Pitanja i odgovori – Opća uredba o zaštiti podataka

Bruxelles, 24. siječnja 2018.

Paket za reformu zaštite podataka koji je stupio na snagu u svibnju 2016. i koji će se primjenjivati od svibnja 2018. obuhvaća Opću uredbu o zaštiti podataka („Uredba”) i Direktivu o zaštiti podataka za policijska i kaznenopravna tijela.

IP/17/386

Reforma je ključan korak za jačanje temeljnih prava građana u digitalno doba i olakšavanje poslovanja pojednostavnjivanjem pravila za poduzeća na jedinstvenom digitalnom tržištu.

Zašto Komisija danas donosi smjernice?

Opća uredba o zaštiti podataka temelj je za slobodan protok podataka čitavim jedinstvenim digitalnim tržištem. Komisija želi osigurati da su svi subjekti – vlade EU-a, nacionalna tijela za zaštitu podataka, poduzeća i građani – spremni za stupanje Uredbe na snagu 25. svibnja 2018. Pravila su donesena u travnju 2016. Iako se Uredba izravno primjenjuje, u određenim su aspektima potrebne bitne prilagodbe, kao što su izmjene postojećih zakona koje trebaju provesti vlade država članica EU-a ili uspostava Europskog odbora za zaštitu podataka, koji trebaju osnovati tijela za zaštitu podataka kako bi izmjene nesmetano funkcionirale u praksi.

Budući da je do primjene novog propisa ostalo nešto više od sto dana, u smjernicama se daje pregled onoga što bi Europska komisija, nacionalna tijela za zaštitu podataka i nacionalne uprave još trebali poduzeti kako bi faza pripreme bila uspješno dovršena.

Što Komisija poduzima kako bi osigurala ispravnu primjenu Opće uredbe o zaštiti podataka?

Komisija od 2016. podržava:

– države članice i njihova tijela, osnivanjem stručne skupine koja će državama članicama pomoći u pripremama za Uredbu

– pojedinačna tijela za zaštitu podataka i osnivanje Europskog odbora za zaštitu podataka, podržavanjem skupine koja trenutačno okuplja nacionalna tijela za zaštitu podataka (radna skupina iz članka 29.)

– dionike, organiziranjem okruglih stolova s poduzećima, uključujući MSP-ove.

Komisija je danas objavila novi, praktični internetski alat kako bi pomogla građanima, poduzećima, a posebno MSP-ovima, te drugim organizacijama da se usklade s novim pravilima o zaštiti podataka i pokazala im kako da od njih imaju koristi.

Osim toga, Komisija je za financiranje tijela za zaštitu podataka namijenila 1,7 milijuna EUR, a tim bi se sredstvima trebalo financirati i osposobljavanje stručnjaka u području zaštite podataka. Dodatnih je 2 milijuna EUR dostupno za potporu nacionalnim tijelima za podizanje razine osviještenosti među poduzećima, posebno MSP-ovima.

Što će se promijeniti provedbom Opće uredbe o zaštiti podataka?

Uredbom se ažuriraju i osuvremenjuju načela utvrđena u Direktivi o zaštiti podataka iz 1995. kako bi se zajamčila prava na privatnost. Usmjerena je na:

- jačanje prava pojedinaca
- jačanje unutarnjeg tržišta EU-a
- osiguravanje snažnije provedbe pravila
- pojednostavnjenje međunarodnih prijenosa osobnih podataka i
- utvrđivanje globalnih standarda za zaštitu podataka.

Na temelju tih promjena građani će dobiti **veću kontrolu** nad svojim osobnim podacima i olakšat će im se njezina upotreba. Promjene su osmišljene kako bi se osigurala zaštita osobnih podataka, bez obzira na to kamo se podaci šalju te gdje se obrađuju ili pohranjuju, čak i kad se lokacija nalazi izvan EU-a, što je često na internetu.

Koje su koristi za građane?

