INSTITUT ZA EKONOMSKU DIPLOMATIJU

POLITIKA ZAŠTITE PODATAKA O LIČNOSTI

Beograd, 2019

Evidencija promena

Oznaka:	IED-GDPR
Verzija:	01
Datum verzije:	21.8.2019.
Izradio:	Gojko Grubor
Verifikovao:	Prof. dr Miroslav Raičević
Odobrio:	Prof. dr Miroslav Raičević
Nivo poverljivosti:	Interna
Vlasnik politike:	Lice imenovano za obavljanje poslova zaštite podataka o ličnosti
Čuvanje politike:	U web serveru Kompanije u e-formi i u glavnoj arhivi u štampanoj formi
Lice zaduženo za zaštitu podataka o ličnosti i Lice za kontakt	Olivera Žižović, e-mail: ozizovic@economicdiplomacy.co.rs

Sadržaj

1. Namena, obim i korisnici

Institut za ekonomsku diplomatiju, Zemun, Beograd (u nastavku **IED**), namerava da se usaglasi sa primenljivim zakonima i regulativama Republike Srbije koje se odnose na zaštitu podataka o ličnostima. Ova politika ističe osnovne principe obrade ličnih podataka kupaca, dobavljača, poslovnih partnera, zaposlenih i drugih pojedinaca ili predstavnika zakona (u nastavku **Klijenti**) i ukazuje na odgovornosti Kompanije i zaposlenih u radnjema obrade podataka.
Ova politika se primenjuje na Kompaniju i njena povezana društva.
Korisnici ovog dokumenta su stalno ili privremeno zaposleni i svi podugovarači koji rade u ime Kompanije.

2. Referentna dokumenta

- EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
- *Zakon o zaštiti podataka o ličnosti ("Sl. glasnik RS", br. 87/2018)*
- *Zakon o informacionoj bezbednosti Republike Srbije*, „Sl. Glasnik RS ", br. 6/2016
- *Zakon o obligacioni odnosima Republike Srbije*, *("Sl. list SFRJ", br. 29/78, 39/85, 45/89 - odluka USJ i 57/89, "Sl. list SRJ", br. 31/93 i "Sl. list SCG", br. 1/2003 - Ustavna povelja)*

3. Definicije termina

Definicije termina korišćene u ovom dokument su sadržane u Članu 4 Zakona o zaštiti podataka o ličnosti (u daljem tekstu **ZZPL**):

Podaci o ličnosti: Svaka informacija koja se odnosi na identifikaciju ili lične identifikacione informacije fizičkih lica (*lica na koje se podaci odnose*) koja mogu biti direktno ili indirektno identifikovana, posebno na osnovu nekog identifikatora kao što je ime, lični broj, podatak o lokaciji, ili jedan ili više faktora specifičnih za fizički, psihološki, genetski, mentalni, ekonomski, kulturološki ili društveni identitet fizičkog lica.

Osetljivi podaci o ličnosti: Podaci o ličnosti koji po svojoj prirodi, posebno osetljivosti za prava i slobode lica na koja se podaci odnose, zaslužuju specifične mere zaštite pošto kontekst (radnje) obrade podataka može izazvati visok rizik za fundamentalna prava i slobode fizičkih lica. Ovi podaci uključuju rasnu ili etičku pripadnost, religijsko ili filozofska uverenje, genetičke podatke, biometrijske podatke za jedinstvenu identifikaciju fizičkih lica.

Rukovalac podataka: Fizičko ili pravno lice, predstavnik javne vlasti, agencija ili drugo telo koje samo ili zajedno određuje namenu i sredstva obrade ličnih podataka.

Obrađivač podataka: Fizičko ili pravno lice, predstavnik javne vlasti, agencija ili drugo telo koje obrađuje lične podatke u ime kontrolora.

Obrada: Svaka operacija ili skup operacija koje se izvršavaju nad ličnim podacima ili skupu ličnih podataka, manuelnim ili automnatizovanim sredstvima, kao što su: *skupljanje, snimanje, organizacija, struktuiranje, pohranjivanje, adaptacija ili izmena, izvlačenje, konsultovanje, upotreba, otkrivanje prenosom, distribucija ili stavljanje na raspolaganje na drugi način, usklađivanje ili kombinovanje, restrikcija, brisanje ili uništavanje podataka.*

Anonimizacija (sinonim: **šifrovanje**) **:** Nepovratan proces naknadne identifikacije ličnih podataka tako da fizičko lice ne može biti identifikovano u razumnom vremenu, sa razumnim troškovima i tehnologijom bilo od strane rukovaoca ili drugih lica za identifikaciju tog lica. Principi obrade ličnih podataka ne primenjuju se na anonimizovane podatke koji nisu više podaci o ličnosti lični.

Pseudonimizacija (sinonim: **kodiranje**)**:** Obrada ličnih podataka na takav način da na dalje ne može biti povezan sa specifičnim fizičkim licem bez upotrebe dodatnih informacija. Takve dodatne informacije moraju da se drže odvojeno i da su zaštićene tehničkim i organizacionim merama koje osiguravaju da se podaci o ličnosti ne mogu pridružiti fizičkom licu. Pseudonimizacija smanjuje, ali ne eliminiše potpuno sposobnost povezivanja ličnih podataka sa fizičkim licem na koga se podaci odnose. Ovi podaci su još uvek lični podaci i na njih se odnose načela obrade ličnih podataka.

