EVROPSKA KOMISIJA

Bruselj, 4.11.2010
COM(2010) 609 konč.

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

Celovit pristop k varstvu osebnih podatkov v Evropski uniji

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

„Celovit pristop k varstvu osebnih podatkov v Evropski uniji“

1. NOVI IZZIVI NA PODROČJU VARSTVA OSEBNIH PODATKOV

Direktiva o varstvu podatkov[1] iz leta 1995 je mejnik v zgodovini varstva osebnih podatkov v Evropski uniji. V njej sta določeni dve od najstarejših in enako pomembnih ambicij procesa evropskega vključevanja: varstvo temeljnih pravic in svoboščin posameznikov, zlasti temeljne pravice do varstva podatkov, na eni strani in delovanje notranjega trga, v tem primeru prosti pretok osebnih podatkov, na drugi.

Petnajst let pozneje ta dva cilja in načela Direktive še vedno veljajo. **Vendar pa sta hiter tehnološki razvoj in globalizacija korenito spremenila naš svet in prinesla nove izzive za varstvo osebnih podatkov.**

Tehnologija danes posameznikom omogoča preprosto izmenjavo informacij o njihovem vedenju in prioritetah ter javno in globalno dostopnost teh informacij v obsegu, kakršnega še ni bilo. Spletna socialna omrežja s sto milijoni članov s celega sveta so morda najbolj očiten, vendar ne edini primer za to. „Računalništvo v oblaku“, tj. ponujanje računalniških storitev prek spleta, pri čemer so programska oprema, sredstva v skupni rabi in podatki na oddaljenih strežnikih („v oblaku“), lahko prav tako pomeni izzive za varstvo podatkov, saj lahko vključuje izgubo nadzora posameznikov nad potencialno občutljivimi informacijami, kadar shranijo svoje podatke s programi na gostiteljski strojni opremi. Kot je potrdila nedavna študija, se zdi, da se organi za varstvo podatkov, poslovna združenja in organizacije potrošnikov strinjajo, da so tveganja za zasebnost in varstvo osebnih podatkov v zvezi s spletno dejavnostjo vedno večja[2].

Obenem **načini zbiranja osebnih podatkov postajajo vse bolj izpopolnjeni in jih je težje odkriti**. Tako na primer uporaba naprednih orodij gospodarskim subjektom omogoča, da se s spremljanjem vedenja posameznikov lahko bolj uspešno obračajo nanje. Z vse pogostejšo uporabo postopkov, ki omogočajo avtomatsko zbiranje podatkov, kot so elektronske vozovnice, elektronsko cestninjenje ali elektronske naprave za določanje zemljepisnega položaja, pa je mogoče lažje določiti lokacijo posameznikov zgolj zato, ker uporabljajo mobilno napravo. Tudi organi javne uprave vse pogosteje uporabljajo osebne podatke za različne namene, npr. za sledenje posameznikom v primeru izbruha nalezljive bolezni, za učinkovitejše preprečevanje terorizma in kaznivih dejanj ter boj proti njim, pri upravljanju sistemov socialne varnosti, za davčne namene, pri storitvah e-uprave itd.

Ob tem se ni mogoče izogniti vprašanju, ali se veljavna zakonodaja EU o varstvu podatkov lahko še naprej v celoti in učinkovito spopada z navedenimi izzivi.

---

[1] Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL L 281, 23.11.1995, str. 31).

[2] Glej Študijo o gospodarskih koristih tehnologij za boljše varovanje zasebnosti (*Study on the economic benefits of privacy enhancing technologies*), London Economics, julij 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf), str. 14.

Za obravnavo tega vprašanja je Komisija začela pregled veljavnega pravnega okvira s konferenco na visoki ravni maja 2009, sledilo pa je javno posvetovanje do konca leta 2009[3]. Izvajati so se začele tudi številne študije[4].

Ugotovitve so potrdile, da ključna načela Direktive še vedno veljajo in da bi bilo treba ohraniti njen tehnološko nevtralen značaj. Za več vprašanj pa se je štelo, da so problematična in pomenijo posebne izzive. Mednje spadajo:

- *obravnavanje vpliva novih tehnologij*

Odgovori posameznikov in organizacij v okviru posvetovanj so potrdili potrebo po razjasnitvi in opredelitvi uporabe načel varstva podatkov pri novih tehnologijah, da se dejansko zagotovi učinkovito varstvo osebnih podatkov posameznikov ne glede na to, katera tehnologija se uporabi za obdelavo njihovih podatkov, ter da se upravljavci podatkov popolnoma zavedajo posledic uporabe novih tehnologij za varstvo podatkov. To deloma ureja Direktiva 2002/58/ES (t. i. direktiva o e-zasebnosti)[5], ki je podrobnejša in dopolnjuje direktivo o splošnem varstvu podatkov na področju elektronskih komunikacij[6].

- *krepitev razsežnosti notranjega trga pri varstvu podatkov*

Eden od glavnih pomislekov zainteresiranih strani, zlasti večnacionalnih družb, je nezadostna usklajenost zakonodaj držav članic s področja varstva podatkov, in sicer kljub skupnemu pravnemu okviru EU. Poudarjena je bila potreba po večji pravni varnosti, zmanjšanju upravnih bremen ter zagotovitvi enakih pogojev za gospodarske subjekte in druge upravljavce podatkov.

- *obravnavanje globalizacije in izboljšanje mednarodnih prenosov podatkov*

Več zainteresiranih strani je poudarilo, da zaradi vse večjega zunanjega izvajanja obdelave podatkov, zelo pogosto zunaj EU, prihaja do različnih težav v zvezi s pravom, ki velja za obdelavo, in določitvijo s tem povezane odgovornosti. Kar zadeva mednarodne prenose

---

3 Glej odgovore udeležencev javnega posvetovanja Komisije: http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm. Več usmerjenih posvetovanj z zainteresiranimi stranmi je potekalo leta 2010. Podpredsednica Komisije Viviane Reding je predsedovala tudi srečanju z zainteresiranimi stranmi na visoki ravni 5. oktobra 2010 v Bruslju. Komisija se je posvetovala tudi z delovno skupino iz člena 29, ki je celovito prispevala k posvetovanju leta 2009 (DS 168) in julija 2010 sprejela posebno mnenje o konceptu odgovornosti (DS 173).

4 Poleg Študije o gospodarskih koristih tehnologij za boljše varovanje zasebnosti (glej opombo 2) glej tudi Primerjalno študijo o različnih pristopih k novim izzivom na področju varovanja zasebnosti, zlasti na podlagi tehnološkega razvoja (*Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*), januar 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf). Izvaja se tudi študija za oceno učinka prihodnjega pravnega okvira EU za varstvo osebnih podatkov.

5 Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah), (UL L 201, 31.7.2002, str. 37).

6 Direktiva o varstvu podatkov 95/46/ES določa standarde varstva podatkov za vse zakonodajne akte EU, vključno z direktivo o e-zasebnosti 2002/58/ES (spremenjena z Direktivo 2009/136/ES – UL L 337, 18.12.2009, str. 11). Direktiva o e-zasebnosti se uporablja za obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v javnih komunikacijskih omrežjih. Načela iz direktive o varstvu podatkov je preoblikovala v posebna pravila za sektor elektronskih komunikacij. Direktiva 95/46/ES se med drugim uporablja za komunikacijske storitve, ki niso namenjene javnosti.

podatkov, je veliko organizacij menilo, da veljavni sistemi niso popolnoma zadovoljivi ter da bi jih bilo treba pregledati in posodobiti, da bi prenosi postali enostavnejši in manj obremenjujoči.

- *zagotovitev trdnejše institucionalne ureditve za učinkovito izvrševanje predpisov o varstvu podatkov*

Zainteresirane strani soglašajo, da je treba pristojnosti organov za varstvo podatkov okrepiti in tako zagotoviti boljše izvrševanje predpisov o varstvu podatkov. Nekatere organizacije so zahtevale tudi večjo preglednost dela delovne skupine iz člena 29 (*glej točko 2.5. spodaj*) ter pojasnitev njenih nalog in pristojnosti.

