Awareness raising campaign for SMEs

GDPR Smjernice za mikro, male i srednje poduzetnike

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

An Coimisiún um Chosaint Sonraí Data Protection Commission

Croatian Personal Data Protection Agency azop Agencija za zaštitu osobnih podataka

VUB VRIJE UNIVERSITEIT BRUSSEL

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S RIGHTS, EQUALITY AND CITIZENSHIP 2014-2019 PROGRAMME UNDER GRANT AGREEMENT N°874524.

Što GDPR znači za Vaše poslovanje?

Opća uredba o zaštiti podataka (GDPR) stupila je na snagu 25. svibnja 2018. u svim državama članicama EU. GDPR pruža jedinstveni zakonodavni okvir o zaštiti podataka na području Europskog gospodarskog prostora, a isti predstavlja značajno usklađivanje zahtjeva i standarda zaštite podataka u cijeloj EU. Ovaj jedinstveni horizontalni zakonodavni okvir olakšava poslovanje organizacijama i poduzetnicima, promiče odgovornost pri postupanju s osobnim podacima i pomaže osigurati primjenu istih standarda zaštite podataka u cijeloj EU.

Iako je GDPR uredba Europske unije s izravnim učinkom, GDPR također pruža određeni prostor državama članicama EU za implementaciju daljnjeg zakonodavstva za postavljanje nacionalnih standarda u nekim područjima kao što su obrada zdravstvenih podataka i kaznenih presuda, dob za davanje privole u kontekstu nuđenja usluga informacijskog društva djetetu i okolnosti u kojima se prava pojedinca na zaštitu podataka mogu ograničiti. Sukladno tome, važno je da sve tvrtke i organizacije u Republici Hrvatskoj budu svjesne da se od njih traži da se pridržavaju standarda i obveza zaštite podataka iz GDPR-a te Zakona o provedbi Opće uredbe o zaštiti podataka (NN 42/18).

Ovaj vodič i prateće kontrolne liste osmišljeni su kako bi pomogli posebno malim i srednjim poduzećima (SMEs), koji vrlo često nemaju odgovarajuća financijska sredstva i ljudske resurse potrebne za usklađivanje s GDPR-om. Korištenje ovog vodiča trebalo bi pomoći organizacijama tijekom pripreme za poslovnu budućnost koja je usklađena sa zakonodavnim okvirom za zaštitu podataka.

Ako obrađujete osobne podatke kao dio svog poslovanja, na vas se primjenjuje GDPR. Važno je zapamtiti da:

- ✓ Podaci o kupcima i zaposlenicima su osobni podaci
- ✓ Jednostavno pohranjivanje osobnih podataka elektroničkim putem ili u tiskanom obliku predstavlja 'obradu' osobnih podataka.

Osnovne definicije iz GDPR-a

GDPR: Opća uredba o zaštiti podataka (2016/679) nova je uredba EU o zaštiti podataka koja je stupila na snagu 25. svibnja 2018.

Osobni podaci: Podaci koji se odnose na živu osobu koja je ili može biti identificirana, uključujući podatke koji se mogu kombinirati s drugim informacijama za identifikaciju pojedinca. Ovo može biti vrlo široka definicija, ovisno o okolnostima, i može uključivati podatke koji se odnose na identitet, karakteristike ili ponašanje pojedinca ili utječu na način na koji se ta osoba tretira ili procjenjuje.

Obrada: znači izvođenje bilo koje aktivnosti ili skupa aktivnosti na osobnim podacima, uključujući:

- ✓ dobivanje, bilježenje ili čuvanje podataka;
- ✓ organiziranje ili mijenjanje podataka;
- ✓ dohvaćanje, savjetovanje ili korištenje podataka;
- ✓ otkrivanje podataka trećoj strani (uključujući objavu); i

- ✓ brisanje ili uništavanje podataka.

Voditelj obrade podataka: Voditelj obrade je organizacija ili osoba koja odlučuje u koje svrhe i na koji način se osobni podaci obrađuju. Svrha obrade podataka uključuje "zašto" se osobni podaci obrađuju, a "sredstvo" obrade uključuje "kako" se podaci obrađuju.

Izvršitelj obrade: Osoba ili organizacija koja obrađuje osobne podatke u ime voditelja obrade.

Ispitanik: Ispitanik je osoba na koju se osobni podaci odnose (zaposlenici u organizaciji, klijenti, korisnici usluga, pojedinci).