Nadzorno telo (*Supervisory Authority*)**:** Nezavisno javno telo koje je uspostavljeno u državama članicama EU prema čanu 51 EU GDPR i u Republici Srbiji prema Članu 73 Zakona, Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti.

Glavno sedište rukovaoca (*Main establishment as regards a controller*)**:** Glavno sedište rukovaoca je mesto glavne adminsnistracije IED u Srbiji.

Glavno sedište obrađivača (*Main establishment as regards a processor*): Glavno sedište obrađivača IED je na mestu glavne administracije IED u Srbiji.

4. Osnovna načela obrade podataka o ličnosti

Načela (principi) zaštite podataka opisuju osnovne odgovornosti organizacije koja rukuje podacima o ličnosti. Prema članu 4(8) Zakona rukovalac (kontrolor) „je fizičko ili pravno lice, odnosno organ vlasti koji samostalno ili zajedno sa drugima određuje svrhu i način obrade. Zakonom kojim se određuje svrha i način obrade, može se odrediti i rukovalac ili propisati uslovi za njegovo određivanje“ .

4.1. Zakonitost, poštenje i transparentnost

Podaci o ličnosti moraju se skupljati i obrađivati zakonito, pošteno i transparentno u odnosu na lice na koje se podaci odnose (GDPR princip "zakonitosti, poštenja i transparentnosti"). Zakonita obrada je obrada koja se vrši u skladu sa ZZPL, Član 5(1), odnosno drugim zakonom kojim se uređuje obrada.

4.2. Ograničenje namene

Podaci o ličnosti moraju se prikupljati u svrhe koje su konkretno određene, izričite, opravdane i zakonite i dalje se ne mogu obrađivati na način koji nije u skladu sa tim svrhama (na primer, profilisanje i marketing) ("ograničenje u odnosu na svrhu obrade", ZZPL, član 5(2)).

4.3. Minimizacija podataka

Lični podaci skupljani, obrađivani i pohranjivani u Kompaniji moraju biti adekvatni, relevantni i ograničeni na minimalnu količinu koja je neophodna za namene za koje su skupljani, obrađivani i pohranjivani. IED mora primeniti anonimizaciju ili pseudonimizaciju podataka o ličnosti ako postoji visok rizik za prava i slobode fizičkih lica i mogućnost da se smanji rizik za fizička lica.

4.4. Tačnost

Podaci o ličnosti skupljeni u Kompaniji moraju biti tačni i, gde je neophodno, ažurno održavani. IED će preduzeti racionalne korake da se netačni lični podaci, imajući u vidu namenu za koju su skupljani i obrađivani, blagovremeno izbrišu ili isprave (ZZPL, član 5(4)).

4.5. Ograničen period čuvanja

Lični podaci će se čuvati u Kompaniji u obliku koji omogućava identifikaciju lica samo u roku koji je neophodan za ostvarivanje svrhe obrade ("ograničenje čuvanja", ZZPL, član 5(5).

4.6. Integritet, poverljivost i raspoloživost

Uzimajući u obzir poslednju tehnologiju i druge raspoložive mere zaštite podataka i informacija, troškove implementacije i verovatnoću i intenzitet rizika za lične podatke, IED mora primeniti odgovarajuće tehničke i organizacione mere za obradu ličnih podataka na način koji osigurava odgovarajuću bezbednost ličnih podataka, uključujući raspoloživost kada su potrebni i zaštitu od slučajnog ili nezakonitog uništenja, gubitka, izmene, neovlašćenog pristupa ili otkrivanja (ZZPL, član 5(6)).

4.7. Kontrolisana odgovornost (Accountability)

Direktor IED kao rukovalac (kontrolor) podataka je odgovoran i sposoban da demonstrira usaglašenost sa gore opisanim načelima ZZPL, implementira i održava mere adekvatne zaštite podataka o ličnosti.

5. Izgradnja sistema zaštite podataka u poslovnim radnjema IED

Da bi demonstrao usaglašenost sa načelima zaštite podataka o ličnosti Zakona, IED će ugraditi sistem zaštite podataka u poslovne procese i radnje obrade podataka o ličnostii.

5.1. Obaveštavanje fizičkih lica

IED će objaviti *Obaveštenje o privatnosti klijenata* na web sajtu IED i napraviti link prema ovoj Politici. *Obaveštenje o privatnosti klijenata* treba da sadrži sve neophodne informacije koje se odnose na skupljanje podataka, radnje obrade, vreme zadržavanja podataka, mere zaštite podataka, lokaciju obrade, odgovornosti itd. (videti sekciju 6.1 Politike).

5.2. Izbor i pristanak fizičkog i pravnog lica

U poslovanju IED fizička lica za korišćenje usluga IED daju pristanak za obradu svojih podataka o ličnosti neposrednim prijavljivanjem za školu/seminar/kurs/radionici na osnuvu raspoloživih informacija u *Obaveštenju o zaštiti privatnosti klijenata*. Pravna lica (lica na koja se podaci odnose) daju eksplicitno svoj pristanak za skupljanje i obradu njihovih ličnih podataka u zakonski uzajamno prihvaćenim i potpisanim sporazumima/ugovorima (videti 6.2 sekciju Politike) za davanje usluga.

