



EVROPSKA KOMISIJA

Bruselj, 25.1.2012
COM(2012) 9 final

**SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU, SVETU, EVROPSKEMU
EKONOMSKO-SOCIALNEMU ODBORU IN ODBORU REGIJ**

**Varovanje zasebnosti v povezanem svetu
Evropski okvir varstva podatkov za 21. stoletje**

(Besedilo velja za EGP)

[\[...\]](#)

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU, SVETU, EVROPSKEMU EKONOMSKO-SOCIALNEMU ODBORU IN ODBORU REGIJ

Varovanje zasebnosti v povezanem svetu Evropski okvir varstva podatkov za 21. stoletje

(Besedilo velja za EGP)

1. DANAŠNJI IZZIVI VARSTVA PODATKOV

Hitri razvoj tehnologije in globalizacija sta močno spremenila način vse bolj obsežnega zbiranja osebnih podatkov, dostopanja do njih, njihove uporabe in njihovega prenosa. Novi načini izmenjave informacij preko družabnih omrežij in oddaljeno shranjevanja velikih količin podatkov so postali del življenja mnogih od 250 milijonov uporabnikov interneta v Evropi. Hkrati pa so osebni podatki postali izjemno pomembni za številna podjetja. Zbiranje, združevanje in analiziranje podatkov potencialnih strank je pogosto zelo pomemben del njihovih gospodarskih dejavnosti¹.

V tem novem digitalnem okolju **imajo posamezniki pravico do učinkovitega nadzora nad svojimi osebnimi podatki**. Varstvo podatkov je temeljna pravica v Evropi, vsebovana v členu 8 Listine Evropske unije o temeljnih pravicah in tudi v členu 16(1) Pogodbe o delovanju Evropske unije (PDEU), zato jo je treba ustrezno zaščititi.

Zaradi pomanjkanja zaupanja potrošniki oklevajo pri spletnih nakupih in pri sprejemanju novih storitev. Zato je visoka raven varstva podatkov bistvena tudi za krepitev zaupanja v spletne storitve ter za izpolnitev potenciala digitalnega gospodarstva, s čimer se spodbujata **gospodarska rast in konkurenčnost industrijskih panog EU**.

Potrebna so sodobna, skladna pravila za vso EU za prost pretok podatkov iz ene države članice v drugo. Podjetja potrebujejo jasna in enotna pravila, ki bodo zagotavljala pravno varnost in zmanjševala upravno breme. To je bistvenega pomena za delovanje enotnega trga ter za **spodbujanje gospodarske rasti, ustvarjanje novih delovnih mest in spodbujanje inovacij**². Posodobitev evropskih predpisov o varstvu podatkov, ki krepi razsežnost varstva podatkov na enotnem trgu, zagotavlja visoko raven varstva podatkov za posameznike ter spodbuja pravno varnost, jasnost in doslednost, zato ima varstvo podatkov osrednjo vlogo v stockholmskem akcijskem

¹ Trg za analizo zelo velikih količin podatkov se v svetu letno poveča za 40 odstotkov: http://www.mckinsey.com/mgi/publications/big_data/.

² Glej tudi sklepe Evropskega sveta z dne 23. oktobra 2011, v katerih sta poudarjeni „ključna vloga“ enotnega trga „pri zagotavljanju rasti in zaposlovanja“ ter potreba po oblikovanju digitalnega enotnega trga do leta 2015.

načrtu Evropske komisije³ in v Evropski digitalni agendi⁴ ter, v širšem smislu, prispeva k strategiji EU za rast (Evropa 2020⁵).

Evropska direktiva iz leta 1995⁶, osrednji zakonodajni akt varstva osebnih podatkov v Evropi, je pomenila prelomnico v zgodovini varstva podatkov. Njena cilja, zagotoviti delujoč enotni trg ter učinkovito zaščito temeljnih pravic in svoboščin posameznikov, veljata tudi danes. Vendar pa je bila ta direktiva sprejeta pred 17 leti, ko je bil internet še v povojih. V današnjem novem digitalnem okolju, polnem izzivov, veljavna pravila ne zagotavljajo niti potrebnega usklajevanja niti potrebne učinkovitosti za zagotavljanje pravice do varstva osebnih podatkov. Evropska komisija zato zdaj predlaga korenito reformo evropskega okvira varstva podatkov.

Poleg tega je Lizbonska pogodba s členom 16 PDEU ustvarila novo pravno podlago za posodobljen in celovit pristop k varstvu podatkov in prostemu pretoku osebnih podatkov, tudi na področju policijskega sodelovanja in pravosodnega sodelovanja v kazenskih zadevah⁷. Ta pristop se odraža v sporočilu Evropske komisije o stockholmskem programu in stockholmskem akcijskem načrtu⁸, ki poudarja, da mora Unija „vzpostaviti celovit sistem varstva osebnih podatkov, v katerem bodo zajete vse pristojnosti Unije“, in „zagotoviti dosledno uporabo pravice do varstva podatkov“.