Procjena učinka na zaštitu podataka (DPIA): opisuje proces osmišljen kako bi se identificirali rizici koji proizlaze iz obrade osobnih podataka i minimiziranje tih rizika u najvećoj mogućoj mjeri i što je prije moguće. Procjene učinka su važni alati za uklanjanje rizika i za dokazivanje usklađenosti s GDPR-om.

Pravna osnova za obradu: Za obradu osobnih podataka morate imati pravnu osnovu. Pravni temelji za obradu osobnih podataka navedeni su u članku 6. GDPR-a. To su privola pojedinca ili kada je obrada potrebna za: izvršenje ugovora; poštivanje zakonske obveze; zaštita životno važnih interesa osobe; obavljanje zadaće koja se obavlja u javnom interesu; ili u svrhu ostvarivanja legitimnih interesa tvrtke/organizacije ili nekog drugog (osim kada su ti interesi nadjačani interesima ili pravima i slobodama ispitanika).

Politika zadržavanja: Koliko dugo će vaša organizacija čuvati osobne podatke pojedinca? Na to će utjecati brojni čimbenici. Za vašu organizaciju mogu postojati zakonski zahtjevi, ovisno o vrsti vašeg poslovanja. Čuvajte podatke najkraće moguće vrijeme u skladu sa zahtjevima vašeg poslovanja, pohranite ih na siguran način dok su u vašem posjedu i pazite da ih potpuno i sigurno izbrišete u dogovoreno vrijeme.

Posebne kategorije osobnih podataka (osjetljivi podaci): oni su definirani u članku 9. stavku 1. GDPR-a kao podaci koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu te obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, podataka koji se odnose na zdravlje ili podataka o spolnom životu ili seksualnoj orijentaciji pojedinca. Obrada takvih podataka nije dopuštena osim ako je ispunjen jedan ili više uvjeta iz članka 9. stavka 2. GDPR-a. Ako je ovaj zahtjev ispunjen, voditelji obrade također moraju imati pravnu osnovu prema članku 6. za opravdanje obrade osobnih podataka posebne kategorije.

Privola: Člankom 7. GDPR-a ojačani su uvjeti potrebni za privolu kao pravnu osnovu za obradu osobnih podataka. Potrebno je razmotriti je li privola dana dobrovoljno i ispitanik mora imati mogućnost povući privolu za obradu u bilo kojem trenutku. Privola se ne smije pretpostaviti i mora se dobiti prije početka obrade podataka.

Ključni koraci za usklađenje s GDPR-om:

- ✓ Odredite koje osobne podatke posjedujete (to se može postići navođenjem informacija navedenih u članku 30. GDPR-a ili za manje tvrtke prilagođenim procesom kao što je popratni predložak koji identificira pojedinosti osobnih podataka koji se čuvaju).
- ✓ Provedite procjenu rizika osobnih podataka koje posjedujete i vaših aktivnosti obrade podataka (članak 24., uvodna izjava 75.)
- ✓ Uvedite odgovarajuće tehničke i organizacijske mjere kako bi se osiguralo da podaci (u digitalnim i papirnatim datotekama) budu sigurno pohranjeni. Sigurnosne mjere koje bi trebali primijeniti ovisit će o vrsti osobnih podataka koje posjedujete i riziku za vaše klijente i zaposlenike u slučaju da vaše sigurnosne mjere budu ugrožene (članak 32.).
- ✓ Identificirajte pravnu osnovu na koju se oslanjate (privola? ugovor? legitimni interes? zakonska obveza?) kako biste opravdali svoju obradu osobnih podataka (članci 6. do 8.).
- ✓ Osigurajte da prikupljate samo minimalnu količinu osobnih podataka koja je potrebna za poslovanje, te da su podaci točni i čuvani ne duže nego što je potrebno za svrhu za koju su prikupljeni (članak 5.).
- ✓ Budite transparentni sa svojim kupcima o razlozima za prikupljanje njihovih osobnih podataka, specifičnim namjenama u koje će se oni koristiti i koliko dugo trebate čuvati njihove podatke u arhivi (npr. putem obavijesti na vašoj web stranici ili natpisima na prodajnim mjestima) (članci 12., 13. i 14).
- ✓ Utvrdite spadaju li osobni podaci koje obrađujete u kategoriju posebnih kategorija (osjetljivih) osobnih podataka i, ako da, znajte koje dodatne mjere opreza trebate poduzeti (članak 9.).
- ✓ Odlučite hoćete li morati zadržati usluge službenika za zaštitu podataka (članak 37.).
- ✓ Budite u mogućnosti olakšati zahtjeve korisnika usluga koji žele ostvariti svoja prava prema GDPR-u, uključujući prava na pristup, ispravak, brisanje, povlačenje privole, prenosivost podataka i pravo na prigovor na automatiziranu obradu (članci 12. do 22.).
- ✓ Imajte ažurirane dokumente kao što su Politika privatnosti i/ili interne procedure.