5.3. Skupljanje podataka

IED će nastojati da skuplja što je manju moguću količinu ličnih podataka. Ako lične podatke u ime IED skuplja treća strana, Lice zaduženo za zaštitu podataka o ličnosti u IED, mora osigurati da se lični podaci skupljaju na zakonskoj osnovi.

5.4. Upotreba, zadržavanje i odlaganje podataka

Namene i metodi obrade, ograničeno pohranjivanje i zadržavanje ličnih podataka mora biti konzistentno sa informacijama sadržanim u *Obaveštenju o privatnosti klijenata*. IED će održavavati tačnost, integritet, poverljivost, raspoloživost, otpornost na incidente i relevantnost podataka o ličnosti kroz sve namenjene radnje obrade. Adekvatne tehničke, organizacione i kadrovske mere zaštite projektovane su u IED da štite lične podatke od krađe, uništavanja, izmene, brisanja ili zloupotrebe i spreče proboj ličnih podataka. Direktor IED je odgovoran za usaglašenost navedenu u ovoj sekciji:

(1) Kopiranje ili dupliranje podataka nikada se ne sme vršiti bez znanja Direktora IED, sa izuzetkom stvaranja rezervnih kopija (bekapovanja), osim ako je neophodno za osiguranje namenjene radnje obrade, kao i za regulatorno zadržavanje podataka.
(2) Posle zaključivanja rada po ugovoru/SLA, ili ranije po zahtevu IED, a najkasnije po završetku ugovornih/SLA obaveza, IED će na zahtev prethodnog pristanka klijenta, izbrisati, ili šifrovati (anonimizovati) podatke i arhivirati zajedno sa ugovorima/SLA za čuvanje u zakonskom periodu (do 10 godina) ili po potrebi duže, ako je u legitimnom interesu IED.
(3) Dokumentacija koja je korišćena da demonstrira regularnu obradu podataka u skladu sa ugovorima/SLA, IED će pohraniti i čuvati duže od perioda trajanja ugovora/SLA u skladu sa odgovarajućim zakonskim periodom zadržavanja ili legitimnim interesom IED.

5.5. Otkrivanje podataka trećim stranama

Kad god IED koristi poverljivu treću stranu (dobavljača ili poslovnog partnera) da obrađuje podatke o ličnosti u njeno ime, Lice imenovano za poslove zaštite ličnih podataka, mora osigurati da će obrađivač obezbediti adekvatne tehničke, organizacione i kadrovske mere zaštite podataka o ličnosti koje su proporcioanlne procenjenom riziku.

IED mora ugovorom zahtevati od treće strane (dobavljača ili poslovnog partnera) da obezbedi isti nivo zaštite privatnosti i bezbednosnih mera za zaštitu ličnih podataka. Dobavljač ili poslovni partner moraju obrađivati lične podatke samo da ispune svoje ugovorne/SLA obaveze prema IED ili na osnovu instrukcije koja može sadržavati zakonske, legitimne i druge interese IED i nikako za druge svrhe. Ako dobavljač ili partner obrađuje lične podatke IED zajedno sa nezavisnom trećom stranom od poverenja, IED mora eksplicitno specifikovati njihove odgovornosti, a treća strana dobavljača mora potpisati relevantan ugovor /SLA ili drugi legalni obavezujući dokument, kao što je *Sporazum o obradi podataka sa dobavljačem/ partnerom*.

(1) Dobavljač/partner će osigurati da IED može verifikovati usaglašenost sa obavezama dobavljača/ partnera u skladu sa članom 26 ZZPL. Dobavljač/partner će na zahtev IED dostaviti neophodne informacije o tehničkim, organizacionim i kadrovskim merama zaštite podataka i, posebno, demonstrirati primenu mera zaštite podataka. Dokaz o primeni ovih mera može se obezbediti:
   a. Usaglašavanjem sa kodeksom postupanja u skladu sa čl. 59, ZZPL ili sertifikatom usaglašenosti sa odobrenom procedurom sertifikacije prema Članu 61, ZZPL;
   b. Važećim sertifikatom o proveri, izveštajem ili delom izveštaja obezbeđenog od strane nezavisnog tela (na primer: Lica za zaštitu podataka o ličnosti, Odeljenja IT sektora za informacionu bezbednost, inspektora (proverivača) za proveru zaštite privatnosti podataka, ili proverivača sistema kvaliteta);
   c. Odgovarajućim sertifikatom od strane internog ili nezavisnog tima za sertifikaciju informacione bezbednosti (na primer ISO/IEC 27001);

(2) Gde je, u pojedinačnim slučajevima, neophodna provera i kontrola IED ili proverivača kojeg IED postavi, takva provera i kontrola mora se vršiti u radno vreme i bez interferencije sa operacijama dobavljača/partnera, na osnovu prethodnog obaveštenja i posmatranjem odgovarajućeg perioda na koji se obaveštenje odnosi. Dobavljač/partner može takođe odrediti da je takva provera i kontrola predmet prethodnog obaveštenja, opservacije odgovarajućeg perioda za koji se obaveštenje daje i izvršavanje preduzetih mera poverljivosti za zaštitu podataka drugih kupaca ili dobavljača i poverljivosti implementiranih tehničkih, organizacionih i kadrovskih mera zaštite. Dobavljač/partner je ovlašćen da odbije proverivače/partnere koji su im konkurencija;

(3) Gde za IED inspekciju vrši Poverenik za zaštitu podataka o ličnosti ili drugi ovlašćeni organ sa statutarnim kompetencijama, gornji paragraf 2 će se primeniti sa mogućnošću neophodnih izmena. Izvršavanje preduzetih mera zaštite poverljivosti

neće se zahtevati, ako takvo nadzorno telo ima profesionalnu ili statutarnu obavezu zaštite poverljivosti čije je kršenje predmet sankcija prema primenljivom krivičnom zakonu.

