”).

53 Vidi Prilog 1. Odluci o „sigurnoj luci”: „Pridržavanje ovih načela može biti ograničeno: (a) u onoj mjeri koja je potrebna da se ispune zahtjevi nacionalne sigurnosti, javnog interesa, ili zahtjevi za provedbu zakona; (b) zakonom, vladinom uredbom ili sudskom praksom koji proizvode proturječne obveze ili izričita dopuštenja, ako pri korištenju takvog dopuštenja organizacija može dokazati da je njezino nepoštovanje načela ograničeno u mjeri potrebnoj da se ostvare pretežući zakoniti interesi koje podupire takvo dopuštenje; ili (c) ako direktiva ili nacionalno pravo države članice predviđa iznimke ili odstupanja, uz uvjet da se takve iznimke ili odstupanja primjenjuju u sličnim kontekstima. U skladu s ciljem povećanja zaštite privatnosti, organizacije trebaju nastojati u potpunosti i transparentno provoditi ova načela, uključujući i tako da u svojim postupcima zaštite privatnosti navode kada će se redovito primjenjivati iznimke od načela, dopuštene u prethodno opisanom slučaju (b). Iz istog razloga, ako je mogućnost odabira dopuštena prema načelima i/ili zakonodavstvu SAD-a, očekuje se da se organizacije odluče za veću zaštitu tamo gdje je moguće.”

masovni se razmjer pristupa obavještajnih agencija podacima prenesenim u SAD u kontekstu komercijalnih transakcija u vrijeme usvajanja „sigurne luke" nije mogao predvidjeti.

Nadalje, iz razloga transparentnosti i pravne sigurnosti Ministarstvo trgovine trebalo bi obavijestiti Europsku komisiju o svim zakonskim ili vladinim propisima koji bi mogli utjecati na poštovanje načela privatnosti „sigurne luke"[54]. Uporabu izuzeća od načela treba pozorno pratiti, a ona ne smiju biti korištena na način kojim se narušava zaštita koju pružaju **načela**[55]**.** Osobito, masovnim razmjerom pristupa agencija SAD-a podacima koje obrađuju samocertificirana poduzeća u „sigurnoj luci" dovodi se u pitanje povjerljivost elektronske komunikacije.

7.1. Razmjernost i nužnost

Iz nalaza *ad hoc* radne skupine EU-a i SAD-a za zaštitu podataka proizlazi da u zakonima SAD-a postoji niz pravnih osnova temeljem kojih je dopušteno masovno prikupljanje i obrada osobnih podataka koje poduzeća iz SAD-a pohranjuju ili na drugi način obrađuju. To može uključivati podatke koji su prethodno preneseni iz EU-a u SAD u okviru programa „sigurne luke", čime se postavlja pitanje kontinuiteta poštovanja načela „sigurne luke". Masovni razmjer tih programa može dovesti do toga da agencije SAD-a pristupaju podacima prenesenim u sklopu „sigurne luke" i dalje ih obrađuju izvan okvira onog što je nužno potrebno i razmjerno u odnosu na zaštitu nacionalne sigurnosti kako je predviđena izuzećem iz Odluke o „sigurnoj luci".

7.2. Ograničenja i mogućnosti pravne zaštite

Iz nalaza *ad hoc* radne skupine EU-a i SAD-a za zaštitu podataka proizlazi da se zaštita koju pružaju zakoni SAD-a odnosi uglavnom na državljane SAD-a ili osobe s dozvolom boravka u SAD-u. Nadalje, ne postoje mogućnosti da osobe čiji se podaci obrađuju, bilo iz EU-a ili SAD-a, dobiju mogućnost pristupa, ispravljanja ili brisanja podataka ili administrativnu ili sudsku pravnu zaštitu u vezi s prikupljanjem i daljnjom obradom njihovih osobnih podataka koja se odvija u okviru programa nadzora SAD-a.

7.3. Transparentnost

Poduzeća u svojim politikama zaštite privatnosti često ne navode u kojim slučajevima primjenjuju izuzeća od načela. Time pojedinci i poduzeća nisu svjesni onog što se događa s njihovim podacima. To je od osobite važnosti u odnosu na djelovanje predmetnih programa nadzora SAD-a. Kao rezultat toga, Europljani čiji se podaci prenose poduzeću u SAD-u u okviru „sigurne luke" vjerojatno od tih poduzeća nisu obaviješteni da se može omogućiti pristup njihovim podacima[56]. Time se postavlja pitanje poštovanja načela „sigurne luke" o transparentnosti. Transparentnost treba biti osigurana u najvećoj mogućoj mjeri kojom se ne ugrožava nacionalna sigurnost. Uz postojeće zahtjeve za poduzeća da u svojim politikama zaštite privatnosti navedu u kojim slučajevima načela mogu biti ograničena zakonom, vladinom uredbom ili sudskom praksom, poduzeća treba isto tako potaknuti da u svojim

---

54 Mišljenje 4/2000 o razini zaštite koju pružaju načela „sigurne luke", koje je 16. svibnja 2000. usvojila Radna skupina za zaštitu podataka iz članka 29.