Reforma pojedincima pruža alate za **stjecanje kontrole nad osobnim podacima**, čija je zaštita temeljno pravo u Europskoj uniji. Reformom zaštite podataka **ojačat će se prava građana i izgraditi povjerenje**.

Devet od deset Europljana zabrinuto je što mobilne aplikacije prikupljaju njihove podatke bez njihove suglasnosti, a sedam od deset zabrinuto je zbog načina na koji bi poduzeća mogla iskoristiti podatke koje im otkrivaju. Novim se pravilima nastoji riješiti te probleme na sljedeći način:

- **„pravo na zaborav"**: kad pojedinac više ne želi da se njegovi podaci obrađuju i uz uvjet da ne postoje zakoniti razlozi za njihovo zadržavanje, podaci će se brisati. Riječ je o zaštiti privatnosti pojedinaca, a ne o brisanju prošlih događaja ili ograničavanju slobode tiska;
- **lakši pristup vlastitim podacima**: pojedinci će imati više informacija o tome kako se njihovi podaci obrađuju i te bi informacije morale biti dostupne na jasan i razumljiv način. **Pravom na prijenos podataka** korisnicima će se olakšati prijenos osobnih podataka među različitim pružateljima usluga;
- **pravo na obavijest o povredi osobnih podatka**: poduzeća i organizacije moraju obavijestiti nacionalno nadzorno tijelo o povredama podataka zbog kojih su pojedinci izloženi opasnosti te obavijestiti osobe čiji se podaci obrađuju o svim visokorizičnim povredama podataka što je prije moguće kako bi korisnici mogli poduzeti odgovarajuće mjere;
- **tehnička i integrirana zaštita podataka**: „ integrirana zaštita podataka" i „zaštita podataka u postavkama" sada su ključni elementi pravila EU-a za zaštitu podataka. Mjere za zaštitu podataka bit će ugrađene u proizvode i usluge od najranije faze njihova razvoja, a zadane postavke usmjerene na privatnost postat će norma, primjerice na društvenim mrežama ili u mobilnim aplikacijama.

Pravo na zaborav: kako će to funkcionirati?

Već se postojećom Direktivom pojedincima daje mogućnost brisanja osobnih podataka, posebice kada ti podaci više nisu potrebni. Na primjer, ako je osoba dala suglasnost za obradu podataka za posebnu namjenu (na primjer radi navođenja podataka na stranicama društvenih mreža) i više ne želi tu uslugu, nema razloga da se podaci zadrže u sustavu.

To se posebice odnosi na djecu koja su objavila svoje osobne podatke jer ona često nisu potpuno svjesna posljedica i ne smiju do kraja života snositi posljedice te odluke.

To ne znači da se na svaki zahtjev pojedinca svi njegovi osobni podaci moraju istog trenutka zauvijek izbrisati. Ako je, na primjer, zadržavanje podataka nužno za izvršenje ugovora ili ispunjavanje pravne obveze, podaci se mogu čuvati onoliko dugo koliko je potrebno za tu svrhu.

Predložene odredbe o „pravu na zaborav" vrlo su jasne: **štite se sloboda izražavanja** te povijesna i znanstvena **istraživanja**. Na primjer, političari neće moći ukloniti svoje prethodne izjave s interneta. Time će se, između ostalog, internetskim informativnim stranicama omogućiti nastavak rada na temelju istih načela.

Postoji li posebna zaštita za djecu?

Da, u okviru Uredbe prepoznaje se činjenica da djeca zaslužuju posebnu zaštitu osobnih podataka jer su možda manje svjesna rizika, posljedica, zaštite i svojih prava u vezi s obradom osobnih podataka. Na primjer, djeca imaju koristi od jasnije primjene prava na zaborav.

Kad je riječ o uslugama informacijskog društva koje se nude izravno djeci, Uredbom se predviđa da suglasnost na obradu djetetovih podataka mora dati ili odobriti nositelj roditeljske odgovornosti. Države članice same će odrediti dobnu granicu u rasponu od 13 do 16 godina.