5.6. Prekogranični prenos podataka o ličnosti

Pre prenosa ličnih podataka izvan Republike Srbije (Član 63, ZZPL) moraju se koristiti adekvatne mere samozaštite obezbeđene u standardnom članu Ugovora, uključujući potpisivanje *Ugovor o prenosu podataka*, kako EU GDPR i ZZPL zahtevaju, i u situacijama gde to drugi propisi zahtevaju, sa dobijenim ovlašćenjem lokalnog nadležnog tela za zaštitu podataka (*Poverenik za zaštitu podataka o ličnosti u Srbiji*). Entitet koji prima lične podatke mora se usaglasiti sa skupom principa obrade ličnih podataka opisanih u proceduri *Prekograničnog prenosa podataka koju propisuje Poverenik*.

Opšta načela prenosa podataka (Član 63, ZZPL):

Svaki prenos ličnih podataka koji podležu obradi ili su namenjen za obradu posle prenosa u treću zemlju ili u neku međunarodnu organizaciju izvršiće se samo ako, podležu drugim odredbama (čl. 64, 65. i 67. ovog ZZPL), ako su uslovi postavljeni u ovom poglavlju usaglašeni sa rukovaocem i obrađivačem, uključujući i za dalji prenos ličnih podataka iz jedne treće zemlje ili međunarodne organizacije u drugu treću zemlju ili međunarodnu organizaciju. Sve odredbe u ovom poglavlju biće primenjene da bi se osigurao nivo zaštite fizičkih lica zagarantovan ZZPL. Rukovalac je odgovoran da vodi evidenciju o prenosu podataka o ličnosti u druge države ili međunarodne organizacije (Član 47(5) ZZPL), uključujući i naziv druge države ili međunarodne organizacije, kao i dokumente o primeni mera zaštite ako se podaci prenose u skladu sa članom 69. stav 2. ZZPL.

Prenos podataka podleže odgovarajućim merama samozaštite (Član 64 ZZPL):

(1) U odsustvu odluke prema članu 64(3) ZZPL, rukovalac ili obrađivač može preneti lične podatke u neku treću zemlju ili neku međunarodnu organizaciju, samo ako je rukovalac ili obrađivač obezbedio odgovarajuće mere samozaštite (Član 65 ZZPL), i pod uslovom da su raspoložive mere koje nameću prava lica na koja se podataci odnose i efektivni pravni lek za otklanjanje posledica.
(2) Odgovarajuće mere samozaštite navedene u paragrafu 1 mogu se obezbediti, bez zahteva bilo kojeg specifičnog ovlašćenja, od nadzornog organa, sa:

(a) Zakonskim obavezujućim i instrumentom koji nameće obavezu izvršavanja sa javnom vlasti ili nadleđnim telom;

(b) Obavezujućim organizacionim pravilima za evidenciju radnji obrade u skladu sa članom 47 ZZPL;

(c) Standardnim klauzulama zaštite podataka usvojenim od strane EU Komisije u skladu sa procedurom ispitivanja navedenom u Članu 93(2) GDPR i Članu 50, ZZPL;

(d) Standardnim klauzulama zaštite podataka usvojenim od nadzornog organa i odobrenog od EU Komisije prema Članu 93(2) GDPR i Članu 51 Z ZZPL;

(e) Odobrenim kodom kontrola zaštite prema Članu 59, Zakona zajedno sa obavezujućim i nametnutim angažovanjem rukovaoca i obrađivača u trećoj zemlji za primenu adekvatnih mera samošaštite, uključujući zaštitu prava vlasnika ličnih podataka; ili

(f) Odobren mehanizam sertifikacije prema Člnu 61 ZZPL zajedno sa obavezujućim i nametnutim angažovanjem rukovaoca i obrađivača u trećoj zemlji za primenu odgovarajućih mera samozaštite, uključujući zaštitu prava fizičkih lica.

5.7. Prava pristupa fizičkog lica podacima

Kada radi kao rukovalac podataka, Direktor IED je odgovoran da obezbedi licu na koje se podaci odnose pogodan mehanizam za pristup koji mu omogućava da pristupi svojim ličnim podacima i dozvoli mu da ažurira, ispravi, izbriše ili prenese svoje podatke o ličnosti, ako odgovara, ili se zahteva po ZZPL. Mehanizam za pristup fizičkih lica na koje se podaci o ličnosti odnose biće detaljnije opisan u *Proceduri za zahtev fizičkih lica za pristup podacima* (čiju formu propisuje Poverenik) i obezbeđen uz manuelnu pomoć administratora IKT sistema IED.