55 Mišljenje 4/2000 o razini zaštite koju pružaju načela „sigurne luke", koje je 16. svibnja 2000. usvojila Radna skupina za zaštitu podataka iz članka 29.

56 Neka europska poduzeća u „sigurnoj luci" pružaju relativno transparentne informacije po ovom pitanju. Na primjer Nokia, koja posluje u SAD-u i član je „sigurne luke", u svojoj politici zaštite privatnosti navodi sljedeću obavijest: *„Možemo biti zakonski obvezni vaše osobne podatke otkriti određenim nadležnim tijelima ili trećim osobama, na primjer tijelima kaznenog progona u zemljama u kojima mi ili treće osobe koje nastupaju u naše ime djeluju."*

politikama zaštite privatnosti navedu u kojim slučajevima primjenjuju izuzeća od načela u svrhu ispunjavanja zahtjeva nacionalne sigurnosti, javnog interesa, ili provedbe zakona.

8. ZAKLJUČCI I PREPORUKE

Od njegova donošenja 2000. program „sigurne luke" postao je sredstvo za protok osobnih podataka između EU-a i SAD-a. Važnost učinkovite zaštite u slučaju prijenosa osobnih podataka povećala se zbog eksponencijalnog rasta protoka podataka koji su ključni za digitalno gospodarstvo te vrlo značajnih razvoja u prikupljanju, obradi i korištenju podataka. Internetska poduzeća kao što su Google, Facebook, Microsoft, Apple i Yahoo imaju stotine milijuna klijenata u Europi i prenose osobne podatke na obradu u SAD u razmjeru koji je 2000., kada je uspostavljena „sigurna luka", bio nezamisliv.

Zbog nedostataka u transparentnosti i provedbi sporazuma još uvijek postoje određeni problemi koji bi trebali biti riješeni:

transparentnost politika zaštite privatnosti članova „sigurne luke";

učinkovita primjena načela privatnosti od strane poduzeća iz SAD-a; i

učinkovitost provedbe zakona.

Nadalje, **masovni razmjer pristupa obavještajnih agencija podacima koje u SAD prenose certificirana poduzeća „sigurne luke"** izaziva dodatna ozbiljna pitanja o kontinuitetu prava na zaštitu podataka Europljana pri prijenosu njihovih podataka u SAD.

Iz prethodno navedenih razloga Komisija je utvrdila sljedeće **preporuke**:

Transparentnost

Samocertificirana poduzeća trebala bi javno objaviti svoje politike zaštite privatnosti. Nije dovoljno da poduzeća Ministarstvu trgovine dostave opis svoje politike zaštite privatnosti. Politike zaštite privatnosti trebaju biti napisane jasnim i jednostavnim jezikom i dostupne javnosti na *web*-mjestima poduzeća.

Web-mjesta s politikama zaštite privatnosti samocertificiranih poduzeća trebala bi uvijek sadržavati poveznicu na web-*mjesto Ministarstva trgovine o „sigurnoj luci" gdje su navedeni svi „sadašnji" članovi programa.* Time će se osobama iz Europe čiji se podaci obrađuju omogućiti da odmah, bez dodatnog pretraživanja, provjere je li poduzeće trenutačno član „sigurne luke". To bi pomoglo u povećanju vjerodostojnosti programa smanjivanjem mogućnosti za lažne tvrdnje o poštovanju načela „sigurne luke"**.** Ministarstvo trgovine je u ožujku 2013. počelo slati takve zahtjeve poduzećima, ali je taj postupak potrebno pojačati.

Samocertificirana poduzeća trebala bi objaviti uvjete zaštite privatnosti svih ugovora sklopljenih s podugovarateljima tj. pružateljima usluga računalstva u oblaku. Programom „sigurne luke" dopušteni su daljnji prijenosi podataka od samocertificiranih poduzeća u „sigurnoj luci" trećim osobama koje imaju ulogu „posrednika", primjerice pružateljima usluga u oblaku. Prema našem shvaćanju, u takvim slučajevima Ministarstvo trgovine od samocertificiranih poduzeća zahtijeva sklapanje ugovora. Međutim, pri sklapanju takvog ugovora poduzeće u „sigurnoj luci" o tome bi isto tako trebalo obavijestiti Ministarstvo trgovine i biti obvezno javno objaviti odredbe o zaštiti privatnosti.