Pristup usklađenosti s GDPR-om utemeljen na riziku

Kada vaša organizacija prikuplja, pohranjuje ili koristi (tj. obrađuje) osobne podatke, pojedinci čije podatke obrađujete mogu biti izloženi rizicima. Važno je da organizacije koje obrađuju osobne podatke poduzmu korake kako bi osigurale da se s podacima rukuje zakonito, sigurno, učinkovito i djelotvorno kako bi se zaštitili na najbolji mogući način.

Procjena rizika za prava i slobode pojedinaca ovisi o osobnim podacima koje vaša organizacija obrađuje i određuje se prema izvršenim aktivnostima obrade osobnih podataka, složenosti i opsegu obrade podataka, osjetljivosti obrađenih podataka i zaštiti potrebnoj za podatke koji se obrađuju. Na primjer, kada je aktivnost obrade podataka posebno složena ili kada je uključen veliki volumen ili osjetljivi podaci (tj. internetsko, zdravstveno, financijsko ili osiguravajuće društvo), ocjena rizika bila bi viša u odnosu na obrade osobnih podataka koje se odnose isključivo na pojedinosti o računu zaposlenika ili klijenta.

Kada analizirate profil rizika osobnih podataka koje vaša organizacija obrađuje, korisno je razmotriti opipljivu štetu za pojedince, a koji su detaljno navedeni u uvodnoj izjavi 75 GDPR-a i uključuju obradu koja bi mogla dovesti do: diskriminacije, krađe identiteta ili prijevare, financijskog gubitka, narušavanja ugleda, gubitka povjerljivosti osobnih podataka zaštićenih poslovnom tajnom, neovlaštenog ukidanja pseudonimizacije; ili bilo koji drugi značajan ekonomski ili društveni nedostatak.

Provođenje procjene rizika poboljšat će svijest u vašoj organizaciji o potencijalnim budućim problemima zaštite podataka povezanih s određenim projektom. To će zauzvrat pomoći da se poboljša dizajn vašeg projekta i poboljša vaša komunikacija o rizicima privatnosti podataka s relevantnim dionicima.

GDPR predviđa dva ključna koncepta za buduće planiranje aktivnosti: tehničku i integriranu zaštitu podataka. Iako se preporučuje kao dobra praksa, oba su ova načela sadržana u GDPR-u (članak 25.).

Tehnička zaštita podataka znači ugrađivanje značajki privatnosti podataka i tehnologija za poboljšanje privatnosti podataka izravno u dizajn projekata u ranoj fazi. To će pomoći da se osigura bolja i isplativija zaštita osobnih podataka.

Integrirana zaštita podataka znači da postavke korisničke usluge moraju biti automatski prilagođene zaštiti podataka (npr. izbjegavati automatsko uključivanje postavki privatnosti korisnika), te da se samo podaci koji su nužni za svaku specifičnu svrhu obrade trebaju prikupljati i obrađivati.

Prema GDPR-u, procjena učinka na zaštitu podataka obvezan je zahtjev za prethodnu obradu kada predviđeni projekt/inicijativa/usluga uključuje obradu podataka koja "može imati veliki rizik za prava i slobode fizičkih osoba". To je osobito važno kada se u vašoj organizaciji uvodi nova tehnologija obrade podataka. U slučajevima u kojima nije jasno je li procjena učinka strogo obvezna, provođenje procjene učinka i dalje može biti najbolji pristup i vrlo koristan alat koji pomaže voditeljima obrade da pokažu svoju usklađenost sa zakonodavstvom o zaštiti podataka. Procjene učinka mogu imati različite oblike, ali GDPR postavlja osnovne zahtjeve učinkovite procjene učinka.

Održavanje registra rizika zaštite podataka može vam omogućiti da identificirate i ublažite rizike zaštite podataka, kao i da dokažete usklađenost u slučaju regulatorne istrage ili revizije.