5.8. Prenosivost podataka o ličnosti

Na pisani zahtev lica na koje se podaci odnose, IED će besplatno dostaviti kopiju podataka koje je dobila od lica, u strukturiranom formatu, ili je preneti drugom rukovaocu. Lice za zaštitu podataka o ličnosti ili lice imenovano za poslove zaštite podataka o ličnosti će takav zahtev obraditi u roku od mesec dana od dana podnošenja pisanog zahteva, ako zahtev nije prekomeran (svakodnevan) i ako ne utiče na prava i podatke o ličnosti drugih lica.

5.9. Pravo na zaborav (brisanje podataka)

Fizičko lice na koje se podaci odnose može zahtevati brisanje svojih ličnih podataka (Čl. 30, ZZPL). Kada IED radi kao rukovalac, Lice imenovano za poslove zaštite podataka o ličnosti preduzeće neophodne akcije (uključujući i tehničke mere) da o zahtevu informiše sve treće strane koje koriste ili obrađuju podatke i u razumnom roku (15 dana) izbriše zahtevane podatke, ako ne postoje ograničenja za ispunjavanje ovog zahteva prema ZZPL.

5.10. Odgovornost i nadoknada štete

U slučaju prigovora ili nanete štete za prava i slobiode fizičkih lica, IED i klijent (dobavljač, partner) će biti odgovorni licu na koje se podaci odnose, u skladu sa ZZPL (Članovi 82 do 86, ZZPL).

6. Smernice za poštenu obradu podataka o ličnosti

Podaci o ličnosti se u IED moraju obrađivati samo kada su eksplicitno ovlašćeni od Lica imenovanog za poslove zaštite podataka u IED i odobreni od Direktora IED kao rukovaoca podataka.

IED mora da proceni i odluči da li da izvrši *Procenu uticaja obrade na zaštitu podataka* – DPIA (*Data Protection Impact Assessment)* za svaku aktivnost obrade u skladu sa smernicama (Član 54, ZZPL).

6.1. Obaveštenje o privatnosti za fizička lica

U vreme skupljanja ili pre skupljanja podataka o ličnosti za svaku vrstu radnje obrade, uključujući, ali se ne ograničavajući na davanje usluga, ili markentiške radnje, Lice imenovano za poslove zaštite podataka o ličnosti je odgovorno da propisno obavesti lica na koje se podaci odnose o sledećem: *vrsti skupljenih podataka o ličnosti, namenama obrade, metodama obrade, pravima lica na koje se podaci odnose, periodu zadržavanja, potencijalnom međunarodnom prenosu podataka, deljenju podataka sa trećim stranama i merama IED za zaštitu podataka o ličnosti.* Ove informacije se obezbeđuju za zaposlene kroz dokument *Obaveštenje o privatnosti zaposlenih*, a za klijente *Obaveštenje o privatnosti klijenata*.

Ako IED ima višestruke i različite radnje obrade i obrađuje različite vrste podataka o ličnosti, treba izraditi različita Obaveštenja o privatnosti, zavisno od vrsta obrade podataka i kategorija podataka (na primer, jedno za namenu slanja poštom, a drugo za slanje špedicijom, gde se razlikuju radnje obrade).

Ako se podaci o ličnosti dele sa trećom stranom, Lice imenovano za poslove zaštite podataka o ličnosti IED e mora osigurati da je lice na koje se podaci odnose obavešteno o tome kroz Obaveštenje o privatnosti.

Kada se lični podaci prenose u treću zemlju prema *Politici prekograničnog prenosa* i Zakonu, u Obaveštenju o privatnost treba jasno navesti državu u koju se podaci prenose i entitet kojem se podaci prenose.

6.2. Dobijanje pristanka

Kad god je obrada ličnih podataka zasnovana na pristanku fizičkog lica, ili na drugom zakonskom osnovu, Lice imenovano za poslove zaštite podataka o ličnosti u IED je odgovorno za evidentiranje i održavanje zapisa o tom pristanku, informisanje fizičkih lica, obezbeđivanje opcije za dostavljanje pristanka, i osiguranje da njihov pristanak (kad god se pristanak za

obradu daje na zakonskoj osnovi) može biti u svako vreme povučen, na osnovu pisanog zahteva.

Kada se skupljaju podaci o deci ispod 15 godina starosti, Lice imenovano za poslove zaštite podataka o ličnosti mora osigurati da roditelj (staralac) deteta, dobije *Formular za roditeljski pristanak* koji propisuje Nadzorno telo (Poverenik) (Član 16, ZZPL). Rukovalac mora preduzeti razumne mere u cilju utvrđivanja da li je pristanak dao roditelj koji vrši roditeljsko pravo, odnosno drugi zakonski zastupnik maloletnog lica, uzimajući u obzir dostupne tehnologije.

Kada se zahteva korekcija, dopuna ili uništavanje zapisa podataka o ličnosti, Lice imenovano za poslove zaštite podataka o ličnosti osiguraće da se ovi zahtevi izvrše u razumnom vremenu, registruju i čuvaju logovi zapisa o zahtevima.