- *večja usklajenost pravnega okvira na področju varstva podatkov*

V javnem posvetovanju so vse zainteresirane strani poudarile potrebo po krovnem pravnem aktu, ki bi veljal za dejavnosti obdelave podatkov v vseh sektorjih in politikah Unije ter zagotovil celosten pristop in nemoteno, dosledno in učinkovito varstvo[7].

Zaradi zgoraj navedenih izzivov **mora EU oblikovati celovit in skladen pristop**, ki bo zagotovil **popolno spoštovanje temeljne pravice posameznikov do varstva podatkov v EU in zunaj nje**. Z Lizbonsko pogodbo je EU dobila dodatne možnosti za dosego tega cilja: Listina EU o temeljnih pravicah – v členu 8 je priznana avtonomna pravica do varstva osebnih podatkov – je postala pravno zavezujoča, uvedena pa je bila tudi nova pravna podlaga[8] za sprejetje celovite in skladne zakonodaje Unije o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov. Nova pravna podlaga Evropski uniji omogoča zlasti sprejetje enotnega pravnega akta, ki ureja varstvo podatkov, tudi na področjih policijskega sodelovanja in pravosodnega sodelovanja v kazenskih zadevah. Področje skupne zunanje in varnostne politike je le deloma zajeto v členu 16 PDEU, saj morajo biti posebna pravila za obdelavo podatkov s strani držav članic določena v sklepu Sveta, ki ima drugačno pravno podlago[9].

Komisija bo na podlagi teh novih pravnih možnosti kot glavno prednostno nalogo obravnavala spoštovanje temeljne pravice do varstva podatkov po celi Uniji in v vseh njenih politikah, obenem pa tudi krepitev razsežnosti notranjega trga in omogočanje lažjega prostega pretoka osebnih podatkov. V zvezi s tem je treba ob zagotavljanju temeljne pravice do varstva osebnih podatkov v celoti upoštevati tudi druge pomembne temeljne pravice iz Listine in druge cilje Pogodb.

V tem sporočilu je predstavljen pristop Komisije k modernizaciji pravnega sistema EU za varstvo osebnih podatkov na vseh področjih dejavnosti Unije ob upoštevanju izzivov, ki so posledica globalizacije in novih tehnologij, da se bo nadalje zagotavljala visoka raven varstva posameznikov v zvezi z obdelavo osebnih podatkov na vseh področjih dejavnosti Unije. Tako bo EU lahko še naprej gonilna sila pri spodbujanju visokih standardov varstva podatkov po celem svetu.

---

7 Europol in Eurojust pa sta se v ločenih prispevkih, predloženih po izteku javnega posvetovanja, zavzemala za upoštevanje posebnosti njunega dela v zvezi z usklajevanjem pregona in preprečevanja kaznivih dejanj.

8 Glej člen 16 Pogodbe o delovanju Evropske unije (PDEU).

9 Glej zadnji odstavek člena 16(2) PDEU in člen 39 Pogodbe o Evropski uniji (PEU).

2. GLAVNI CILJI CELOVITEGA PRISTOPA K VARSTVU PODATKOV

2.1. Krepitev pravic posameznikov

2.1.1. Zagotavljanje ustreznega varstva posameznikov v vseh okoliščinah

Cilj veljavnih predpisov EU s področja varstva podatkov je **varovati temeljne pravice fizičnih oseb in zlasti njihovo pravico do varstva osebnih podatkov** v skladu z Listino EU o temeljnih pravicah[10].

Pojem „osebnih podatkov“ je eden ključnih pojmov na področju varstva posameznikov v veljavnih predpisih EU o varstvu podatkov, iz njega pa izhajajo obveznosti upravljavcev in obdelovalcev podatkov[11]. Opredelitev „osebnih podatkov“ zajema vse informacije, ki se bodisi neposredno bodisi posredno nanašajo na določeno ali določljivo fizično osebo. Za odločitev, ali je oseba določljiva, bi bilo treba upoštevati „vsa sredstva, za katera se pričakuje, da jih bo uporabil bodisi upravljavec ali katera koli druga oseba za določitev take osebe“[12]. Dobra stran tega premišljenega pristopa, ki ga je izbral zakonodajalec, je prožnost, zaradi katere lahko velja za različne situacije in razvoj dogodkov, ki vplivajo na temeljne pravice, vključno s tistimi, ki jih ob sprejetju Direktive ni bilo mogoče predvideti. Vendar so posledica takega širokega in prožnega pristopa številni primeri, v katerih pri izvajanju Direktive ni vedno jasno, kateri pristop je treba uporabiti, ali posamezniki uživajo pravice do varstva podatkov in ali morajo upravljavci podatkov upoštevati obveznosti iz Direktive[13].

Obstajajo situacije, ki vključujejo obdelavo posebnih informacij in bi zahtevale dodatne ukrepe na podlagi prava Unije. Takšni ukrepi v nekaterih primerih že obstajajo. Tako je na primer shranjevanje podatkov na terminalski opremi (npr. mobilnih telefonih) dovoljeno samo pod pogojem, da posameznik s tem soglaša. Na ravni EU bi bilo morda treba obravnavati tudi šifrirane podatke, generirane s ključem, podatke o lokaciji, tehnologije za iskanje podatkov, ki omogočajo kombiniranje podatkov iz različnih virov, ali primere, v katerih morata biti zagotovljeni zaupnost in celovitost v sistemih informacijske tehnologije[14].

Vsa zgoraj navedena vprašanja je zato treba skrbno preučiti.

Komisija bo preučila, **kako zagotoviti skladno uporabo predpisov o varstvu podatkov ob upoštevanju vpliva novih tehnologij na pravice in svoboščine posameznikov ter cilja zagotovitve prostega pretoka osebnih podatkov na notranjem trgu.**

---

10 Glej zadevi Sodišča Evropskih skupnosti C-101/01, *Bodil Lindqvist*, Recueil 2003, str. I-1297, točki 96 in 97, in C-275/06, *Productores de Música de España (Promusicae) proti Telefónica de España SAU*, Zodl. 2008, str. I-271. Glej tudi sodno prakso Evropskega sodišča za človekove pravice, npr. zadevi: *S. in Marper proti Združenemu kraljestvu*, 4.12.2008 (pritožbi št. 30562/04 in 30566/04), in *Rotaru proti Romuniji*, 4.5.2000; pritožba št. 28341/95, točka 55, ECHR 2000-V.

11 Za opredelitvi „upravljavcev“ in „obdelovalcev“ podatkov glej člen 2(d) in (e) Direktive 95/46/ES.

12 Glej uvodno izjavo 26 Direktive 95/46/ES.

13 Glej na primer zadevo v zvezi z naslovi IP, ki jo je delovna skupina iz člena 29 preučila v Mnenju 4/2007 o pojmu osebnih podatkov (DS 136).

14 Glej na primer sodbo nemškega zveznega ustavnega sodišča (*Bundesverfassungsgericht*) z dne 27. februarja 2008, 1 BvR 370/07.

2.1.2. Povečanje preglednosti za posameznike, na katere se nanašajo osebni podatki

Preglednost je temeljni pogoj, da lahko posamezniki nadzorujejo lastne podatke in da je zagotovljeno učinkovito varstvo osebnih podatkov. Zato je pomembno, da upravljavci podatkov posameznike **dobro in jasno ter na pregleden način obvestijo** o tem, kako in kdo zbira ter obdeluje njihove podatke, iz katerih razlogov in kako dolgo ter katere so njihove pravice, če želijo dostopiti do svojih podatkov, jih popraviti ali izbrisati. Zadevne določbe o informacijah, ki jih je treba zagotoviti posameznikom, na katere se nanašajo osebni podatki[15], niso zadostne.