Alati za provjeru usklađenosti sa GDPR-om:

Osim općeg popisa za provjeru usklađenosti s GDPR-om, u nastavku možete pronaći detaljnija pitanja iz sljedećih područja:

- ✓ Osobni podaci
- ✓ Prava ispitanika
- ✓ Točnost i čuvanje podataka
- ✓ Zahtjevi transparentnosti
- ✓ Ostale obveze voditelja obrade
- ✓ Zaštita podataka

- ✓ Povrede podataka
- ✓ Međunarodni prijenosi podataka

Sljedeća tablica pomoći će organizacijama u mapiranju osobnih podataka koje obrađuju, identificiranju pravne osnove i razdoblja čuvanja za svaku kategoriju podataka. Provođenje ove vježbe pomoći će identificirati gdje su potrebne hitne korektivne radnje kako bi se organizacija uskladila s GDPR-om.

Kategorije osobnih podataka i ispitanika	**Vrste osobnih podataka**	**Izvor osobnog podatka**	**Svrhe u koje se obrađuju osobni podaci**	**Pravna osnova za obradu**	**Posebne kategorije osobnih podataka**	**Pravne osnove za obradu posebnih kategorija osobnih podataka**	**Rok pohrane podataka**	**Aktivnosti potrebne za usklađenje s GDPR-om?**
npr. podaci o zaposlenicima; podaci o umirovljenim zaposlenicima; podaci o kupcima (podaci o prodaji); marketinška baza podataka; snimke videonadzora.	npr. ime, adresa, bankovni podaci, povijest kupnje, povijest pregledavanja na mreži, video i slike	Navedite izvor(e) osobnih podataka, npr. prikupljeni izravno od pojedinaca; od trećih strana	Unutar svake kategorije osobnih podataka navedite svrhe za koje se podaci prikupljaju i pohranjuju, npr. marketing, poboljšanje usluga, istraživanje, razvoj proizvoda, integritet sustava, pitanja ljudskih resursa, oglašavanje.	Za svaku svrhu u koju se osobni podaci obrađuju navedite pravnu osnovu na kojoj se temelje npr. privola, ugovor, zakonska obveza (članak 6.).	Ako se prikupljaju i pohranjuju posebne kategorije osobnih podataka, navedite pojedinosti o prirodi podataka, npr. zdravstveni, genetski, biometrijski podaci.	Navedite pravnu osnovu na temelju koje se prikupljaju i pohranjuju posebne kategorije osobnih podataka npr. izričita privola, zakonska osnova (članak 9.).	Za svaku kategoriju osobnih podataka navedite razdoblje u kojem će se podaci pohranjivati npr. jedan mjesec? jedna godina? Kao opće pravilo, podaci se ne smiju čuvati duže nego što je potrebno za svrhu za koju su uopće prikupljeni.	Identificirajte radnje koje su potrebne kako bi se osiguralo da su sve aktivnosti obrade osobnih podataka usklađene s GDPR-om, npr. to može uključivati brisanje podataka ako nema daljnje svrhe zadržavanja

Osobni podaci

	Pitanje	Da	Ne	Komentari/popravna radnja
Obrada osobnih podataka temljem privole (Članci 7., 8. i 9.)	Jeste li pregledali mehanizme svoje organizacije za prikupljanje privole kako biste osigurali da je ona dobrovoljno dana, posebna, informirana i da je jasan pokazatelj da je pojedinac odlučio pristati na obradu svojih podataka putem izjave ili jasne potvrdne radnje.			
	Ako su osobni podaci pohranjeni na temelju privole, zadovoljava li privola zahtjeve iz GDPR-a?			
	Jeste li uspostavili proceduru koja pojedincu omogućuje povlačenje privole za obradu svojih osobnih podataka?			
Obrada osobnih podataka djece (Članak 8.)	Kada se djetetu pružaju internetske usluge, postoje li postupci za provjeru dobi i dobivanje privole od roditelja/nositelja roditeljske odgovornosti, gdje je to potrebno?			
Obrada osobnih podataka na temelju legitimnog interesa	Ako je legitimni interes pravna osnova na kojoj se obrađuju osobni podaci, je li provedena odgovarajuća analiza kako bi se osiguralo da je korištenje ove pravne osnove primjereno? (analiza mora pokazati da 1) postoji valjani legitimni interes, 2) da je obrada podataka nužna u svrhu ostvarivanja legitimnog interesa, i 3) da obrada ne šteti pravima pojedinca).			