Da bi na pregleden način pripravila reformo evropskega okvira varstva podatkov, Komisija že od leta 2009 organizira javna posvetovanja o varstvu podatkov⁹ in se intenzivno dogovarja z zainteresiranimi stranmi.¹⁰ Komisija je 4. novembra 2010 objavila sporočilo z naslovom „Celovit pristop k varstvu osebnih podatkov v Evropski uniji“¹¹, ki navaja glavne poudarke reforme. Od septembra do decembra 2011 je vodila tudi poglobljeno razpravo z evropskimi nacionalnimi organi za varstvo podatkov in evropskim nadzornikom za varstvo podatkov, da bi proučila možnosti za doseganje doslednejše uporabe evropskih predpisov o varstvu podatkov v vseh državah članicah EU¹².

³ COM(2010) 171 konč.

⁴ COM(2010) 245 konč.

⁵ COM(2010) 2020 konč.

⁶ Direktiva 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL L 281, 23.11.1995, str. 31).

⁷ Posebna pravila za obdelavo s strani držav članic na področju skupne zunanje in varnostne politike bodo določena s sklepom Sveta na podlagi člena 39 PEU.

⁸ COM(2009) 262 oziroma COM(2010) 171.

⁹ Organizirani sta bili dve javni posvetovanji o reformi varstva podatkov: eno posvetovanje je potekalo od julija do decembra 2009 (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm), drugo pa od novembra 2010 do januarja 2011 (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm).

¹⁰ Usmerjena posvetovanja so v letu 2010 potekala z organi držav članic in zainteresiranimi stranmi iz zasebnega sektorja. Novembra 2010 je evropska komisarka za pravosodje Viviane Reding organizirala okroglo mizo o reformi varstva podatkov. V letu 2011 so potekali tudi delavnice in seminarji o posebnih temah (npr. obvestila o kršitvi varstva podatkov).

¹¹ COM(2010) 609.

¹² Glej dopis evropske komisarke za pravosodje Viviane Reding z dne 19. septembra 2011 članom delovne skupine iz člena 29, objavljen na naslovu http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm.

Ti pogovori so jasno pokazali, da državljani in podjetja od Evropske komisije pričakujejo korenito reformo evropskih predpisov o varstvu podatkov. Po oceni učinka različnih političnih možnosti¹³ Evropska komisija zdaj predlaga **trden in dosleden zakonodajni okvir politik Unije, ki krepi pravice posameznikov in razsežnost varstva podatkov na enotnem trgu ter zmanjšuje birokracijo za podjetja**¹⁴. Komisija predlaga, naj novi okvir sestavljata:

- **uredba** (ki bo nadomestila Direktivo 95/46/ES) o splošnem okviru EU za varstvo podatkov¹⁵;
- in **direktiva** (ki bo nadomestila Okvirni sklep 2008/977/PNZ¹⁶) o pravilih varstva osebnih podatkov, ki se obdelujejo za namene **preprečevanja, odkrivanja, preiskovanja ali pregona kaznivih dejanj in povezanih pravosodnih dejavnosti**.

To sporočilo navaja glavne elemente reforme evropskega okvira varstva podatkov.

2. POSAMEZNIKI NAJ IMAJO NADZOR NAD SVOJIMI OSEBNIMI PODATKI

Na podlagi Direktive 95/46/ES, ki je danes glavni evropski zakonodajni akt na področju varstva podatkov, načini, ki so posameznikom na voljo za izvajanje njihove pravice do varstva podatkov, niso dovolj usklajeni v vseh državah članicah. Prav tako niso dovolj usklajena pooblastila nacionalnih organov za varstvo podatkov, da bi omogočala dosledno in učinkovito uporabo predpisov. To pomeni, da je dejansko izvajanje teh pravic težje v nekaterih državah članicah kot v drugih, še zlasti na spletu.

Te težave je moč pripisati tudi ogromni količini podatkov, ki se zberejo vsak dan, in pa dejstvu, da se uporabniki ne zavedajo popolnoma, da se njihovi podatki zbirajo. Čeprav je veliko Evropejcev mnenja, da je razkritje osebnih podatkov vedno bolj del sodobnega življenja¹⁷, 72 % uporabnikov interneta v Evropi še vedno meni, da morajo na spletu navesti preveč osebnih podatkov¹⁸. Pestí jih občutek, da nimajo nadzora nad svojimi podatki. Ne dobijo namreč dovolj informacij o tem, kaj se zgodi

¹³ Glej oceno učinka SEC(2012)72

¹⁴ To bo pozneje vključevalo spremembe za prilagoditev posebnih in sektorskih pravnih aktov, na primer Uredbe ES št. 45/2001 (UL L 8, 12.1.2001, str. 1).