Glavni elementi preglednosti so zahteve, da so **informacije lahko dostopne in razumljive ter izražene v jasnem in preprostem jeziku**. To je še zlasti pomembno v spletnem okolju, kjer so obvestila o varovanju zasebnosti kar pogosto nejasna, težko dostopna, nepregledna[16] in niso vedno skladna z veljavnimi predpisi. Primer za to bi lahko bilo spletno vedenjsko oglaševanje, pri katerem zaradi velikega števila vključenih akterjev in tehnološke zapletenosti posameznik težko ve in razume, ali se zbirajo osebni podatki, kdo jih zbira in v kateri namen.

V zvezi s tem potrebujejo posebno varstvo **otroci**, saj se mogoče manj zavedajo nevarnosti in posledic ter slabše poznajo zaščitne ukrepe in pravice v zvezi z obdelavo osebnih podatkov[17].

Komisija bo preučila:

– uvedbo **splošnega načela pregledne obdelave** osebnih podatkov v pravni okvir,

– uvedbo **posebnih obveznosti** za upravljavce podatkov glede vrste informacij, ki jih morajo priskrbeti, in **načinov** za to, vključno v zvezi z **otroki**,

– sestavo enega ali več **standardnih obrazcev EU** („**obvestil o varovanju zasebnosti**“), ki naj bi jih uporabljali upravljavci podatkov.

Pomembno je tudi, da so posamezniki obveščeni, kadar se njihovi podatki po naključju ali nezakonito uničijo, izgubijo, spremenijo, do njih dostopajo nepooblaščene osebe ali se razkrijejo nepooblaščenim osebam. Pri nedavnem pregledu direktive o e-zasebnosti je bilo uvedeno **obvezno obveščanje o kršitvah varstva osebnih podatkov**, vendar le za telekomunikacijski sektor. Ker do kršitev varstva podatkov prihaja tudi v drugih sektorjih (npr. v finančnem sektorju), bo Komisija preučila možnosti razširitve obveznosti obveščanja o kršitvah varstva osebnih podatkov na druge sektorje v skladu z izjavo Komisije pred Evropskim parlamentom glede obveščanja o kršitvah varstva podatkov leta 2009 v okviru reforme regulativnega okvira za elektronske komunikacije[18]. Ta preučitev ne bo vplivala na

---

15 Glej člena 10 in 11 Direktive 95/46/ES.

16 Raziskava Eurobarometra iz leta 2009 je pokazala, da so se obvestila o varovanju zasebnosti na spletnih straneh približno polovici vprašanih zdela „zelo“ ali „precej nejasna“ (glej Flash Eurobarometer št.°282: http://ec.europa.eu/public_opinion/flash/fl_282_en.pdf).

17 Glej kvalitativno raziskavo Varnejši internet za otroke (zajela je otroke, stare 9 do 10 in 12 do 14 let), ki je pokazala, da so otroci nagnjeni k podcenjevanju nevarnosti, povezanih z uporabo interneta, in omalovaževanju posledic svojega tveganega vedenja (dostopna na: http://ec.europa.eu/information_society/activities/sip/surveys/qualitative/index_en.htm).

18 „Komisija je seznanjena z voljo Evropskega parlamenta, da obveznost obveščanja o kršitvah varstva osebnih podatkov ne sme biti omejena na sektor elektronskih komunikacij, ampak mora veljati tudi za osebe, kot so ponudniki storitev informacijske družbe […]. Zato bo Komisija nemudoma začela s pripravami, vključno s posvetovanjem z zainteresiranimi stranmi, da bo lahko, če bo potrebno, do konca leta 2011 na tem področju predložila predloge […].“ Na voljo na: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-

določbe direktive o e-zasebnosti, ki jih je treba prenesti v nacionalno zakonodajo do 25. maja 2011[19]. Na tem področju bo treba zagotoviti dosleden in skladen pristop.

Komisija bo:

– preučila možnosti za uvedbo **splošnega obveščanja o kršitvah varstva osebnih podatkov** v splošni pravni okvir, vključno z naslovljenci takih obvestil in merili, kdaj obveznost obveščanja velja.

2.1.3. Povečanje nadzora nad lastnimi podatki

Pomembna predpogoja za zagotavljanje, da so posamezniki deležni visoke ravni varstva podatkov, sta **omejevanje obdelave s strani upravljavcev podatkov glede njenih namenov (načelo zmanjšanja količine podatkov)** in ohranitev **učinkovitega nadzora posameznikov nad lastnimi podatki**. Člen 8(2) Listine določa, da ima vsakdo „pravico dostopa do podatkov, zbranih o njem, in pravico zahtevati, da se ti podatki popravijo". Posameznikom bi moral biti vedno omogočen dostop do osebnih podatkov, njihov popravek, izbris ali blokiranje, razen če zakoniti razlogi to preprečujejo. V veljavnem pravnem okviru te pravice že obstajajo. Vendar pa način njihovega uresničevanja ni usklajen, zato jih je v nekaterih državah članicah lažje uresničevati kot v drugih. To pomeni poseben izziv zlasti v spletnem okolju, kjer se podatki pogosto shranijo, ne da bi bila zadevna oseba o tem obveščena in/ali s tem soglašala.

Posebej pomemben primer je spletno socialno mreženje, saj pomeni velik izziv za učinkovit nadzor posameznika nad lastnimi osebnimi podatki. Komisija je prejela številna vprašanja posameznikov, ki niso vedno mogli pridobiti osebnih podatkov, npr. svojih slik, od ponudnikov spletnih storitev in so bili torej ovirani pri uresničevanju svojih pravic do dostopa, popravka in izbrisa.

Te pravice bi bilo zato treba natančneje opredeliti, pojasniti in po možnosti okrepiti.

Komisija bo zato preučila možnosti za:

– krepitev **načela zmanjšanja količine podatkov**,

– **izboljšanje načinov uresničevanja pravic do dostopa, popravka, izbrisa ali blokiranja podatkov** (npr. z uvedbo rokov za odziv na zahteve posameznikov, omogočanjem uresničevanja pravic z elektronskimi sredstvi ali z zagotovitvijo pravice do načeloma brezplačnega dostopa),

– pojasnitev tako imenovane „**pravice biti pozabljen**", tj. pravice posameznikov, da se njihovi podatki več ne obdelujejo in da se izbrišejo, ko niso več potrebni za zakonite namene. To velja na primer, kadar obdelava temelji na soglasju osebe, ki ga ta oseba prekliče, ali kadar se obdobje shranjevanja izteče,

– dopolnitev pravic posameznikov, na katere se nanašajo osebni podatki, z zagotovitvijo „**prenosljivosti podatkov**", tj. zagotovitvijo izrecne pravice posameznika do umika lastnih podatkov (npr. slik ali seznama prijateljev) iz aplikacije ali storitve, tako da se umaknjeni podatki, kolikor je to tehnično izvedljivo, lahko prenesejo v drugo aplikacijo ali storitev brez oviranja s strani upravljavcev podatkov.

0360+0+DOC+XML+V0//SL. Glej tudi uvodno izjavo 59 Direktive 2009/136/ES o spremembah direktive o e-zasebnosti 2002/58/ES: „Splošni interes uporabnikov o obveščenosti seveda ni omejen na področje elektronskih komunikacij, zato bi se morale prednostno uvesti izrecne in obvezne zahteve glede priglasitve, ki bi veljale za vsa področja na ravni Skupnosti."

[19] Člen 4 Direktive 2009/136/ES.