Prava ispitanika

	Pitanje	Da	Ne	Komentari/popravna radnja
Pristup osobnim podacima (Članak 15.)	Postoji li dokumentirana politika/procedura za slučajeve kad ispitanik zatraži pristup svojim osobnim podacima?			
	Je li vaša organizacija u stanju odgovoriti na takav zahtjev u roku od mjesec dana?			
Pravo na prenosivost podataka (Članak 20.)	Jesu li uspostavljene procedure kojima se pojedincima dostavljaju njihovi osobni podaci u strukturiranom, uobičajeno korištenom i strojno čitljivom formatu?			
Pravo na ispravak i brisanje (Članci 16. i 17.)	Postoje li kontrole i postupci koji omogućuju brisanje ili ispravljanje osobnih podataka (gdje je primjenjivo)?			
Pravo na ograničenje obrade (Članak 18.)	Postoje li kontrole i postupci za zaustavljanje obrade osobnih podataka ako je pojedinac iz valjanih razloga zatražio ograničenje obrade?			
Pravo na prigovor na obradu osobnih podataka (Članak 21.)	Jesu li pojedinci informirani o svom pravu na prigovor na određene vrste obrade kao što je izravni marketing ili u slučaju kad je pravni temelj za obradu legitimni interesi ili je obrada nužna za zadatak koji se obavlja u javnom interesu?			
	Postoje li kontrole i postupci za prestanak obrade osobnih podataka ako se pojedinac usprotivio obradi?			
Automatizirano pojedinačno donošenje odluka, uključujući izradu profila (Članak 22.)	Ako se automatizirano donošenje odluka, koje ima pravni ili značajan sličan utjecaj na pojedinca, temelji na privoli, je li prikupljena izričita privola?			
	Kada se donese automatizirana odluka koja je neophodna za sklapanje ili izvršenje ugovora ili se temelji na izričitoj privoli pojedinca, je li podjedinac u mogućnosti ostvariti svoje pravo na ljudsku intervenciju i osporavanje odluke?			
Ograničenja prava ispitanika (Članak 23.)	Jesu li dokumentirane okolnosti u kojima se prava pojedinca na zaštitu podataka mogu zakonski ograničiti?			

Točnost i ograničenje pohrane

	Pitanje	Da	Ne	Komentari/popravna radnja
Ograničavanje svrhe	Koriste li se osobni podaci samo u svrhe za koje su izvorno prikupljeni?			
Smanjenje količine podataka	Jesu li prikupljeni osobni podaci ograničeni na ono što je nužno za svrhe u koje se obrađuju?			
Točnost	Jesu li uspostavljeni postupci kojima se osigurava da su osobni podaci ažurni i točni, a gdje je potreban ispravak, potrebne promjene se vrše bez odgađanja?			
Ograničenje pohrane	Jesu li uspostavljene politike i postupci zadržavanja podataka kako bi se osiguralo da se podaci čuvaju ne duže nego što je potrebno za svrhe u koje su prikupljeni?			
Ostale pravne obveze vezane uz pohranu	Podliježe li vaše poslovanje drugim pravilima koja zahtijevaju minimalno razdoblje čuvanja (npr. medicinske/porezne evidencije)?			
	Imate li uspostavljene postupke koji osiguravaju da su podaci sigurno uništeni, u skladu s vašim politikama zadržavanja?			
Umnožavanje spisa	Jesu li uspostavljene procedure koje osiguravaju da nema nepotrebnog ili nereguliranog umnožavanja zapisa?			

Zahtjevi transparentnosti

	Pitanje	Da	Ne	Komentari/popravna radnja
Transparentnost prema klijentima i zaposlenicima (Članci 12., 13. i 14.)	Jesu li korisnici/zaposlenici usluga u potpunosti i na sažet, transparentan, jedsnostavan i razumljiv način informirani o tome kako koristite njihove podatke? Jesu li te informacije korisnicima/zaposlenicima lako dostupne?			
	Kada se osobni podaci prikupljaju izravno od pojedinaca, postoje li postupci za pružanje informacija navedenih u članku 13. GDPR-a?			
	Jesu li uspostavljeni postupci kojima se osigurava da su osobni podaci ažurni i točni, a gdje je potreban ispravak, potrebne promjene se vrše bez odgađanja?			
	Ako se osobni podaci ne prikupljaju od ispitanika, već od treće strane, postoje li postupci za pružanje informacija navedenih u članku 14. GDPR-a?			
	Pri interakciji s pojedincima, kao što je pružanje usluge, prodaja robe ili videonadzor, da li se pojedince proaktivno informira o njihovim pravima iz GDPR-a?			
	Jesu li informacije o načinu na koji organizacija omogućava pojedincima ostvarivanje prava iz GDPR-a objavljene u lako dostupnom i čitljivom formatu?			