Cilj je posebne odredbe zaštititi djecu od situacija u kojima bi bila prisiljena objaviti osobne podatke bez potpunog razumijevanja posljedica. Odredbom se neće tinejdžerima onemogućiti uporaba interneta za traženje informacija, savjeta ili uporaba u obrazovne svrhe. Osim toga, u Uredbi se navodi da suglasnost nositelja roditeljske odgovornosti neće biti potrebna kad je riječ o preventivnim uslugama ili uslugama savjetovanja koje se nude izravno djetetu.

Koje su koristi za poduzeća?

Reformom se osiguravaju **jasnoća i dosljednost pravila koja će se primjenjivati te se obnavlja povjerenje potrošača**, što poduzećima omogućuje da u potpunosti iskoriste mogućnosti koje im se pružaju na jedinstvenom digitalnom tržištu.

Podaci su valuta današnjeg digitalnog gospodarstva. Osobni podaci koji se prikupljaju, analiziraju i šalju diljem zemaljske kugle postali su iznimno važni u gospodarskom smislu. Prema nekim procjenama vrijednost osobnih podataka europskih građana mogla bi do 2020. narasti do gotovo

jednog bilijuna EUR godišnje. Jačanjem visokih europskih normi zaštite podataka zakonodavci stvaraju poslovne mogućnosti.

Paket za reformu zaštite podataka pomaže u ostvarivanju tog potencijala na jedinstvenom digitalnom tržištu na sljedeće načine:

- **jedan kontinent, jedan zakon**: jedinstveno paneuropsko pravo o zaštiti podataka, kojim se zamjenjuje trenutačna nedosljedna kombinacija nacionalnih prava. Poduzeća će morati postupati u skladu s jednim zakonom, a ne njih 28. Korist se procjenjuje na 2,3 milijarde EUR godišnje;
- **jedinstvena kontaktna točka**: jedinstvena kontaktna točka za poduzeća. Poduzeća će morati odgovarati samo jednom nadzornom tijelu, umjesto njih 28, čime postaje jednostavnije i jeftinije poslovati diljem EU-a;
- **ista pravila za sva poduzeća – bez obzira na mjesto gdje imaju poslovni nastan**: europska se poduzeća trenutačno moraju pridržavati strožih standarda nego poduzeća s poslovnim nastanom izvan EU-a koja također posluju na našem jedinstvenom tržištu. Nakon reforme poduzeća sa sjedištem izvan EU-a morat će primjenjivati ista pravila za ponudu roba i usluga na tržištu EU-a. Time se stvaraju ravnopravni uvjeti;
- **tehnološka neutralnost**: Uredbom se stvara pogodno okruženje za daljnji razvoj inovacija na temelju novih pravila.

Što je jedinstvena kontaktna točka?

U jedinstvenom tržištu podataka nije dovoljno imati jednaka pravila samo u teoriji. Pravila se svugdje moraju primjenjivati na isti način. „Jedinstvenom kontaktnom točkom" pojednostavit će se suradnja među tijelima za zaštitu podataka u pogledu pitanja koja utječu na cijelu Europu. Poduzeća će morati odgovarati samo jednom nadzornom tijelu, umjesto njih 28. Time će se osigurati pravna sigurnost za poduzeća. Poduzeća će imati koristi od bržeg donošenja odluka, uspostave jedinstvenog sugovornika (uklanjanja višestrukih kontaktnih točaka) i smanjenja birokracije. Imat će koristi od dosljednosti odluka u situacijama kada se isti postupak obrade podataka provodi u nekoliko država članica.
Pojedinci će imati veću kontrolu.

Kako će to pomoći poduzećima?

Novo pravo na **prenosivost podataka** omogućuje građanima da svoje podatke prenesu s jednog poduzeća na drugo. Novoosnovana i manja poduzeća imat će pristup tržištima podataka kojima su prije dominirali digitalni divovi, što će im omogućiti da rješenjima kojima se čuva privatnost privuku veći broj potrošača. Time će se povećati konkurentnost europskog gospodarstva.