2.1.4. Prizadevanja za večjo ozaveščenost

Preglednost je bistvena, izboljšati pa je treba tudi ozaveščenost javnosti in zlasti mladih o tveganjih v zvezi z obdelavo osebnih podatkov in njihovih pravicah. Raziskava Eurobarometra iz leta 2008 je pokazala, da velika večina ljudi v državah članicah EU meni, da je ozaveščenost o varstvu osebnih podatkov v njihovi državi nizka[20]. Prizadevanja za večjo ozaveščenost bi morali zato spodbujati številni akterji, tj. organi držav članic, zlasti organi za varstvo podatkov in izobraževalne institucije, pa tudi upravljavci podatkov in združenja civilne družbe. Prizadevanja bi morala vključevati nezakonodajne ukrepe, kot so kampanje ozaveščanja v tiskanih in elektronskih medijih ter zagotovitev jasnih informacij na spletnih straneh z natančno navedbo pravic posameznikov, na katere se nanašajo osebni podatki, in odgovornosti upravljavcev podatkov.

Komisija bo raziskala:

– možnost **sofinanciranja prizadevanj za večjo ozaveščenost o varstvu podatkov** iz proračuna Unije,

– potrebo po vključitvi **obveznosti izvajanja dejavnosti za večjo ozaveščenost** na tem področju v pravni okvir in možnosti za to.

2.1.5. Zagotavljanje prostovoljne privolitve

V zvezi s prostovoljno privolitvijo veljavna pravila določajo, da je privolitev posameznika v obdelavo njegovih osebnih podatkov „prostovoljno dana posebna in informirana izjava volje“, s katero posameznik izrazi soglasje, da se osebni podatki o njem obdelujejo[21]. Vendar se ti pogoji v državah članicah trenutno različno razlagajo, in sicer od splošne zahteve po pisni privolitvi do sprejemljivosti implicitne privolitve.

Zaradi nepreglednosti politik varovanja zasebnosti je v spletnem okolju za posameznike pogosto težje poznati svoje pravice in dati prostovoljno privolitev. To še bolj otežuje dejstvo, da v nekaterih primerih niti ni jasno, kaj bi bila prostovoljno dana posebna in informirana privolitev v obdelavo podatkov, kot npr. pri vedenjskem oglaševanju, pri katerem za nastavitve brskalnika nekateri menijo, da pomenijo privolitev uporabnika, drugi pa ne.

Zato bi bilo treba pojasniti pogoje za privolitev posameznika, na katerega se nanašajo osebni podatki, da bi bilo v skladu s členom 8 Listine EU o temeljnih pravicah vedno zagotovljeno, da je posameznik dal prostovoljno privolitev, da se tega popolnoma zaveda ter da ve, v kakšno obdelavo podatkov je privolil. Jasnost ključnih konceptov lahko koristi tudi razvoju samoregulativnih pobud za razvoj praktičnih rešitev v skladu s pravom EU.

Komisija bo preučila načine za **pojasnitev in krepitev pravil o privolitvi**.

2.1.6. Varstvo občutljivih podatkov

Obdelava občutljivih podatkov, tj. podatkov, ki kažejo na rasni ali etnični izvor, politična mnenja, verska ali filozofska prepričanja, pripadnost sindikatu, in obdelava podatkov v zvezi z zdravjem ali spolnim življenjem je trenutno že splošno prepovedana, omejene izjeme pa so

---

[20] Glej raziskavo Flash Eurobarometer št. 225 – Varstvo podatkov v Evropski uniji: http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

[21] Glej člen 2(h) Direktive 95/46/ES.

dovoljene pod določenimi pogoji in ob ustreznih zaščitnih ukrepih[22]. Ob upoštevanju tehnološkega in drugega družbenega razvoja pa je treba ponovno obravnavati veljavne določbe o občutljivih podatkih, premisliti, ali bi bilo treba dodati druge kategorije podatkov, in nadalje pojasniti pogoje za njihovo obdelavo. To zadeva na primer genetske podatke, ki trenutno niso izrecno navedeni kot kategorija občutljivih podatkov.

Komisija bo preučila(,):

– ali bi bilo treba za „**občutljive podatke**“ šteti tudi druge kategorije podatkov, na primer **genetske** podatke,

– nadaljnje pojasnjevanje in **usklajevanje pogojev** za obdelavo kategorij občutljivih podatkov.

2.1.7. Povečanje učinkovitosti pravnih sredstev in sankcij

Za izvrševanje predpisov o varstvu podatkov so bistvene **učinkovite določbe o pravnih sredstvih in sankcijah**. Veliko primerov, v katerih je posameznik prizadet zaradi kršitve predpisov o varstvu podatkov, zadeva tudi znatno število drugih posameznikov v podobni situaciji.

Zato bo Komisija:

– preučila možnost **razširitve kroga upravičencev za vložitev tožbe pri nacionalnih sodiščih** na organe za varstvo podatkov in združenja civilne družbe, kot tudi na **druga združenja, ki zastopajo interese posameznikov, na katere se nanašajo osebni podatki**,

– ocenila potrebo po **krepitvi veljavnih določb o sankcijah**, da bi postale učinkovitejše, na primer z izrecno vključitvijo kazenskih sankcij v primeru hudih kršitev varstva podatkov.

2.2. Krepitev razsežnosti notranjega trga

2.2.1. Večja pravna varnost in zagotovitev enakih pogojev za upravljavce podatkov

Varstvo podatkov v EU ima **močno razsežnost notranjega trga**, tj. potrebo po zagotovitvi prostega pretoka osebnih podatkov med državami članicami na notranjem trgu. Posledica tega je, da usklajevanje nacionalnih predpisov o varstvu podatkov v okviru Direktive ni omejeno le na minimalno uskladitev, temveč se načeloma konča s celovito uskladitvijo[23].

Obenem je z Direktivo državam članicam na nekaterih področjih priznan manevrski prostor, da lahko na podlagi te direktive ohranijo v veljavi ali uvedejo posebne ureditve za posebne položaje[24]. To je skupaj z dejstvom, da je pri prenosu Direktive s strani držav članic prišlo do nekaterih nepravilnosti, vodilo k **razlikam med nacionalnimi predpisi, v katere je bila prenesena Direktiva, kar je v nasprotju z enim od njenih glavnih ciljev, tj. zagotavljanjem prostega pretoka osebnih podatkov na notranjem trgu**. To velja za številne sektorje in situacije, npr. pri obdelavi osebnih podatkov v okviru zaposlovanja ali za namene javnega zdravja. Neusklajenost je ena od glavnih težav, na katere so pogosto opozorile zainteresirane strani iz zasebnega sektorja, zlasti gospodarski subjekti, saj zanje

---

22 Glej člen 8 Direktive 95/46/ES.

23 Sodba Sodišča Evropskih skupnosti v zadevi C-101/01, *Bodil Lindqvist*, Recueil 2003, str. I-1297, točki 96 in 97.

24 *Ibidem*, točka 97. Glej tudi uvodno izjavo 9 Direktive 95/46/ES.

pomeni dodatne stroške in upravno breme. To še posebej zadeva upravljavce podatkov, ki imajo sedež v več državah članicah in morajo upoštevati zahteve in prakse v vsaki od njih. Poleg tega razlike pri izvajanju Direktive v državah članicah povzročajo pravno negotovost ne samo za upravljavce podatkov, temveč tudi za posameznike, na katere se nanašajo osebni podatki, s čimer je ogrožena enaka raven varstva, ki naj bi jo Direktiva dosegla in zagotovila.

Komisija bo preučila sredstva za **nadaljnje usklajevanje predpisov o varstvu podatkov na ravni EU**.

2.2.2. Zmanjšanje upravnih bremen

Zagotovitev enakih pogojev bo zmanjšala potrebo po upoštevanju razhajajočih se nacionalnih zahtev in tako znatno zmanjšala upravna bremena za upravljavce podatkov. K zmanjšanju upravnih bremen in stroškov za upravljavce podatkov bi lahko prispevala tudi **pregled in poenostavitev veljavnega sistema obveščanja**[25]. Upravljavci podatkov soglašajo, da je veljavna splošna obveznost obveščanja organov za varstvo podatkov o vseh postopkih obdelave podatkov precej nerodna in kot taka brez prave dodane vrednosti za varstvo osebnih podatkov posameznikov. To je eden od primerov, v katerih Direktiva državam članicam priznava določen manevrski prostor, da se same odločijo o morebitnih izjemah in poenostavitvah ter ustreznih postopkih.