Ostale obveze voditelja obrade

	Pitanje	Da	Ne	Komentari/popravna radnja
Ugovori s dobavljačima (Članci 27. do 29.)	Jesu li ugovori s dobavljačima i drugim trećim stranama koji obrađuju osobne podatke u vaše ime pregledani kako bi se osiguralo da su uključeni svi odgovarajući zahtjevi zaštite podataka?			
Službenici za zaštitu podataka (Članci 37. do 39.)	Trebate li imenovati službenika za zaštitu podataka prema članku 37. GDPR-a?			
	Jeste li kontakt podaci službenika za zaštitu podataka javno dostupni?			
	Jeste li AZOP-u dostavili izvješće/odluku o imenovanju službenika za zaštitu podataka?			
Procjena učinka na zaštitu podataka (Članak 35.)	Ako se vaša obrada podataka smatra visokorizičnom, imate li postupak za utvrđivanje potrebe i provođenje procjene učinka? Jesu li ti postupci dokumentirani?			

Ostale obveze voditelja obrade

	Pitanje	Da	Ne	Komentari/popravna radnja
Odgovarajuće tehničke i organizacijske mjere (Članak 32.)	Jeste li procijenili rizike povezane s obradom osobnih podataka i poduzeli mjere za njihovo ublažavanje?			
Dokumentirani sigurnosni program	Postoji li dokumentirani proces za rješavanje pritužbi i pitanja vezanih uz sigurnost koji specificira tehničke, administrativne i fizičke mjere zaštite za osobne podatke?			
	Postoji li određena osoba koja je odgovorna za sprječavanje i istraživanje povreda osobnih podataka?			
	Primjenjuju li se standardne tehnologije enkripcije za prijenos, pohranu i primanje osjetljivih osobnih podataka pojedinaca?			
	Jesu li osobni podaci sustavno uništavani, brisani ili anonimizirani kada ih više nije zakonski potrebno čuvati?			
	Može li se pristup osobnim podacima pravovremeno vratiti u slučaju fizičkog ili tehničkog incidenta?			

Povrede podataka

	Pitanje	Da	Ne	Komentari/popravna radnja
Obveze vezane uz povrede osobnih podataka (Članci 33. i 34.)	Ima li organizacija dokumentiran plan odgovora na incidente u vezi s privatnošću i sigurnošću osobnih podataka?			
	Postoje li postupci za obavještavanje tijela za zaštitu podataka o povredi podataka?			
	Postoje li postupci za obavještavanje ispitanika o povredi podataka (gdje je primjenjivo)?			
	Preispituju li se planovi i procedure redovito?			
	Jesu li sve povrede podataka u potpunosti dokumentirane?			
	Postoje li postupci suradnje između voditelja obrade podataka, dobavljača i drugih partnera za rješavanje povreda podataka?			

Prijenosi osobnih podataka trećim zemljama ili međunarodnim organizacijama

	Pitanje	Da	Ne	Komentari/popravna radnja
Prijenosi osobnih podataka trećim zemljama ili međunarodnim organizacijama (Članci 44. do 50.)	Prenose li se osobni podaci izvan EGP-a, npr. u SAD ili druge zemlje?			
	Uključuje li to neke posebne kategorije osobnih podataka?			
	Koja je svrha transfera?			
	Kome se prenose podaci?			
	Jesu li navedeni svi prijenosi osobnih podataka, uključujući i svrhu obrade, iz koje se zemlje izvoze i koja zemlja prima podatke i tko je primatelj osobnih podataka?			
Zakonitost međunarodnih prijenosa	Postoji li pravna osnova za prijenos, npr. odluka Komisije o primjerenosti; standardne ugovorne klauzule. Jesu li te baze dokumentirane?			
Transparentnost	Jesu li ispitanici u potpunosti obaviješteni o namjeravanim međunarodnim prijenosima njihovih osobnih podataka?			