Primjer: koristi za pojedince, koristi za poduzeća

Novo malo poduzeće želi ući na tržište i ponuditi internetski društveni medij u obliku web-mjesta za razmjenu. Na tržištu već postoje veliki igrači koji imaju velik tržišni udio. U skladu s postojećim pravilima svaki novi korisnik mora razmotriti želi li ispočetka unositi osobne podatke koje želi objaviti kako bi uspostavio profil na novom web-mjestu. To bi moglo odvratiti neke korisnike koji razmišljaju o prelasku u novo poduzeće.

Prema reformi zaštite podataka: *pravo na prijenos podataka olakšat će potencijalnim novim korisnicima prijenos osobnih podataka među različitim pružateljima usluga. Potrošačima se time omogućuje kontrola nad svojim osobnim podacima, a istodobno se promiče tržišno natjecanje i potiče uključivanje novih poduzeća na tržište.*

Koje su koristi za MSP-ove?

Reforma zaštite podataka usmjerena je na **poticanje gospodarskog rasta** smanjenjem troškova i birokracije za europska poduzeća, što također vrijedi za mala i srednja poduzeća (MSP-ove). Uvođenjem jednog pravila umjesto njih 28 u okviru reforme zaštite podataka EU-a pomoći će se MSP-ovima da se probiju na nova tržišta. U brojnim su slučajevima obveze voditelja i izvršitelja obrade podataka prilagođene veličini poduzeća i/ili prirodi podataka koji se obrađuju. Na primjer:

- **MSP-ovi ne moraju imenovati službenika za zaštitu podataka**, osim ako njihove glavne djelatnosti zahtijevaju redovno i sustavno praćenje ispitanika u velikim razmjerima ili ako obrađuju posebne kategorije osobnih podataka, kao što su podaci koji otkrivaju rasno ili etničko podrijetlo ili vjerska uvjerenja. Osim toga, službenik ne mora biti zaposlen u punom radnom vremenu, već to može biti *ad hoc* savjetnik, što je mnogo jeftinije;
- **MSP-ovi ne trebaju voditi evidenciju obrade podataka**, osim ako obrada nije povremena ili ako je vjerojatno da će prouzročiti rizik za prava i slobode ispitanika;
- **MSP-ovi neće biti obvezni pojedincima prijaviti svaki slučaj povrede osobnih podataka**, nego samo ako povrede ozbiljno ugrožavaju njihova prava i slobode.

Kako će se novim pravilima uštedjeti?

Uredbom će se uspostaviti jedinstveno paneuropsko pravo o zaštiti podataka, što znači da poduzeća mogu postupati u skladu samo s jednim zakonom, umjesto s njih 28. Nova će pravila donijeti korist u iznosu od otprilike **2,3 milijarde EUR godišnje**.

Primjer: smanjenje troškova

Lanac prodavaonica ima sjedište u Francuskoj i prodavaonice u franšiznom poslovanju u 14 drugih država članica EU-a. Svaka prodavaonica prikuplja podatke povezane s kupcima i prenosi ih u sjedište u Francuskoj radi daljnje obrade.

Prema postojećim pravilima: *pri obradi podataka u sjedištu primjenjivali bi se francuski zakoni o zaštiti podataka, ali pojedinačne bi prodavaonice ipak morale izvješćivati nacionalno tijelo za zaštitu podataka, kako bi se potvrdilo da se podaci obrađuju u skladu s nacionalnim zakonodavstvom u državi u kojoj se prodavaonice nalaze. To znači da bi se sjedište poduzeća moralo savjetovati s lokalnim odvjetnicima u vezi sa svakom povredom prava kako bi se osigurala usklađenost postupanja sa zakonom. Ukupni troškovi koji proizlaze iz obveza izvješćivanja u svim zemljama mogli bi iznositi više od 12 000 EUR.*

Prema Reformi zaštite podataka: *zakon o zaštiti podataka u svih 14 država članica EU-a bit će jednak: jedna Europska unija – jedan zakon. Zbog toga se neće biti potrebno savjetovati s lokalnim odvjetnicima kako bi se osigurala usklađenost postupanja s lokalnim zakonom o prodavaonicama u franšiznom poslovanju. Time se izravno smanjuju troškovi i stvara pravna sigurnost.*

Kako će se reformom zaštite podataka poticati inovacije i uporaba velike količine podataka?