¹⁵ Uredba uvaja tudi omejeno število tehničnih sprememb Direktive o e-zasebnosti (Direktiva 2002/58/ES, kakor je bila nazadnje spremenjena z Direktivo 2009/136/ES, UL L 337, 18.12.2009, str. 11), da se bo upoštevala pretvorba Direktive 95/46/ES v uredbo. Materialnopravne posledice nove uredbe in nove direktive za Direktivo o e-zasebnosti bodo pravočasno predmet pregleda Komisije, ki bo upoštevala rezultate pogajanj o pripravljenih predlogih z Evropskim parlamentom in Svetom.

¹⁶ Okvirni sklep 2008/977/PNZ z dne 27. novembra 2008 o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah (UL L 350, 30.12.2008, str. 60). Poročilo o izvajanju Okvirnega sklepa s strani držav članic (COM(2012)12) se sprejme kot del svežnja reform varstva podatkov.

¹⁷ Glej posebno raziskavo Eurobarometra 359 – Odnosi do varstva podatkov in elektronske identitete v Evropski uniji (*Attitudes on Data Protection and Electronic Identity in the European Union*), junij 2011, str. 23.

¹⁸ Prav tam, str. 54.

z njihovimi osebnimi podatki, komu vse se ti posredujejo in v kakšne namene. Pogosto sploh ne vedo, kako lahko na spletu uveljavijo svoje pravice.

„Pravica biti pozabljen“

Nek evropski študent, uporabnik spletne storitve družabnega mreženja, se je odločil, da bo zahteval dostop do vseh svojih osebnih podatkov, ki jih ima to spletno omrežje. Pri tem je odkril, da družabno omrežje zbira precej več podatkov, kot je mislil, in da so nekateri osebni podatki, ki jih je bil izbrisal, še vedno shranjeni.

Reforma evropskih predpisov o varstvu podatkov bo zagotovila, da se to ne bo več dogajalo, in sicer z uvedbo:

– izrecne zahteve, ki spletne storitve družabnega mreženja (in vse druge upravljavce obdelave podatkov) obvezuje, naj zmanjšajo obseg osebnih podatkov uporabnikov, ki jih zbirajo in obdelujejo;

– zahteve, da privzete nastavitve ne omogočajo javnega dostopanja do podatkov;

– izrecne obveznosti za upravljavce obdelave podatkov, da izbrišejo osebne podatke posameznika, če zadevni posameznik izrecno zahteva izbris in ko ni drugega utemeljenega razloga za hrambo teh podatkov.

V zadevnem primeru bi moral ponudnik družabnega omrežja takoj in v celoti izbrisati vse študentove podatke.

Kot je poudarjeno v Evropski digitalni agendi, so pomisleki v zvezi z zasebnostjo med najpogostejšimi razlogi, zakaj ljudje ne kupujejo blaga in storitev na spletu. Glede na prispevek sektorja informacijske in komunikacijske tehnologije (IKT) k splošni rasti produktivnosti v Evropi – 20 % neposredno iz sektorja IKT in 30 % iz naložb v IKT¹⁹ – je zaupanje v take storitve izredno pomembno za spodbujanje rasti v gospodarstvu EU in za konkurenčnost evropske industrije.

Obvestila o kršitvi varnosti podatkov

Hakerji so vdrl v igralno storitev, namenjeno uporabnikom v EU. Kršitev se je nanašala na podatkovne zbirke osebnih podatkov (tudi imena, naslove in morda celo podatke o kreditnih karticah) več deset milijonov uporabnikov po vsem svetu. Podjetje je prizadete uporabnike o tem obvestilo šele po enem tednu.

Reforma evropskih predpisov o varstvu podatkov bo zagotovila, da se to ne bo več dogajalo. Nova predpisa bosta podjetja zavezovala:

- k boljšim varnostnim ukrepom za preprečevanje kršitev in izogibanje kršitvam;

- k obveščanju o kršitvah varnosti podatkov tako nacionalnih organov za varstvo podatkov – po možnosti v 24 urah od odkritja kršitve – kot tudi prizadetih posameznikov, in sicer nemudoma.

Cilj novih zakonodajnih aktov, ki jih predlaga Komisija, je okrepiti pravice, dati ljudem na voljo učinkovita in delujoča orodja, ki jim bodo zagotavljala, da bodo v celoti seznanjeni s tem, kaj se dogaja z njihovimi osebnimi podatki, in jim omogočali učinkovitejše uveljavljanje pravic.

¹⁹

Glej Evropsko digitalno agendo, citat, str. 4.