Podaci o ličnosti se u IED obrađuju samo za namene za koje su originalno skupljeni. U slučaju da IED želi obrađivati podatke za drugu namenu, IED će tražiti eksplicitan pristanak od lica na koje se podaci odnose u jasnom i konciznom pisanom formatu (na primer, za marketing). Svaki takav zahtev će uključivati originalnu namenu(e) za koju su se podaci skupljali, novu ili dodatnu namenu(e) obrade, kao i razlog za promenu namene(a) obrade. Lice imenovano za poslove zaštite podataka o ličnosti u IED odgovorno je za usaglašenost sa pravilima u ovoj sekciji.

Metod skupljanja podataka o ličnosti u IED usaglašen je i biće usaglašavan ubuduće sa ZZPL o zaštiti podataka o ličnosti, dobrom praksom i standardima zaštite podataka i informacija.

Lice imenovano za poslove zaštite podataka o ličnosti je odgovorno za kreiranje i održavanje *Registra obaveštenja o privatnosti*.

7. Organizacija i odgovornosti IED

Odgovornost za osiguranje odgovarajuće obrade podataka o ličnosti je svakog ko radi za ili sa IED i ima pristup podacima o ličnosti koje IED obrađuje.

Ključne odgovornosti za obradu podataka o ličnosti u IED imaju sledeće organizacione uloge:

Direktor IED: Odobrava opštu strategiju IED i donosi odluke o skupljanju, obradi i zaštiti podataka o ličnosti klijenata u IED, radi kao rukovalac radnje obrade, određuje namenu obrade, organizuje i vodi evidenciju o radnjama obrade podataka o ličnosti u IED (Član 47(5) ZZPL)**.**

Lice za zaštitu podataka o ličnosti ili lice imenovano za poslove zaštite podataka o ličnosti: Odgovorno je za menadžment programa za zaštitu podataka o ličnosti, za razvoj i promociju politike zaštite privatnosti krajnjim korisnicima i za druge radnje definisane u opisu poslova Lica za zaštitu podataka o ličnosti (Članovi 56, 57 i 58 ZZPL);

Pravnik IED: Monitoriše i analizira zakone o zaštiti podataka o ličnosti, prati promene zakonskih regulativa, razvija zahteve za usaglašenost i pomaže sektorima Kompanije u dostizanju ciljeva *Politike zaštite privatnosti*.

IT sektor IED:

- Odgovoran je da osigura da svi sistemi, servisi i oprema koja se koristi za obradu i skladištenje podataka o ličnosti dostignu prihvatljive standarde informacione bezbednosti i zaštite podataka o ličnosti.
- Izvršava regularne provere i skeniranja da osigura da tehničke mere zaštite hardvera i softvera, i organizacione mere funkcionišu propisno.

Marketing manadžer:

- Odgovoran je za odobravanje, uz kosultaciju Direktora, svakog saopštenja o zaštiti podataka o ličnosti koje se prilaže uz komunikaciona sredstva kao što su e-mail, faks poruke i pisma.
- Odgovara na svaki upitnik o zaštiti podataka od strane novinara ili drugih medija.
- Gde je neophodno, radi sa Licem imenovanim za poslove zaštite podataka o ličnosti, da osigura marketing i da usaglasi inicijative za promociju IED sa principima zaštite podataka.

Menadžer ljudskih resursa:

- Odgovoran je za podizanje svesti svih zaposlenih o zaštiti podataka o ličnosti zaposlenih i klijenata.
- Organizuje obuku zaposlenih o zaštiti podataka o ličnosti i razvoj svesti zaposlenih koji rade sa podacima o ličnosti.
- Osigurava zaštitu podataka o ličnosti u životnom ciklusu, od trenutka prijema do arhiviranja, i da se podaci o ličnosti zaposlenih i klijenata obrađuju na osnovu legitimnih, neophodnih i poslovnih potreba zaposlenih i klijenata.

Manadžer za nabavku: Odgovoran je za prenos odgovornosti o podacima o ličnosti IED dobavljaču/partneru i poboljšanje svesti dobavljača/partnera o zaštiti podataka o ličnosti, kao i za prosleđivanje zahteva za podatke o ličnosti trećoj strani koju dobavljač/partner koristi. Organizaciona jedinica za nabavku zadržava pravo da proveri bezbednosne kapacitete dobavljača/partnera i treće strane.

Manadžer za prodaju: Odgovoran je za prenos odgovornosti za zaštitu podataka o ličnosti IED kupcu i poboljšanje svesti kupaca o zaštiti podataka o ličnosti, kao i za prosleđivanje zahteva za zaštitu podataka o ličnosti trećoj strani.

8. Smernice za uspostavljanje vodećeg nadzornog tela

8.1. Neophodnost uspostavljanja vodećeg nadzornog tela

Identifikovanje vodećeg nadzornog tela za zaštitu podataka o ličnosti (Poverenika), važno je samo ako IED vrši prekograničnu obradu ličnih podataka.

Prekogranična obrada podataka se vrši, ako *obradu ličnih podataka vrši podružnica (predstavništvo) IED sa sedištem u drugoj državi članici EU.*

8.2. Glavno sedište IED i vodeće nadzorno telo

8.2.1. Glavno sedište rukovaoca podataka o ličnosti

Direktor IED treba da identifikuje glavno sedište, koje je obično administrativno sedište uprave IED, gde se donose strateške odluke, tako da se može odrediti vodeće nadzorno telo.