Prema nekim procjenama vrijednost osobnih podataka europskih građana mogla bi do 2020. narasti do gotovo jednog bilijuna EUR godišnje. Novim će se pravilima EU-a poduzećima pružiti fleksibilnost, a istodobno će se štititi temeljna prava pojedinaca.

„Tehnička i integrirana zaštita podataka" postat će temeljno načelo. To će potaknuti poduzeća na osmišljanje inovacija i razvoj novih ideja, metoda i tehnologija za sigurnost i zaštitu osobnih podataka. Primjena tog načela te procjene utjecaja zaštite podataka poduzećima će pružiti učinkovite alate za stvaranje tehnoloških i organizacijskih rješenja.

Uredbom se promiču tehnike za zaštitu osobnih podataka, kao što su **anonimizacija** (uklanjanje podataka koji omogućuju identifikaciju kada oni nisu potrebni), **pseudonimizacija** (zamjena podataka koji omogućuju identifikacju umjetnim identifikacijskim oznakama) i **šifriranje** (šifriranje poruka tako da ih mogu čitati samo ovlaštene osobe). Time se potiče primjena analize „ velikih količina podataka", za koju je moguće upotrijebiti anonimizirane ili pseudonimizirane podatke.

Primjer: samovozeći automobili

Za tehnologiju samovozećih automobila bitni su protoci podataka, uključujući razmjenu osobnih podataka. Pravila o zaštiti podataka idu ruku pod ruku s inovativnim i naprednim rješenjima. Na primjer, vozila koja su opremljena sustavom eCall za hitne pozive u slučaju sudara mogu automatski pozvati najbliži centar hitne pomoći. Ovo je primjer izvedivog i učinkovitog rješenja u skladu s načelima zaštite podataka u EU-u.

Primjenom novih pravila rad sustava eCall postati će lakši, jednostavniji i učinkovitiji u pogledu zaštite podataka. Načelo je zaštite podataka da kada se osobni podaci prikupljaju za jednu ili više svrha, ne bi se smjeli dalje obrađivati na način koji nije u skladu s izvornom svrhom. Time se ne zabranjuje obrada podataka u neku drugu svrhu niti se ograničava uporaba „neobrađenih podataka" u analizi.

Ključan čimbenik u odlučivanju o tome je li nova svrha nespojiva s prvotnom svrhom jest pitanje njezine poštenosti. Pri procjeni poštenosti uzimat će se u obzir čimbenici kao što su učinci na privatnost pojedinaca (npr. posebne i ciljane odluke o identificiranim osobama) te činjenica očekuje li pojedinac razumno da će se njegovi osobni podaci upotrebljavati na nov način.

U slučaju samovozećih automobila neobrađeni se podaci mogu upotrebljavati za analizu lokacija na kojima najčešće dolazi do nesreća te analizu načina kako bi se nesreće u budućnosti mogle izbjeći. Neobrađene je podatke moguće upotrijebiti i za analizu prometnih tokova radi smanjenja prometnih gužvi.

Poduzeća bi trebala moći predvidjeti moguće uporabe i koristi povezane s velikim količinama podataka te o njima obavijestiti pojedince, čak i ako još nisu poznate točne pojedinosti analize. Poduzeća bi trebala razmišljati o tome mogu li se podaci anonimizirati za potrebe tih budućih obrada. Na taj se način neobrađeni podaci mogu zadržati i upotrijebiti kao velike količine podataka, a istodobno se štite prava pojedinaca.

Novim se pravilima o zaštiti podataka poduzećima omogućuje da riješe problem nedostatka povjerenja, koji može utjecati na voljnost osoba da sudjeluju u inovativnim načinima uporabe osobnih podataka.