Komisija za okrepitev pravice posameznikov do varstva podatkov predlaga nova predpisa, ki bosta:

izboljšala zmožnost posameznikov, da nadzorujejo svoje podatke, in sicer z:

- zagotavljanjem, da je njihovo **soglasje**, ko se to zahteva, **podano izrecno, kar pomeni, da temelji bodisi na izjavi bodisi na jasnem konkludentnem ravnanju zadevne osebe** in je podano prostovoljno;
- dajanjem uporabnikom interneta učinkovito **pravico biti pozabljen** v spletnem okolju: pravico, da se njihovi podatki izbrišejo, če uporabniki svoje soglasje umaknejo in če ni drugih utemeljenih razlogov za hrambo podatkov;
- zagotavljanjem **posamezniku enostavnega dostopa do lastnih podatkov in pravice do prenosljivosti podatkov**: pravice do pridobitve kopije shranjenih podatkov od upravljavca in možnosti, da uporabnik podatke prenese od enega ponudnika storitev k drugemu, brez kakršnih koli ovir;
- krepitevijo **pravice do obveščenosti**, tako da posamezniki v celoti razumejo, kako se njihovi osebni podatki obdelujejo, zlasti takrat, ko se dejavnosti obdelave nanašajo na **otroke**;
izboljšala načine, na katere bodo posamezniki uveljavljali svoje pravice, in sicer s:

- krepitevijo **neodvisnosti in pooblastil nacionalnih organov za varstvo podatkov**, tako da bodo ti lahko ustrezno in učinkovito obravnavali pritožbe, imeli pooblastila za izvajanje učinkovitih preiskav, sprejemali zavezujoče odločitve ter nalagali učinkovite in odvračilne sankcije;
- krepitevijo **upravnega in sodnega varstva**, kadar so **kršene** pravice do varstva podatkov. Zlasti bodo lahko strokovna združenja v imenu posameznika vložila tožbo pri sodišču;

okrepila varnost podatkov, in sicer s:

- spodbujanjem uporabe **tehnologij za boljše varovanje zasebnosti** (tehnologij, ki varujejo zasebnost informacij z zmanjševanjem obsega shranjevanja osebnih podatkov), **privzetih nastavitvev, ki upoštevajo spoštovanje zasebnosti, in shem potrjevanja zasebnosti**;
- uvedbo **splošne obveznosti**²⁰ upravljavcev obdelave podatkov, **da morajo o kršitvah varnosti podatkov nemudoma obvestiti** tako organe za varstvo podatkov (ki jih je treba po možnosti obvestiti v 24 urah), kot tudi prizadete posameznike;

povečala odgovornost tistih, ki obdelujejo podatke, zlasti na naslednje načine:

- upravljavci obdelave podatkov bodo morali imenovati **uradno osebo za varstvo podatkov** v podjetjih z več kot 250 zaposlenimi in v podjetjih, ki se ukvarjajo z dejavnostmi obdelave, ki zaradi svoje narave, obsega in namenov

²⁰

To je trenutno obvezno samo v telekomunikacijskem sektorju na podlagi Direktive o e-zasebnosti.

pomenijo posebno tveganje za pravice in svoboščine posameznikov („tvegana obdelava“);

– uvedeno bo **načelo „vgrajene zasebnosti“**, s čimer bo zagotovljeno upoštevanje zaščitnih ukrepov za varstvo podatkov v fazi načrtovanja postopkov in sistemov;

– uvedena bo obveznost izvajanja **ocen učinka varstva podatkov** za organizacije, ki se ukvarjajo s tvegano obdelavo.

3. PREDPISA O VARSTVU PODATKOV, PRIMERNA ZA DIGITALNI ENOTNI TRG

Kljub veljavnemu cilju Direktive v zvezi z zagotavljanjem enake ravni varstva podatkov v EU se predpisi v različnih državah članicah še vedno precej razlikujejo. Posledično se morajo upravljavci obdelave podatkov ukvarjati s 27 različnimi nacionalnimi zakonodajami in zahtevami. Rezultat tega je **razdrobljeno pravno okolje**, ki je ustvarilo **pravno negotovost** in neenako zaščito za posameznike. To je podjetjem povzročilo **nepotrebne stroške in upravna bremena** ter deluje odvračilno na podjetja, ki delujejo na enotnem trgu in morda želijo svojo dejavnost razširiti preko nacionalnih meja.

Viri in pooblastila nacionalnih organov za varstvo podatkov se med državami članicami močno razlikujejo²¹. V nekaterih primerih svojih nalog ne morejo zadovoljivo opraviti. Sodelovanje med temi organi na evropski ravni – preko obstoječe svetovalne skupine (tako imenovane delovne skupine iz člena 29)²² – ne privede vedno do doslednega izvajanja nalog in ga je prav tako treba izboljšati.

Dosledno izvajanje predpisov o varstvu podatkov v Evropi

Multinacionalno podjetje z več poslovalnicami v EU je v Evropi začelo uporabljati sistem spletnega kartiranja, ki zbira posnetke vseh zasebnih in javnih zgradb, lahko pa posname tudi ljudi na ulici. V neki državi članici je vključitev nezamegljenih slik oseb, ki niso vedele, da so jih fotografirali, veljala za nezakonito, v drugi državi članici pa ni šlo za tako kršitev predpisov s področja varstva podatkov. Posledično ni bilo skladnega odziva nacionalnih organov za varstvo podatkov za odpravo posledic tega dejanja.