Usklajen in poenostavljen sistem bi zmanjšal stroške in upravna bremena, in sicer zlasti večnacionalnih družb, ki imajo sedež v več državah članicah.

Komisija bo preučila različne možnosti za **poenostavitev in uskladitev veljavnega sistema obveščanja**, vključno z morebitno sestavitvijo **enotnega registracijskega obrazca v EU**.

2.2.3. Pojasnitev pravil o pravu, ki se uporablja, in odgovornosti držav članic

V prvem poročilu Komisije o izvajanju direktive o varstvu podatkov je bilo že leta 2003[26] poudarjeno, da so bile določbe o pravu, ki se uporablja[27], „v več primerih pomanjkljive, zaradi česar bi lahko prišlo do kolizij zakonov, ki jih ta člen želi preprečiti“. Stanje se od takrat ni izboljšalo, zato upravljavcem podatkov in nadzornim organom za varstvo podatkov ni vedno jasno, katera država članica je pristojna in katero pravo se uporabi, kadar je vključenih več držav članic. Tako je zlasti v primerih, kadar za upravljavca podatkov veljajo različne zahteve v različnih državah članicah, kadar ima večnacionalna družba sedež v več kot eni državi članici ali kadar upravljavec podatkov nima sedeža v EU, vendar zagotavlja storitve prebivalcem v EU.

Zapletenost je vse večja tudi zaradi globalizacije in tehnološkega razvoja: upravljavci podatkov vedno pogosteje delujejo v več državah članicah in jurisdikcijah ter stalno zagotavljajo storitve in pomoč. Internet upravljavcem podatkov s sedežem zunaj Evropskega gospodarskega prostora (EGP)[28] zelo olajšuje zagotavljanje storitev na daljavo in obdelavo osebnih podatkov v spletnem okolju. Pogosto je težko ob katerem koli času določiti lokacijo

[25] Glej člen 18 Direktive 95/46/ES.

[26] Poročilo Komisije – Prvo poročilo o izvajanju direktive o varstvu podatkov (95/46/ES) – COM(2003) 265.

[27] Glej člen 4 Direktive 95/46/ES.

[28] Evropski gospodarski prostor vključuje Norveško, Lihtenštajn in Islandijo.

osebnih podatkov in uporabljene opreme (npr. pri aplikacijah in storitvah „računalništva v oblaku").

Vendar Komisija meni, da zaradi obdelave osebnih podatkov, ki jo izvaja upravljavec podatkov s sedežem v tretji državi, posamezniki ne bi smeli ostati brez varstva, do katerega so upravičeni v skladu z Listino EU o temeljnih pravicah in zakonodajo EU o varstvu podatkov.

Komisija bo preučila, kako **spremeniti in razjasniti veljavne določbe o pravu, ki se uporablja**, vključno z veljavnimi merili za njegovo določanje, da bi se povečala pravna varnost, kako pojasniti odgovornost držav članic pri uporabi predpisov o varstvu podatkov ter kako posameznikom v EU, na katere se nanašajo osebni podatki, zagotoviti isto stopnjo varstva ne glede na zemljepisno lokacijo upravljavca podatkov.

2.2.4. Krepitev odgovornosti upravljavcev podatkov

Upravna poenostavitev **ne bi smela voditi k splošnemu zmanjšanju odgovornosti upravljavcev podatkov za zagotavljanje učinkovitega varstva podatkov**. Nasprotno, Komisija meni, da bi bilo njihove obveznosti treba jasneje določiti v pravnem okviru, tudi glede mehanizmov notranjega nadzora in sodelovanja z nadzornimi organi za varstvo podatkov. Poleg tega bi moralo biti zagotovljeno, da taka odgovornost velja tudi za upravljavce, ki morajo upoštevati dolžnosti poklicne molčečnosti (npr. odvetnike), ter v vse pogostejših primerih, ko upravljavci podatkov za obdelavo podatkov pooblastijo druge subjekte (npr. obdelovalce).

Komisija bo zato raziskala načine za **zagotovitev, da upravljavci podatkov uporabljajo učinkovite politike in mehanizme za zagotavljanje skladnosti s predpisi o varstvu podatkov**. Pri tem bo upoštevala trenutno razpravo o možni uvedbi načela odgovornosti („accountability")[29]. Taki ukrepi ne bi vodili k povečanju upravnih bremen upravljavcev podatkov, saj bi se osredotočali na vzpostavitev zaščitnih ukrepov in mehanizmov, ki olajšujejo spoštovanje določb o varstvu podatkov ter hkrati zmanjšujejo in poenostavljajo nekatere upravne formalnosti, kot so uradna obvestila (*glej točko 2.2.2 zgoraj*).

V zvezi s tem bi spodbujanje uporabe tehnologij za boljše varovanje zasebnosti (Privacy Enhancing Technologies – PET), kot je bilo že poudarjeno v sporočilu Komisije na to temo iz leta 2007, ter načela „vgrajene zasebnosti" (Privacy by Design) lahko imelo pomembno vlogo, in sicer tudi pri zagotavljanju varnosti podatkov[30].

---

29 Glej zlasti mnenje, ki ga je delovna skupina iz člena 29 sprejela 13. julija, 3/2010.

30 Glede PET glej: Sporočilo Komisije Evropskemu parlamentu in Svetu o spodbujanju varstva podatkov s tehnologijami za boljše varovanje zasebnosti (PET) – COM(2007) 228. Načelo „vgrajene zasebnosti" pomeni, da sta zasebnost in varstvo podatkov vgrajena v celoten življenjski cikel tehnologije, od začetne faze načrtovanja do uvedbe, rabe in končno zavrženja. To načelo je med drugim omenjeno v sporočilu Komisije z naslovom „Evropska digitalna agenda" – COM(2010) 245.

Komisija bo za krepitev odgovornosti upravljavcev podatkov preučila naslednje elemente:

– obvezno imenovanje neodvisnega **pooblaščenca za varstvo podatkov** ter uskladitev pravil o njegovih nalogah in pristojnostih[31], z razmislekom o ustreznem pragu, da bi se zlasti za mala podjetja in mikropodjetja preprečila nepotrebna upravna bremena,

– vključitev obveznosti upravljavcev podatkov v pravni okvir, da v določenih primerih izvedejo **oceno učinka na varstvo podatkov**, na primer kadar se obdelujejo občutljivi podatki ali kadar je vrsta obdelave kako drugače povezana s posebnimi tveganji, zlasti pri uporabi posebnih tehnologij, mehanizmov ali postopkov, vključno z oblikovanjem profilov in video nadzorom,

– nadaljnje spodbujanje uporabe tehnologij za boljše varovanje zasebnosti in možnosti za dejansko izvajanje koncepta **„vgrajene zasebnosti“**.

2.2.5. Spodbujanje samoregulativnih pobud in preučitev sistemov potrjevanja EU

Komisija še vedno meni, da **samoregulativne pobude** upravljavcev podatkov lahko **prispevajo k boljšemu izvrševanju predpisov o varstvu podatkov**. Veljavne določbe o samoregulaciji iz direktive o varstvu podatkov, namreč glede pripravljanja kodeksov ravnanja[32], so se do zdaj redko uporabljale in se zainteresiranim stranem iz zasebnega sektorja ne zdijo zadostne.