Pružanje jasnih i učinkovitih informacija pojedincima pomoći će u izgradnji povjerenja pojedinca u analizu i inovacije. Nije potrebno pružiti informacije o točnom načinu obrade podataka, već o njezinoj svrsi.

Prividna složenost inovativnih proizvoda i analize velikih količina podataka nije izgovor da se od osoba ne zatraži suglasnost kad je to potrebno. Međutim, suglasnost nije jedina osnova za obradu.

Poduzeća kao osnovu za obradu podataka mogu upotrijebiti ugovor, zakon ili u nedostatku drugih osnova, „usklađivanje interesa". Ti su „službeni zahtjevi", kao što je suglasnost, utvrđeni pravilima kojima se pojedincima pruža potrebna kontrola nad vlastitim podacima te se svima pruža pravna sigurnost. Novim pravilima EU-a omogućit će se fleksibilnost u pogledu ispunjavanja zahtjeva.

Kako će funkcionirati Europski odbor za zaštitu podataka?

Sva su europska tijela za zaštitu podataka trenutačno objedinjena u „radnoj skupini iz članka 29.", koja je utvrđena u skladu s člankom 29. Direktive o zaštiti podataka (Direktiva 95/46/EZ). To će se tijelo zamijeniti Europskim odborom za zaštitu podataka (EDPB), koji će se sastojati od predstavnika nacionalnih tijela za zaštitu podataka iz svake države članice EU-a, Europskog nadzornika za zaštitu podataka i Komisije (bez prava glasa). Predsjednik EDPB-a birat će se iz redova članova odbora. Jednako kao i radna skupina iz članka 29. Europski odbor za zaštitu podataka pratit će ispravnost primjene novih pravila o zaštiti podataka, savjetovati Europsku komisiju o relevantnim pitanjima te davati savjete i smjernice o raznim temama povezanima sa zaštitom podataka. U okviru Opće uredbe o zaštiti podataka EDPB će također donositi obvezujuće odluke u slučaju sporova između nacionalnih tijela za zaštitu podataka, što će poticati ujednačenu primjenu pravila o zaštiti podataka diljem EU-a.

Koje će se kazne primjenjivati za poduzeća koja prekrše nova pravila o zaštiti podataka?

Općom uredbom o zaštiti podataka utvrđuje se niz instrumenata za provedbu novih pravila, uključujući sankcije i novčane kazne. Kad je riječ o određivanju primjerene novčane kazne, svaki će se predmet pomno procijeniti, a u obzir će se uzeti niz čimbenika:

- težina/trajanje kršenja
- broj pogođenih ispitanika i razina štete koju su pretrpjeli
- namjera kršenja
- mjere poduzete za ublažavanje štete
- stupanj suradnje s nadzornim tijelom.

Uredbom se utvrđuju dvije gornje granice za novčane kazne u slučaju nepoštivanja pravila. Najviši iznos novčane kazne prvom se gornjom granicom utvrđuje na 10 milijuna EUR ili, u slučaju poduzeća, do 2 % ukupnog godišnjeg prometa na svjetskoj razini. Prva kategorija novčanih kazni primjenjuje se na primjer kada voditelj obrade podataka ne provede procjenu učinka, kako se zahtijeva Uredbom. Viša gornja granica za novčane kazne iznosi najviše 20 milijuna EUR ili 4 % godišnjeg prometa na svjetskoj razini. Kao primjer možemo navesti povredu prava ispitanika u okviru Uredbe. Kazne se prilagođavaju ovisno o okolnostima svakog pojedinog slučaja.

Kako se Općom uredbom o zaštiti podataka štite osobni podaci u slučaju kibernapada?