Reforma evropskih predpisov o varstvu podatkov bo zagotovila, da se to v prihodnosti ne bo več dogajalo, saj:

– bodo zahteve v zvezi z varstvom podatkov in zaščitni ukrepi določeni z uredbo EU z neposredno uporabo v vsej Uniji;

– bo le tisti organ za varstvo podatkov, ki je pristojen na območju sedeža matičnega podjetja, pristojen za odločanje o tem, ali je ravnanje podjetja v zakonodajnih okvirih;

²¹ Več podrobnosti v zvezi s tem je mogoče najti v oceni učinka, priloženi pravnim predlogom, SEC(2012) 72.

²² Delovna skupina iz člena 29 je bila ustanovljena leta 1996 (s členom 29 Direktive 95/46/ES). Ima svetovalno vlogo ter je sestavljena iz predstavnikov nacionalnih nadzornih organov za varstvo podatkov, evropskega nadzornika za varstvo podatkov in Komisije. Več informacij o njenih dejavnosti je mogoče najti na naslovu http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

– bo hitro in učinkovito usklajevanje med nacionalnimi organi za varstvo podatkov – glede na to, da je storitev usmerjena na posameznike v več državah članicah – pomagalo zagotoviti, da bosta nova evropska predpisa o varstvu podatkov veljala dosledno v vseh državah članicah in se tako tudi izvajala.

Pristojnosti nacionalnih organov je treba okrepiti in izboljšati njihovo sodelovanje, da se zagotovita dosledno izvajanje in, ne nazadnje, enotna uporaba predpisov v vsej EU.

Trden, jasen in enoten zakonodajni okvir na evropski ravni bo pomagal razviti potencial digitalnega enotnega trga ter spodbudil gospodarsko rast, inovacije in ustvarjanje novih delovnih mest. Uredba bo odpravila razdrobljenost pravnih ureditev v 27 državah članicah in odstranila ovire za vstop na trg, kar je še posebej pomembno za mikro, mala in srednje velika podjetja.

Nova predpisa bosta evropskim podjetjem dala tudi globalno konkurenčno prednost. V okviru reformiranega pravnega okvira bodo lahko svojim strankam zagotovila, da bodo dragoceni osebni podatki obdelani s potrebno skrbnostjo in previdnostjo. Zaupanje v skladno evropsko pravno ureditev bo za ponudnike storitev ključnega pomena, za vlagatelje, ki med umeščanjem storitev iščejo optimalne pogoje, pa dobra spodbuda.

Za okrepitev **razsežnosti varstva podatkov na enotnem trgu** Komisija predlaga naslednje:

– določitev pravil varstva podatkov na evropski ravni s pomočjo **uredbe, ki se bo neposredno uporabljala v vseh državah članicah**²³, kar bo preprečilo nadaljnjo kumulativno in sočasno uporabo različnih nacionalnih predpisov s področja varstva podatkov. To bo **že z vidika upravnih bremen podjetjem prineslo okoli 2,3 milijarde EUR neto prihrankov letno**;

– **poenostavitev zakonodajnega okolja z drastičnim zmanjšanjem birokracije** in odpravo **formalnosti**, kot so splošne zahteve glede obveščanja (kar bo privedlo do neto prihrankov v višini 130 milijonov EUR na leto že samo z vidika upravnih bremen). Zaradi pomena mikro, malih in srednje velikih podjetij za konkurenčnost evropskega gospodarstva je posebna pozornost posvečena njihovim posebnim potrebam;

– **nadaljnjo krepitev neodvisnosti in pristojnosti nacionalnih organov za varstvo podatkov**, tako da bodo ti lahko izvajali preiskave, sprejemali zavezujoče odločitve ter nalogali učinkovite in odvratilne kazenske sankcije, države članice pa jim bodo morale za to zagotoviti **zadostna sredstva**;

– **vzpostavitev sistema „vse na enem mestu“ za varstvo podatkov v EU**: upravljavci obdelave podatkov v EU se bodo obračali na le **en organ za varstvo**

²³

Predlagana direktiva naj bi določila pravila, veljavna na področjih policijskega sodelovanja in pravosodnega sodelovanja v kazenskih zadevah (glej točko 4), kar bo državam članicam omogočilo večjo prožnost na tem področju.

podatkov, in sicer na organ v tisti državi članici, v kateri je sedež matičnega podjetja;

– ustvarjanje pogojev za **hitro in učinkovito sodelovanje med organi za varstvo podatkov**, vključno z obveznostjo organa za varstvo podatkov v zvezi z izvedbo preiskav in inšpekcijskih pregledov, če to od njega zahteva drug organ za varstvo podatkov, ter za medsebojno priznavanje odločitev organov;

– **vzpostavitev mehanizma usklajenosti** na ravni EU, da se zagotovi, da so v odločitvah organa za varstvo podatkov, ki imajo širši učinek v Evropi, v celoti upoštevana mnenja drugih zadevnih organov za varstvo podatkov in da so odločitve popolnoma skladne z zakonodajo EU;

– nadgraditev delovne skupine iz člena 29 v **neodvisni evropski odbor za varstvo podatkov**, da bi se izboljšal njen prispevek k dosledni uporabi zakonodaje s področja varstva podatkov in da bi se zagotovila močna podlaga za sodelovanje med organi za varstvo podatkov, vključno z evropskim nadzornikom za varstvo podatkov, ter da bi se izboljšale sinergije in učinkovitost, z napovedjo, da bo evropski nadzornik za varstvo podatkov zagotovil sekretariat evropskemu odboru za varstvo podatkov.