8.2.2. Glavno sedište obrađivača podataka o ličnosti

Kako IED radi i kao obrađivač podataka o ličnosti, gde se vrše glavne radnje obrade, onda će glavno sedište biti mesto centralne administracije u Srbiji.

9. Odgovor na incident povrede podataka o ličnosti

Kada IED, tj. Lice imenovano za poslove zaštite podataka o ličnosti, uoči ili posumnja, ili identifikuje incident stvarne povrede ličnih podataka, mora da preduzme internu proveru, spreči širenje incidenta i zahteva blagovremene mere oporavka sistema zaštite, u skladu sa ovom *Politikom*. Gde postoji rizik, posebno visok rizik za prava i slobode lica na koja se podaci odnose, IED (tj. Lice imenovano za poslove zaštite podataka o ličnosti) će obavestiti nadležno nadzorno telo (Poverenika) i Nacionalni CERT bez odlaganja, a najkasnije u roku od 72 sata, a u najkraćem mogućem roku vlasnike podataka (do 15 dana).

10. Provera i odgovornost

IED će nastojati da proverava kvalitet implementacije ove Politike, da unapređuje tehničke, organizacione i kadrovske mere zaštite i kontrole podataka o ličnosti klijenata.
Svaki zaposleni u IED, koji obrađuje podatke o ličnosti moraju biti upoznati i obučeni o podacima o ličnosti, o sistemima kontrole i načinu prikupljanja i obrade, zakonskim propisima i odgovornostima koje proizilaze iz ZZPL. Ako zaposleni u ZZPL povredi prava i slobode lica na koje se podaci odnose, prema ovoj Politici, biće podvrgnut disciplinskim, prekršajnim ili krivičnim merama, zavisno od nanete štete poslovnom sistemu IED.

11. Obaveze dobavljača i partnera prema IED

Adekvatne tehničke i organizacione mere (Prilog 1), koje IED primenjuje za zaštitu podataka o ličnosti, podložne su tehničkom progresu i daljem razvoju. U tom smislu, IED je dozvoljeno da implementira alternativne adekvatne mere zaštite podataka o ličnosti, pri čemu nivo bezbednosti definisanih mera zaštite ne sme biti smanjen, a bitne promene moraju biti dokumentovane.

IED će u ugovoru ili SLA tražiti od klijenata (dobavljača i partnera), da primenjuju adekvatne tehničke i organizacione mere zaštite podataka o ličnost koje u ugovorima i SLA, ili aneksima ugovora i SLA, dobiju od IED:

(1) Klijent će podržati IED/Rukovaoca u ispunjavanju prava i prigovora fizičkih lica prema *Zakonu o zaštiti podataka o ličnosti* i u skladu sa ovom Politikom.

(2) Klijent će dalje podržati Kompaniju/ Rukovaoca u usaglašavanju sa obavezama koje se odnose na zaštitu podataka o ličnosti, zahteve za izveštavanje o povredama podataka o ličnosti, procenu uticaja obrade podataka na zaštitu podataka o ličnosti i na prethodne konsultacije sa nadležnim nadzornim telima, što uključuje:

a. Osiguranje odgovarajućeg nivoa zaštite podataka o ličnosti dobijenih od Kompanije, kroz adekvatne tehničke i organizacione mere zaštite koje uzimaju u obzir okolnosti i namenu obrade, procenjenu verovatnoću i intenzitet potencijalne povrede zakona i načela zaštite podataka zbog bezbednosnih ranjivosti, i omogućavaju trenutnu detekciju relevantnih događaja povreda.
b. Obavezu trenutnog izveštavanja IED o povredi podataka o ličnost.
c. Dužnost pružanja pomoći IEDE u vezi sa obavezama IED da obezbedi informacije koje se odnose na fizička lica i da trenutno dostavlja IED takve informacije.
d. Podršku IED sa procenom uticaja obrade na zaštitu podataka o ličnost.
e. Podršku IED sa prethodnom konsultacijom nadzornog otrgana.

(3) Klijent (dobavljač, partner) garantuje da će svim zaposlenim uključenim u ugovor o obradi podataka o ličnosti IED, kao i drugim takvim licima koja mogu biti uključena u Ugovor o obradi podataka sa IED, u okviru obima odgovornosti klijenta, biti zabranjeno da obrađuju podatke izvan obima obrade datog instrukcijama IED. Dalje, klijent garantuje da će svako lice koje obrađuje podatke u ime rukovaoca preduzeti mere za čuvanje tajnosti ili sprovoditi statutarnu obavezu za čuvanje tajnosti. Sve obaveze za čuvanje tajnosti treba da ostanu na snazi i po prekidu ili isteku Ugovora o obradi podataka IED.

(4) Klijent (dobavljač, partner) će blagovremeno obavestiti kontaktnu osobu u IED o svakom pitanju koje se odnosi na zaštitu podataka koji proističu iz Ugovora/Sporazuma sa IED.

(5) Ako fizička lica podnesu bilo koji zahtev protiv IED u skladu nsa Čl. 82 Zakona o zaštiti podataka o ličnosti, klijent (dobavljač, partner) će podržati IED u odbrani protiv takvih zahteva, gde je moguće i opravdano.