Komisija bo preučila tudi možnost oblikovanja **shem potrjevanja** EU **(npr. „pečatov zaupnosti“)** za postopke, tehnologije, proizvode in storitve, ki so v skladu s predpisi o spoštovanju zasebnosti[33]. To ne bi samo usmerjalo posameznikov kot uporabnikov takih tehnologij, proizvodov in storitev, temveč bi bilo pomembno tudi v zvezi z odgovornostjo upravljavcev podatkov: z odločitvijo za uporabo potrjenih tehnologij, proizvodov ali storitev bi upravljavec lahko dokazal, da je izpolnil svoje obveznosti (*glej točko 2.2.4 zgoraj*). Seveda bi bilo nujno **zagotoviti zanesljivost takšnih pečatov zaupnosti** in preveriti, kako se ujemajo s pravnimi obveznostmi in mednarodnimi tehničnimi standardi.

Komisija bo:

– preučila sredstva za **nadaljnje spodbujanje samoregulativnih pobud**, vključno z dejavnim spodbujanjem kodeksov ravnanja,

– preverila izvedljivost oblikovanja **shem potrjevanja EU** na področju zasebnosti in varstva podatkov.

2.3. Spremembe predpisov o varstvu podatkov na področju policijskega in pravosodnega sodelovanja v kazenskih zadevah

Direktiva o varstvu podatkov se uporablja za vse postopke obdelave osebnih podatkov v državah članicah v javnem in zasebnem sektorju. Vendar se ne uporablja za obdelavo osebnih podatkov „med dejavnostjo, ki ne sodi na področje uporabe zakonodaje Skupnosti“, kot so

---

31 Možnost upravljavca podatkov, da imenuje pooblaščenca za varstvo podatkov in tako na neodvisen način zagotavlja skladnost s predpisi EU in nacionalnimi predpisi o varstvu podatkov ter pomaga posameznikom, je že uporabilo več držav članic (npr. *Beauftragter für den Datenschutz* v Nemčiji in *correspondant informatique et libertés (CIL)* v Franciji).

32 Glej člen 27 Direktive 95/46/ES.

33 V zvezi s tem glej tudi sporočilo o tehnologijah za boljše varovanje zasebnosti, glej opombo 30.

dejavnosti v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah[34]. Lizbonska pogodba je odpravila prejšnjo „stebrno strukturo“ EU ter uvedla novo in celovito pravno podlago za varstvo osebnih podatkov v vseh politikah Unije[35]. Ob upoštevanju navedenega in Listine EU o temeljnih pravicah je bilo v sporočilih Komisije o stockholmskem programu in akcijskem načrtu izvajanja stockholmskega programa[36] poudarjeno, da je treba vzpostaviti „celovit sistem varstva“ in okrepiti „položaj EU na področju varstva osebnih podatkov posameznikov v okviru politik EU, vključno s pregonom in preprečevanjem kaznivih dejanj.

Akt EU o varstvu osebnih podatkov na področju policijskega in pravosodnega sodelovanja v kazenskih zadevah je **Okvirni sklep 2008/977/PNZ**[37]. Okvirni sklep je pomemben korak naprej na področju, na katerem so bili skupni standardi varstva podatkov zelo potrebni. Vendar pa je treba delo nadaljevati.

Okvirni sklep se uporablja samo za čezmejno izmenjavo osebnih podatkov znotraj EU, ne pa tudi za domače postopke obdelave v državah članicah. To razlikovanje je v praksi težavno in lahko zaplete dejansko izvajanje in uporabo okvirnega sklepa[38].

Okvirni sklep vsebuje tudi preširoko izjemo od načela omejitve namena. Naslednja pomanjkljivost je dejstvo, da ne vsebuje določb, da je treba različne kategorije podatkov razlikovati glede na stopnjo točnosti in zanesljivosti, da je treba podatke, ki temeljijo na dejstvih, razlikovati od podatkov, ki temeljijo na mnenjih ali osebnih ocenah[39], ter da je treba razlikovati med različnimi kategorijami posameznikov, na katere se nanašajo osebni podatki (storilci kaznivih dejanj, osumljenci, žrtve, priče itd.), s posebnimi jamstvi za podatke v zvezi z osebami, ki niso osumljene[40].

Poleg tega **Okvirni sklep ne nadomešča različnih zakonodajnih aktov za posamezne sektorje na področju policijskega in pravosodnega sodelovanja v kazenskih zadevah, ki so bili sprejeti na ravni EU**[41], zlasti tistih, ki urejajo delovanje Europola, Eurojusta, schengenskega informacijskega sistema (SIS) in carinskega informacijskega sistema (CIS)[42], in vsebujejo posebne ureditve varstva podatkov in/ali se ponavadi sklicujejo na akte Sveta Evrope o varstvu podatkov. V zvezi z dejavnostmi na področju policijskega in pravosodnega sodelovanja so se vse države članice zavezale, da bodo spoštovale Priporočilo Sveta Evrope

---

34 Glej prvo alineo člena 3(2) Direktive 95/46/ES.

35 Glej člen 16 PDEU.

36 Glej COM(2009) 262, 10.6.2009, in COM(2010) 171, 20.4.2010.

37 Okvirni sklep Sveta 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). Okvirni sklep predvideva samo minimalno uskladitev standardov varstva podatkov.

38 Tako razlikovanje ne obstaja v zadevnih aktih Sveta Evrope, kot so: Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (CETS št. 108), njen dodatni protokol v zvezi z nadzornimi organi in čezmejnim prenosom podatkov (ETS št. 181) ter Priporočilo št. R (87) 15 Odbora ministrov državam članicam glede določanja uporabe osebnih podatkov v policijskem sektorju, sprejeto 17. septembra 1987.

39 Kot zahteva načelo 3.2 Priporočila št. R (87) 15.

40 V nasprotju z načelom 2 Priporočila št. R (87) 15 ter poročili o ocenah tega priporočila.

41 Glej pregled takih aktov v sporočilu Komisije z naslovom „Pregled upravljanja informacij na območju svobode, varnosti in pravice“ – COM(2010) 385.

42 Za zagotavljanje nadzora varstva podatkov so bili z ustreznimi akti ustanovljeni skupni nadzorni organi, in sicer dodatno k splošnim nadzornim pooblastilom Evropskega nadzornika za varstvo podatkov v zvezi z institucijami, organi, uradi in agencijami Unije na podlagi Uredbe (ES) št. 45/2001.

št. R (87) 15, v katerem so določena načela Konvencije št. 108 za policijski sektor. Vendar ne gre za pravno zavezujoč akt.

To stanje lahko neposredno vpliva na možnosti posameznikov za uresničevanje njihovih pravic do varstva podatkov na tem področju (npr. da vedo, kateri osebni podatki se obdelujejo in izmenjujejo, kdo to izvaja in v kateri namen, ter kako izvrševati svoje pravice, kot je pravica do dostopa do podatkov).

Za dosego cilja vzpostavitve celovitega in skladnega sistema v EU in v razmerju s tretjimi državami je **treba spremeniti veljavne predpise o varstvu podatkov na področju policijskega sodelovanja in pravosodnega sodelovanja v kazenskih zadevah**. Komisija poudarja, da pojem celovitega sistema varstva podatkov ne izključuje posebnih pravil o varstvu podatkov za policijski in pravosodni sektor znotraj splošnega okvira, in sicer ob ustreznem upoštevanju posebne narave teh področij, kot je navedeno v izjavi št. 21, ki je priložena Lizbonski pogodbi. To pomeni na primer, da je treba preučiti obseg, v katerem bi uresničevanje nekaterih pravic do varstva podatkov s strani posameznika v določenem primeru ogrozilo preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvajanje kazenskih sankcij.