- **U skladu s Općom uredbom o zaštiti osobnih podataka podatke bi se trebalo obrađivati na način kojim bi se jamčila odgovarajuća sigurnost osobnih podataka**, uključujući sprečavanje neovlaštenog pristupa osobnim podacima i opremi za obradu podataka ili njihove neovlaštene uporabe. Iz tog bi razloga voditelj i izvršitelj obrade trebali procijeniti rizike povezane s obradom osobnih podataka te provesti mjere za ublažavanje tih rizika (članak 32. Opće uredbe o zaštiti osobnih podataka).
- **Voditelji obrade morat će obavijestiti ispitanike o povredama osobnih podataka bez nepotrebnog odlaganja.** Obveza će biti relevantna ako je vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode fizičke osobe, kako bi joj se omogućilo da poduzme nužne mjere opreza (članak 33. Opće uredbe o zaštiti osobnih podataka).
- **Voditelji obrade morat će o tome također obavijestiti relevantno nadzorno tijelo za zaštitu podataka, osim ako voditelj obrade može dokazati da nije vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode fizičkih osoba.** Te se obavijesti moraju dostaviti bez nepotrebnog odgađanja i, ako je moguće, najkasnije 72 sata nakon što je voditelj obrade za nju saznao (članak 34. Opće uredbe o zaštiti osobnih podataka).
- **Opća uredba o zaštiti podataka sadržava jasna pravila o uvjetima za izricanje upravnih novčanih kazni.** Tijela za zaštitu podataka moći će izricati kazne za poduzeća koja ne poštuju pravila EU-a, ako na primjer nisu obavijestila potrošače ili tijela za zaštitu podataka o povredama osobnih podataka.

Kako će se nova pravila primjenjivati u praksi?

Primjer: *multinacionalno poduzeće s nekoliko poslovnih nastana u državama članicama pruža uslugu internetskog sustava navigacije i kartiranja diljem EU-a. Taj sustav prikuplja slike svih privatnih i javnih zgrada, a može fotografirati i pojedince.*

Prema postojećim pravilima: *mjere za zaštitu podataka koje provode voditelji obrade bitno se razlikuju u državama članicama. U jednoj državi članici, uporaba te usluge dovela je do velikog nezadovoljstva u javnoj i političkoj sferi i neki su se njezini aspekti smatrali nezakonitima. Poduzeće je nakon pregovora s nadležnim tijelom za zaštitu podataka ponudilo dodatna jamstva i zaštitne mjere za pojedince koji borave u toj državi članici, no poduzeće se odbilo obvezati da će ponuditi ista dodatna jamstva za pojedince u drugim državama članicama. Voditelji obrade podataka koji posluju prekogranično trenutačno moraju trošiti vrijeme i novac (na pravne savjete i na pripremu potrebnih obrazaca ili dokumenata) u skladu s različitim, a nekad i proturječnim, obvezama.*

Prema novim pravilima: *novim se pravilima utvrđuje jedinstveno paneuropsko pravo o zaštiti podataka kojim se zamjenjuje trenutačna nedosljedna kombinacija nacionalnih prava. Svako poduzeće, bez obzira na to ima li poslovni nastan u EU-u ili ne, morat će primjenjivati pravo EU-a o zaštiti podataka ako svoje usluge želi nuditi u EU-u.*

Primjer: *malo marketinško poduzeće želi proširiti svoje aktivnosti iz Francuske u Njemačku.*

Prema postojećim pravilima: *njegove će djelatnosti obrade podataka podlijegati zasebnom skupu pravila u Njemačkoj i poduzeće će morati odgovarati novom regulatornom tijelu. Troškovi pribavljanja pravnih savjeta i prilagodbe poslovnih modela kako bi se ušlo na novo tržište mogu stvarati prepreku. Na primjer, neke države članice naplaćuju pristojbe za obavješćivanje za obradu podataka.*

Prema novim pravilima: *novim će se pravilima o zaštiti podataka ukinuti sve obveze obavješćivanja i troškovi koji su s njima povezani. Cilj je Uredbe o zaštiti podataka ukloniti prepreke prekograničnoj trgovini.*

MEMO/18/387

Osobe za kontakt s medijima:

Christian WIGAND (+32 2 296 22 53)
Melanie VOIN (+ 32 2 295 86 59)

Upiti građana: Europe Direct telefonom na 00 800 67 89 10 11 ili e-poštom