Nova uredba EU bo zagotovila trdno zaščito temeljne pravice do varstva podatkov v vsej Evropski uniji in okrepila delovanje enotnega trga. Hkrati bodo – glede na dejstvo, da (kot je poudarilo Sodišče EU²⁴), pravica do varstva osebnih podatkov ni absolutna, temveč jo je treba obravnavati glede na vlogo, ki jo ima v družbi,²⁵ in jo uravnotežiti z drugimi temeljnimi pravicami v skladu z načelom sorazmernosti²⁶ – v Uredbi izrecne določbe, ki bodo zagotovile spoštovanje drugih temeljnih pravic, kot so pravica do svobode izražanja in obveščanja ter pravica do obrambe, pa tudi pravica do poklicne molčečnosti (kot velja za pravno stroko), brez poseganja v status cerkva po zakonih držav članic.

4. UPORABA PODATKOV V POLICIJSKEM SODELOVANJU IN PRAVOSODNEM SODELOVANJU V KAZENSKIH ZADEVAH

Začetek veljavnosti Lizbonske pogodbe in zlasti uvedba nove pravne podlage (člen 16 PDEU) omogočata vzpostavitev celovitega okvira varstva podatkov, ki bo zagotavljal visoko raven varstva podatkov posameznikov, obenem pa bo upošteval posebno naravo področij policijskega sodelovanja in pravosodnega sodelovanja v kazenskih zadevah. Zlasti omogoča, da prenovljeni okvir varstva podatkov EU ureja

²⁴ Sodba Sodišča EU z dne 9. novembra 2010 v združenih zadevah C-92/09 in C-93/09, Volker und Markus Schecke in Eifert, ZOdl. 2010, še ni uradno objavljena.

²⁵ V skladu s členom 52(1) Listine mora biti kakršno koli omejevanje uresničevanja pravice do varstva podatkov predpisano z zakonom ter mora spoštovati bistveno vsebino pravice in svoboščin, ob upoštevanju načela sorazmernosti pa je dovoljeno samo, če je potrebno in če dejansko ustreza ciljem splošnega interesa, ki jih priznava Evropska unija, ali če je potrebno zaradi zaščite pravic in svoboščin drugih.

²⁶ Sodba Sodišča EU z dne 6. novembra 2003 v zadevi C-101/01, Lindqvist, Recueil 2003, str. I-12971, točke 82–90; sodba z dne 16. decembra 2008 v zadevi C-73/07, Satamedia, ZOdl. 2008, str. I-9831, točke 50–62.

čezmejno in nacionalno obdelavo osebnih podatkov. To bi zmanjšalo razlike v zakonodaji držav članic, kar bi verjetno prispevalo k vsesplošnemu varstvu osebnih podatkov. Lahko bi tudi pripomoglo k lažji izmenjavi informacij med policijskimi in pravosodnimi organi držav članic ter s tem izboljšalo sodelovanje na področju boja proti težjim oblikam kriminala v Evropi. Obdelavo podatkov s strani policijskih in pravosodnih organov v kazenskih zadevah trenutno ureja predvsem Okvirni sklep 2008/977/PNZ, ki pa je začel veljati pred Lizbonsko pogodbo. Komisija ne more uveljavljati njegovih pravil, saj gre za okvirni sklep, to pa je prispevalo k zelo neenakomernemu izvajanju. Poleg tega je področje uporabe tega okvirnega sklepa omejeno na čezmejne dejavnosti obdelave.²⁷ To pomeni, da evropski predpisi, ki urejajo tako obdelavo in varujejo temeljno pravico do varstva podatkov, trenutno ne zajemajo obdelave osebnih podatkov, ki niso predmet izmenjav. To v nekaterih primerih za policijske in druge organe pomeni praktične težave, saj morda ne vedo, ali gre za obdelavo podatkov na nacionalni ali čezmejni ravni; prav tako pa ne morejo predvideti, ali bodo „nacionalni“ podatki postali predmet poznejše čezmejne izmenjave.²⁸

Cilj novega, reformiranega evropskega okvira varstva podatkov je torej zagotoviti dosledno in visoko raven varstva podatkov, **da se izboljša medsebojno zaupanje med policijskimi in pravosodnimi organi različnih držav članic ter s tem še okrepi prosti pretok podatkov in učinkovito sodelovanje med policijskimi in pravosodnimi organi.**