Komisija bo zlasti:

– razmislila o **razširitvi uporabe splošnih predpisov o varstvu podatkov na področjih policijskega sodelovanja in pravosodnega sodelovanja v kazenskih zadevah**, vključno z obdelavo na domači ravni z uvedbo usklajenih **omejitev** nekaterih pravic posameznikov do varstva podatkov, kjer je to potrebno, npr. pravice do dostopa ali načela preglednosti,

– preučila potrebo po uvedbi **posebnih in usklajenih določb** v novi splošni okvir varstva podatkov, na primer o varstvu podatkov v zvezi z obdelavo **genetskih podatkov** v kazenskopravne namene ali o razlikovanju različnih kategorij posameznikov, na katere se nanašajo osebni podatki (priče, osumljenci itd.), na področju policijskega sodelovanja in pravosodnega sodelovanja v kazenskih zadevah,

– leta 2011 začela **posvetovanje** z vsemi zadevnimi zainteresiranimi stranmi o najboljšem načinu za **spremembe veljavnih nadzornih sistemov na področjih policijskega sodelovanja in pravosodnega sodelovanja v kazenskih zadevah**, da bi se zagotovil učinkovit in dosleden nadzor nad vsemi institucijami, organi, uradi in agencijami Unije glede varstva podatkov,

– ocenila potrebo po dolgoročni **uskladitvi veljavnih različnih posebnih aktov za posamezne sektorje, ki so bili sprejeti na ravni EU na področju policijskega in pravosodnega sodelovanja v kazenskih zadevah**, z novim splošnim pravnim okvirom varstva podatkov.

2.4. Globalna razsežnost varstva podatkov

2.4.1. Pojasnitev in poenostavitev pravil o mednarodnem prenosu podatkov

Eno od sredstev, ki omogočajo prenos osebnih podatkov zunaj EU in EGP, je t. i. **„ocena ustreznosti“**. Trenutno lahko ustreznost tretje države, tj. ali tretja država zagotavlja raven varstva, ki jo EU šteje za ustrezno, ugotovijo Komisija in države članice.

Učinek ugotovitve Komisije glede ustreznosti je prosti pretok osebnih podatkov iz 27 držav članic EU in treh članic EGP v zadevno tretjo državo, ne da bi bili potrebni kakršni koli

nadaljnji zaščitni ukrepi. Vendar direktiva o varstvu podatkov trenutno ne vsebuje dovolj podrobnih zahtev za priznanje ustreznosti s strani Komisije. Okvirni sklep pa določb o taki odločitvi Komisije sploh nima.

V nekaterih državah članicah ustreznost na prvi stopnji oceni upravljavec podatkov, ki prenaša osebne podatke v tretjo državo, včasih pa nadzorni organ za varstvo podatkov opravi naknadni nadzor. Takšno stanje lahko vodi k različnim pristopom za ocenjevanje ravni ustreznosti tretjih držav ali mednarodnih organizacij, pri čemer **obstaja nevarnost, da države članice različno ocenijo raven varstva posameznikov, na katere se nanašajo osebni podatki, ki jo zagotavlja tretja država**. Poleg tega veljavni pravni akti ne vsebujejo podrobnih usklajenih zahtev o tem, kateri prenosi se lahko štejejo za zakonite. Posledica so različne prakse držav članic.

Kar zadeva prenose podatkov tretjim državam, ki ne zagotavljajo ustrezne ravni varstva, veljavne standardne klavzule Komisije za prenos osebnih podatkov upravljavcem[43] in obdelovalcem[44] ne veljajo za nepogodbena razmerja in se na primer ne morejo uporabiti za prenose med javnimi upravami.

Mednarodni sporazumi, ki jih sklenejo EU ali njene države članice, pogosto zahtevajo vključitev načel varstva podatkov in posebnih določb. Posledica so lahko različna besedila z nedoslednimi določbami in pravicami, kar lahko privede do različnih razlag v škodo posameznikov, na katere se nanašajo osebni podatki. Zato je Komisija napovedala, da se bo ukvarjala s ključnimi elementi varstva osebnih podatkov v sporazumih med Evropsko unijo in tretjimi državami za namene kazenskega pregona[45].

Tudi druga sredstva, razvita kot oblika samoregulacije, kot so notranji kodeksi ravnanja v podjetjih, znani kot „zavezujoča poslovna pravila“ (Binding Corporate Rules)[46], so lahko koristna pri zakonitem prenosu osebnih podatkov med podjetji, ki pripadajo isti skupini podjetij. Vendar pa so zainteresirane strani predlagale, da bi se ta mehanizem lahko še izboljšal, njegovo izvajanje pa olajšalo.

Za obravnavanje navedenih vprašanj obstaja **splošna potreba po izboljšanju veljavnih mehanizmov za mednarodne prenose osebnih podatkov**, obenem pa je treba zagotoviti ustrezno varstvo osebnih podatkov pri prenosih in obdelavi zunaj EU in EGP.

---

43 Odločba Komisije 2001/497/ES z dne 15. junija 2001 o standardnih pogodbenih klavzulah za prenos osebnih podatkov v tretje države v skladu z Direktivo 95/46/ES (UL L 181, 4.7.2001, str. 19); Odločba Komisije 2002/16/ES z dne 27. decembra 2001 o standardnih pogodbenih klavzulah za prenos osebnih podatkov obdelovalcem s sedežem v tretjih državah v skladu z Direktivo 95/46/ES (UL L 6, 10.1.2002, str. 52); Odločba Komisije 2004/915/ES z dne 27. decembra 2004 o spremembi Odločbe 2001/497/ES glede uvedbe alternativnega sklopa standardnih pogodbenih klavzul za prenos osebnih podatkov v tretje države (UL L 385, 29.12.2004, str. 74).

44 Sklep Komisije z dne 5. februarja 2010 o standardnih pogodbenih klavzulah za prenos osebnih podatkov obdelovalcem s sedežem v tretjih državah v skladu z Direktivo Evropskega parlamenta in Sveta 95/46/ES (UL L 39, 12.2.2010, str. 5).

45 Akcijski načrt izvajanja stockholmskega programa (glej opombo 36).

46 „Zavezujoča poslovna pravila“ so kodeksi ravnanja na podlagi evropskih standardov varstva podatkov, ki jih večnacionalne družbe prostovoljno sestavijo in upoštevajo, da bi zagotovile ustrezne zaščitne ukrepe za prenose ali kategorije prenosov osebnih podatkov med podjetji, ki pripadajo isti skupini podjetij in jih ta poslovna pravila zavezujejo. Glej: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf.

Komisija namerava preučiti, kako:

– **izboljšati in posodobiti veljavne postopke** mednarodnega prenosa podatkov, vključno s pravno zavezujočimi akti in zavezujočimi poslovnimi pravili, da bi se zagotovil **enotnejši in skladnejši pristop EU** v razmerju do tretjih držav in mednarodnih organizacij,

– **pojasniti postopek Komisije za ugotavljanje ustreznosti** ter bolje opredeliti **merila in zahteve** za oceno ravni varstva podatkov v tretji državi ali mednarodni organizaciji,

– opredeliti **glavne elemente EU za varstvo podatkov**, ki bi se lahko uporabljali v vseh vrstah mednarodnih sporazumov.

2.4.2. Spodbujanje univerzalnih načel

Obdelava podatkov je globalizirana in zahteva razvoj univerzalnih načel varstva posameznikov pri obdelavi osebnih podatkov.

Pravni okvir EU za varstvo podatkov **tretjim državam** pogosto služi kot **merilo za urejanje varstva podatkov**. Njegovi učinki znotraj in zunaj Unije so zelo pomembni. **Evropska unija mora zato ostati gonilna sila na področju razvoja in spodbujanja mednarodnih pravnih in tehničnih standardov varstva osebnih podatkov** na podlagi zadevnih predpisov EU in drugih evropskih predpisov o varstvu podatkov. To je še zlasti pomembno v okviru širitvene politike EU.

Kar zadeva mednarodne tehnične standarde, ki so jih razvile organizacije za standardizacijo, Komisija meni, da je skladnost prihodnjega pravnega okvira in teh standardov zelo pomembna za zagotovitev doslednega izvajanja predpisov o varstvu podatkov s strani upravljavcev podatkov v praksi.