Na web-mjestu Ministarstva trgovine jasno označiti sva poduzeća koja su bivši članovi programa. Oznaka „bivši član" na popisu poduzeća članova „sigurne luke" Ministarstva trgovine treba biti popraćena jasnim upozorenjem da poduzeće trenutačno ne ispunjava zahtjeve „sigurne luke". Međutim, u slučaju statusa „bivši član" poduzeće je obvezno

nastaviti primjenjivati zahtjeve „sigurne luke” na podatke koji su primljeni tijekom članstva u „sigurnoj luci”.

Pravna zaštita

Politike zaštite privatnosti na web-mjestima poduzeća trebaju sadržavati poveznicu na pružatelja usluga alternativnog rješavanja sporova i/ili Europski odbor za zaštitu podataka. Time će se osobama iz Europe čiji se podaci obrađuju omogućiti da u slučaju problema odmah kontaktiraju pružatelja usluga alternativnog rješavanja sporova ili Europski odbor. Ministarstvo trgovine je u ožujku 2013. počelo slati takve zahtjeve poduzećima, ali je taj postupak potrebno pojačati.

Alternativno rješavanje sporova trebalo bi biti lako dostupno i prihvatljivo. Neka tijela za alternativno rješavanje sporova u programu „sigurne luke” nastavljaju pojedincima naplaćivati naknade – koje mogu biti prilično skupe za pojedinačnog korisnika – za rješavanje pritužbe (200 – 250 USD). Suprotno tome, u Europi je pristup Odboru za zaštitu podataka koji je predviđen za rješavanje pritužbi besplatan.

Ministarstvo trgovine trebalo bi provoditi sustavniji nadzor pružatelja usluga alternativnog rješavanja sporova u odnosu na transparentnost i dostupnost informacija koje pružaju o postupku koji koriste i popratnim radnjama koje provode u vezi s pritužbama. Time bi rješavanje sporova postalo učinkovit i pouzdan mehanizam koji daje rezultate. Isto tako treba ponoviti da bi javno objavljivanje nalaza o nepoštovanju načela trebalo biti uključeno među obvezne sankcije tijela za alternativno rješavanje sporova.

Provedba

Nakon certifikacije ili ponovne certifikacije poduzeća u okviru „sigurne luke”, određeni broj tih poduzeća trebalo bi biti predmet službenih istraga stvarnog poštovanja svojih politika zaštite privatnosti (izvan okvira provjere sukladnosti s formalnim zahtjevima).

U slučaju utvrđivanja nepoštovanja načela, koje je uslijedilo nakon pritužbe ili istrage, poduzeće bi trebalo biti predmet posebne popratne istrage nakon 1 godine.

U slučaju sumnje na nepoštovanje nekog poduzeća ili pritužbi u tijeku, Ministarstvo trgovine trebalo bi o tome obavijestiti nadležno tijelo za zaštitu podataka iz EU-a.

Treba nastaviti istrage lažnih tvrdnji o pridržavanju načela „sigurne luke”. Poduzeće koje na svojem *web*-mjestu tvrdi da ispunjava zahtjeve „sigurne luke”, ali ga Ministarstvo trgovine ne navodi kao „sadašnjeg” člana programa, time zavarava potrošače i zloupotrebljava njihovo povjerenje. Lažne tvrdnje oslabljuju vjerodostojnost cijelog sustava i stoga bi trebale biti bez odlaganja uklonjene s *web*-mjesta takvih poduzeća.

Pristup nadležnih tijela SAD-a

Politike zaštite privatnosti samocertificiranih poduzeća trebale bi sadržavati informacije o mjeri u kojoj zakoni SAD-a dopuštaju tijelima javne vlasti prikupljanje i obradu podataka prenesenih u okviru „sigurne luke”. Poduzeća treba osobito potaknuti da u svojim politikama zaštite privatnosti navedu u kojim slučajevima primjenjuju izuzeća od načela u svrhu ispunjavanja zahtjeva nacionalne sigurnosti, javnog interesa, ili provedbe zakona.

Važno je da se izuzeće zbog nacionalne sigurnosti koje je predviđeno „sigurnom lukom" koristi samo u mjeri koja je nužno potrebna ili razmjerna.