Komisija za zagotovitev boljšega varstva osebnih podatkov na področjih policijskega sodelovanja in pravosodnega sodelovanja v kazenskih zadevah ter pospešitev izmenjave osebnih podatkov med policijskimi in pravosodnimi organi držav članic v okviru svežnja reform varstva podatkov predlaga direktivo, ki bo:

- **določila splošna načela varstva podatkov** za policijsko sodelovanje in pravosodno sodelovanje v kazenskih zadevah, ob upoštevanju posebne narave teh področij;²⁹
- zagotavljala **minimalna usklajena merila in pogoje za morebitne omejitve** splošnih pravil. To se nanaša zlasti na pravice posameznikov do obveščenosti, kadar policijski in pravosodni organi obravnavajo njihove podatke ali dostopajo do njih. Take omejitve so potrebne za učinkovito preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj;
- določila **posebna pravila, ki bodo zajemala posebno naravo dejavnosti pregona, vključno z razlikovanjem med različnimi vrstami oseb, na katere se nanašajo osebni podatki** in katerih pravice se lahko razlikujejo (kot so priče in osumljenci).

²⁷ Natančneje, Okvirni sklep se uporablja za osebne podatke, ki se posredujejo oziroma so se že posredovali ali bili dani na voljo drugim državam članicam ali bili izmenjani med državami članicami in institucijami ali organi EU (glej člen 1(2)).

²⁸ To je potrdilo več držav članic v odgovorih na vprašalnik Komisije v zvezi s Poročilom o izvajanju Okvirnega sklepa (COM(2012)12).

²⁹ Primerjaj izjavo št. 21 o varstvu osebnih podatkov na področju pravosodnega sodelovanja v kazenskih zadevah in policijskega sodelovanja, priloženo Sklepni listini medvladne konference, na kateri je bila sprejeta Lizbonska pogodba.

5. VARSTVO PODATKOV V GLOBALIZIRANEM SVETU

Pravice posameznikov morajo biti zaščitene, kadar se osebni podatki prenesejo iz EU v tretje države ter kadar so posamezniki iz držav članic tarče in njihove podatke uporabljajo ali analizirajo ponudniki storitev iz tretjih držav. To pomeni, da morajo evropski standardi za varstvo podatkov veljati ne glede na zemljepisno lego podjetja ali njegove poslovalnice, ki obdeluje podatke.

V današnjem globaliziranem svetu se osebni podatki prenašajo prek vedno večjega števila virtualnih in zemljepisnih meja ter shranjujejo na strežnikih v različnih državah. Več podjetij nudi storitve računalništva v oblaku, ki strankam omogočajo dostop do podatkov in njihovo shranjevanje na oddaljenih strežnikih. Ti dejavniki so vzrok za izboljšave obstoječih mehanizmov za prenos podatkov v tretje države. To vključuje odločitve o ustreznosti – tj. odločitve, ki potrjujejo „ustrezne“ standarde za varstvo podatkov v tretjih državah – in ustrezne zaščitne ukrepe, kot so standardne pogodbenne klavzule ali zavezujoča poslovna pravila³⁰, da se zagotovi visoka raven varstva podatkov v mednarodnih postopkih obdelave in pospešijo čezmejni tokovi podatkov.

Zavezujoča poslovna pravila

Neka poslovna skupina mora redno posredovati osebne podatke iz svojih odvisnih podjetij v EU v svoja odvisna podjetja v tretjih državah. Skupina želi uvesti niz zavezujočih poslovnih pravil, da bi delovala skladno z zakonodajo EU, hkrati pa omejiti upravne zahteve za vsak posamezen prenos. V praksi zavezujoča poslovna pravila zagotavljajo, da za celotno skupino velja en niz pravil, in ne različne notranje pogodbe.

Na podlagi veljavnih praks, dogovorjenih na ravni delovne skupine iz člena 29, priznanje, da zavezujoča poslovna pravila podjetja zagotavljajo ustrezne zaščitne ukrepe, pomeni temeljit pregled s strani treh organov za varstvo podatkov (vodje in dveh revizorjev), vendar lahko pripombe podajo tudi drugi. Poleg tega veliko predpisov držav članic zahteva dodatna nacionalna dovoljenja za prenose, ki jih zajemajo zavezujoča poslovna pravila, zaradi česar je postopek njihovega sprejetja močno otežen, drag, dolgotrajen in zapleten.