Komisija:

– bo še naprej **spodbujala razvoj visokih pravnih in tehničnih standardov varstva podatkov** v tretjih državah ter na mednarodni ravni,

– se bo zavzemala za **načelo vzajemnosti varstva** v mednarodnih ukrepih Unije, zlasti glede posameznikov, katerih osebni podatki se prenašajo iz EU v tretje države,

– bo **v ta namen okrepila sodelovanje s tretjimi državami in mednarodnimi organizacijami**, kot so OECD, Svet Evrope, Združeni narodi in druge regionalne organizacije,

– bo **natančno spremljala razvoj mednarodnih tehničnih standardov pri organizacijah za standardizacijo**, kot sta CEN in ISO, za zagotovitev, da koristno dopolnjujejo predpise, ter za zagotovitev operativnega in učinkovitega izvajanja ključnih zahtev za varstvo podatkov.

2.5. Trdnejša institucionalna ureditev za boljše izvrševanje predpisov o varstvu podatkov

Izvajanje in izvrševanje načel in predpisov o varstvu podatkov je ključni element spoštovanja pravic posameznikov.

Pri izvrševanju predpisov o varstvu podatkov imajo **bistveno vlogo organi za varstvo podatkov**. So neodvisni varuhi temeljnih pravic in svoboščin na področju varstva osebnih podatkov in posamezniki se zanašajo na to, da jim ti organi zagotavljajo varstvo njihovih

osebnih podatkov in zakonitost postopkov obdelave. Iz tega razloga Komisija meni, da bi bilo treba njihovo vlogo okrepiti, zlasti ob upoštevanju nedavne sodne prakse Sodišča Evropske unije o njihovi neodvisnosti[47], ter jim zagotoviti potrebna pooblastila in sredstva za ustrezno izvajanje njihovih nalog na nacionalni ravni in v medsebojnem sodelovanju.

Obenem pa Komisija meni, da bi **organi za varstvo podatkov morali okrepiti medsebojno sodelovanje in bolje usklajevati svoje dejavnosti**, in sicer zlasti, kadar se soočajo z vprašanji, ki imajo po svoji naravi čezmejne razsežnosti. Za to gre zlasti, kadar imajo večnacionalne družbe sedež v več državah članicah in so dejavne v vsaki od njih ali kadar je nadzor treba usklajevati z Evropskim nadzornikom za varstvo podatkov[48].

Pomembno vlogo pri tem **ima lahko delovna skupina iz člena 29**[49], ki ima poleg svetovalne funkcije[50] tudi nalogo, da prispeva k enotni uporabi predpisov EU o varstvu podatkov na nacionalni ravni. Ker pa organi za varstvo podatkov še naprej različno uporabljajo in razlagajo predpise EU, čeprav so izzivi na področju varstva podatkov po celi EU enaki, je treba okrepiti vlogo delovne skupine pri usklajevanju stališč organov za varstvo podatkov, da bi se zagotovila enotnejša uporaba na nacionalni ravni in s tem enaka raven varstva podatkov.

Komisija bo preučila,:

– kako bi bilo v novem pravnem okviru mogoče **okrepiti, pojasniti in uskladiti status ter pristojnosti nacionalnih organov za varstvo podatkov**, vključno s polnim izvajanjem koncepta „popolne neodvisnosti“[51],

– kako **izboljšati sodelovanje in usklajevanje med organi za varstvo podatkov**,

– kako zagotoviti doslednejšo uporabo predpisov EU o varstvu podatkov na notranjem trgu. Lahko bi se **okrepila vloga nacionalnih organov za varstvo podatkov, njihovo delo bolje usklajevalo prek delovne skupine iz člena 29 (ki bi morala postati bolj pregledno telo) in/ali vzpostavil mehanizem za zagotavljanje doslednosti na notranjem trgu pod vodstvom Evropske komisije**.

3. SKLEP: KAKO NAPREJ

S tehnologijo se nenehno spreminjajo tudi načini uporabe in prenosa osebnih podatkov v naši družbi. To pomeni izziv za zakonodajalce, da ustvarijo zakonodajni okvir, ki take spremembe preživi. Po reformi bi evropski predpisi o varstvu podatkov morali še naprej zagotavljati visoko raven varstva, posameznikom, javnim upravam in podjetjem na notranjem trgu pa pravno varnost za več generacij. Ne glede na to, kako zapleten je položaj ali kako razvita je tehnologija, mora biti jasno, katero pravo in standarde morajo nacionalni organi izvrševati,

---

47 Sodba Sodišča Evropske unije z dne 9. marca 2010, *Komisija proti Nemčiji*, zadeva C-518/07.

48 To trenutno velja za obsežne informacijske sisteme, npr. za SIS II (glej člen 46 Uredbe (ES) št. 1987/2006 – UL L 318, 28.12.2006, str. 4) in VIS (glej člen 43 Uredbe (ES) št. 767/2008 – UL L 218, 13.8.2008, str. 60).

49 Delovna skupina iz člena 29 je svetovalno telo, ki ga sestavljajo po en predstavnik organov za varstvo podatkov vsake države članice, predstavnik Evropskega nadzornika za varstvo podatkov in predstavnik Komisije (brez glasovalne pravice). Komisija opravlja tudi naloge sekretariata. Glej: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

50 Delovna skupina iz člena 29 ima vlogo svetovanja Komisiji glede ravni varstva v EU in tretjih državah ter glede vseh ukrepov v zvezi z obdelavo osebnih podatkov.

51 Glej sodbo Sodišča Evropske unije z dne 9. marca 2010, *Komisija proti Nemčiji*, zadeva C-518/07.

podjetja in razvijalci tehnologij pa spoštovati. Tudi posamezniki morajo dobro poznati svoje pravice.

Celovit pristop Komisije k obravnavanju vprašanj in doseganju ključnih ciljev, navedenih v tem sporočilu, bo podlaga za nadaljnje razprave z drugimi evropskimi institucijami in zainteresiranimi stranmi ter pozneje za konkretne predloge in ukrepe zakonodajne in nezakonodajne narave. Zato bo Komisija vesela povratnih informacij glede vprašanj, postavljenih v tem sporočilu.

Na tej podlagi bo Komisija **leta 2011** po opravljeni oceni učinka in ob upoštevanju Listine EU o temeljnih pravicah **predlagala zakonodajne akte** za spremembe pravnega okvira na področju varstva podatkov s ciljem krepitve položaja EU na področju varstva osebnih podatkov posameznikov v okviru vseh politik EU, vključno s pregonom in preprečevanjem kaznivih dejanj, in ob upoštevanju posebnosti teh področij. Istočasno bodo obravnavani tudi nezakonodajni ukrepi, npr. glede spodbujanja samoregulacije in preučitve izvedljivosti oblikovanja pečatov zaupnosti EU.

V drugem koraku bo Komisija **ocenila potrebo po prilagoditvi drugih pravnih aktov** novemu splošnemu okviru za varstvo podatkov. Najprej bo treba prilagoditi določbe Uredbe (ES) št. 45/2001. Pozneje bo treba skrbno preučiti tudi učinek na druge akte za posamezne sektorje.

Poleg tega bo Komisija še naprej ustrezno spremljala pravilno izvajanje prava Unije na tem področju in izvajala **dejavno politiko glede kršitev** v primerih nepravilnega izvajanja in uporabe predpisov EU o varstvu podatkov. Trenutni pregled predpisov o varstvu osebnih podatkov ne vpliva na obveznost držav članic za izvajanje in pravilno uporabo veljavnih predpisov na tem področju[52].

Visoka in enotna raven varstva podatkov v EU bo najboljši način za podpiranje in spodbujanje standardov EU za varstvo podatkov na globalni ravni.

[52] To velja tudi za Okvirni sklep Sveta 2008/977/PNZ: države članice sprejmejo ukrepe, potrebne za uskladitev z določbami tega okvirnega sklepa, pred 27. novembrom 2010.