Po reformi varstva podatkov:

- bo ta postopek poenostavljen in racionalnejši;*
- bo zavezujoča poslovna pravila potrjeval samo en organ za varstvo podatkov, z mehanizmi za zagotavljanje hitre vključitve drugih pristojnih organov za varstvo podatkov;*
- bodo zavezujoča poslovna pravila, ko jih bo organ odobril, veljala po vsej EU, dodatna dovoljenja na nacionalni ravni pa ne bodo potrebna.*

Za obravnavo izzivov globalizacije so potrebni prilagodljiva orodja in mehanizmi – še zlasti za podjetja, ki poslujejo po vsem svetu – hkrati pa je treba zagotoviti zaščito

³⁰

Zavezujoča poslovna pravila (BCR) so kodeks praks na podlagi evropskih standardov za varstvo podatkov, ki jih odobri vsaj en organ za varstvo podatkov ter ki jih organizacije pripravijo in upoštevajo prostovoljno, da zagotovijo ustrezne zaščitne ukrepe za vrste prenosov osebnih podatkov med podjetji, ki spadajo v isto poslovno skupino in jih ta pravila zavezujejo. Direktiva 95/46/ES jih izrecno ne zajema, vendar so se razvila v praksi med organi za varstvo podatkov, s podporo delovne skupine iz člena 29.

podatkov posameznikov brez kakršnih koli pravnih praznin. Komisija predlaga naslednje ukrepe:

- **jasna pravila**, ki bodo določala, kdaj se **zakonodaja EU uporablja za upravljavce obdelave podatkov s sedežem v tretjih državah**, zlasti z določitvijo veljavnosti evropskih pravil, kadar se blago in storitve ponujajo posameznikom v EU ali kadar se spremlja njihovo vedenje;
- vse **sklepe o ustreznosti** sprejme Evropska komisija na podlagi izrecnih in jasnih meril, tudi na področju policijskega sodelovanja in pravosodnega sodelovanja v kazenskih zadevah;
- zakoniti tokovi podatkov v tretje države bodo tekli bolj nemoteno zaradi okrepitve in poenostavitve **pravil o mednarodnih prenosih** v države, ki jih ne zajema nobena odločitev o ustreznosti, zlasti z racionalizacijo in razširitvijo uporabe orodij, kot so **zavezujoča poslovna pravila**, tako da jih bo mogoče uporabiti za **obdelovalce podatkov** in znotraj **skupin podjetij**, s čimer se bo bolje odražalo vedno večje število podjetij v dejavnostih obdelave podatkov, zlasti pri računalništvu v oblaku;
- začetek **dialoga** in, kjer je to primerno, **pogajanj** s tretjimi državami – zlasti strateškimi partnerji EU in državami evropske sosedске politike – in zadevnimi mednarodnimi organizacijami (kot so Svet Evrope, Organizacija za gospodarsko sodelovanje in razvoj ter Združeni narodi) za **spodbujanje visokih in interoperabilnih standardov za varstvo podatkov** po vsem svetu.

6. SKLEPNA UGOTOVITEV

Cilj reforme evropskih predpisov o varstvu podatkov je vzpostaviti **sodoben, trden, dosleden in celovit okvir varstva podatkov za Evropsko unijo**. Temeljna pravica posameznikov do varstva podatkov bo okrepljena. Spoštovane bodo tudi druge pravice, kot so pravica do svobode izražanja in obveščanja, pravice otrok, svoboda gospodarske pobude, pravica do nepristranskega sodišča ter pravica do poklicne molčečnosti (kot velja za pravno stroko), ter status cerkva po zakonih držav članic.

Reforma bo v prvi vrsti koristila posameznikom zaradi okrepitve njihovih pravic do varstva podatkov in njihovega zaupanja v digitalno okolje. Reforma bo poleg tega znatno poenostavila pravno okolje za podjetja in javni sektor. Pričakuje se, da bo to spodbudilo razvoj digitalnega gospodarstva na celotnem enotnem trgu EU in zunaj njegovih meja v skladu s cilji strategije Evropa 2020 in Evropske digitalne agende. Poleg tega bo reforma okrepila zaupanje med organi pregona za hitrejšo izmenjavo podatkov med njimi in sodelovanje na področju boja proti hudim kaznivim dejanjem, hkrati pa bo zagotovila visoko raven varstva posameznikov.

Evropska komisija bo tesno sodelovala z Evropskim parlamentom in Svetom za zagotovitev soglasja o novem evropskem okviru varstva podatkov do konca leta 2012. Med postopkom sprejemanja in pozneje, zlasti v okviru izvajanja novih pravnih aktov, bo Komisija vodila **poglobljen in pregleden dialog z vsemi zainteresiranimi stranmi**, ki vključujejo predstavnike iz zasebnega in javnega sektorja. To bo zajemalo predstavnike policijskih in pravosodnih organov, regulatorjev na področju elektronskih komunikacij, organizacij civilne družbe,

organov za varstvo podatkov in akademikov, pa tudi predstavnike specializiranih agencij EU, kot so Eurojust, Europol, Agencija za temeljne pravice ter Evropska agencija za varnost omrežij in informacij.

V luči nenehnega razvoja informacijskih tehnologij in razvijajočega se socialnega vedenja je tak dialog izjemno pomemben za izkoristek vloška, potrebnega za zagotovitev visoke ravni varstva podatkov posameznikov, rasti in konkurenčnosti industrijskih panog EU, operativne učinkovitosti javnega sektorja (vključno s policijo in sodstvom) ter nizke ravni upravnega bremena.