12. Menadžment održavanja zapisa politike

Ime zapisa	Lokacija skladištenja	Lice odgovorno za skladištenje	Kontrole za zaštitu zapisa	Vreme čuvanja
Formular pristanka vlasnika podataka	U IKT sistemu za zaštitu podataka	Lice za zaštitu podataka o ličnosti ili lice imenovano za poslove zaštite ličnih podataka	Samo ovlašćeno lice može pristupiti formularu	10 godina
Formular za povlačenje pristanka lica čiji se podaci obrađuju	U IKT sistemu za zaštitu podataka	Lice za zaštitu podataka o ličnosti ili lice imenovano za poslove zaštite ličnih podataka	Samo ovlašćeno lice može pristupiti formularu	10 godina
Formular za roditeljski pristanak	U IKT sistemu za zaštitu podataka	Lice za zaštitu podataka o ličnosti ili lice imenovano za poslove zaštite ličnih podataka	Samo ovlašćeno lice može pristupiti formularu	10 godina
Formular za povlačenje roditeljskog pristanka	U IKT sistemu za zaštitu podataka	Lice za zaštitu podataka o ličnosti ili lice imenovano za poslove zaštite ličnih podataka	Samo ovlašćeno lice može pristupiti formularu	10 godina
Ugovor o prenosu podataka o ličnostima	U IKT sistemu za zaštitu podataka	Lice za zaštitu podataka o ličnosti ili lice imenovano za poslove zaštite ličnih podataka	Samo ovlašćeno lice može pristupiti formularu	5 godina od prestanka važnosti Sorazuma
Registar obaveštenja o privatnosti	U IKT sistemu za zaštitu podataka	Lice za zaštitu podataka o ličnosti ili lice imenovano za poslove zaštite ličnih podataka	Samo ovlašćeno lice može pristupiti formularu	Permanentno

13. Validacija i menadžment dokumenta

13.1 Validaciju ove politike vrše vlasnik (staratelj) ove politike, *Lice imenovano za poslove zaštite* ***podataka o ličnosti*** i Direktor koji mora kontrolisati i proveravati primenu politike o zaštiti privatnosti, a *Lice za zaštitu podataka o ličnosti* po potrebi i ažurirati dokument najmanje jedanput godišnje.

13.2 Ova politika stupa na snagu danom potpisivanja: 01.12.2019. godine

Direktor
Prof. dr Miroslav Raićević

Prilog 1. TEHNIČKE I ORGANIZACIONE MERE ZAŠTITE RADNJE OBRADE PODATAKA O LIČNOSTI

a) Zaštita poverljivosti radnje obrade podataka o ličnosti	
Obrada podataka	*Kontrola zaštite radnje obrade*
Fizički pristup prostorijama za obradu podataka	Magnetske ili čipovane kartica, ključevi, elektronska brava, sistemi zaštite prostorija, i/ili obezbeđenje na ulazu, alarmni sistemi, video nadzor
Elektronski pristup sistemima za obradu i pohranjivanje podataka	Bezbedna lozinka, mehanizam za automatsko blokiranje/zaključavanje, dvokratna autentifikacija, šifrovanje nosača podataka/medija za pohranjivanje.
Pristup fizičkog lica za čitanja, kopiranja, izmene ili brisanja podataka u IS Kompanije	Koncept autorizacije prava pristupa fizičkog lica na koje se podaci odnose IKT sistemu Kompanije na bazi potrebe i analize rizika događaja sistemskog pristupa i davanje pristupa uz manuelnu pomoć nadministratora sistema Kompanije
Izolovana obrada podataka	Sistemi za podršku više klijenata (na primer: *Multitenat Cloud Computinfg systems*, *Sendbox* sistem etc.)
Proces obrade podataka o ličnosti	**Pseudonimizacija**: Obrada podataka o ličnosti na takav način/metod da se podaci ne mogu povezati sa specifičnim licem bez pomoći dodatnih informacija, pod uslovom da su ove informacije skladištene odvojeno i predmet su odgovarajućih tehničkih i organizacioneih mera zaštite.
a) Zaštita integriteta radnje obrade podataka o ličnosti	
Prenos podataka o ličnosti	Adekvatne tehničke mere zaštite koje uključuju šifrovanje, VPN veze, digitalni potpis za zaštitu od neovlašćenog čitanja, kopiranja i izmena ili brisanja podataka u prenosu.
Tačnosti unosa podataka o ličnosti	Kontrola logovanja i dokument menadžment sistema.
b) Zaštita raspoloživost i otpornosti ličnih podataka	
Kontrola raspoloživosti i sprečavanje slučajne ili namerne destrukcije ili gubitka podataka o ličnosti	Strategija bekapovanja (*online/offline; onsite/offsite*), UPS sitem, antivirusna zaštita, *firewwal*, procedura za izveštavanje i plan vanrednih događaja.
Brz oporavak posle incidenta	Iz sistema za bekapovanje, oporavak izbrisanih podataka alatima i tehnikama digitalne forenzike.
Organizacione mere zaštite	
c) Procedure za regularno testiranje, procenu i evaluaciju	
Menadžment zaštite privatnosti	Politika zaštite privatnosti, Registar radnje obrade
Menadžment odgovora na incident	Politika upravljanja incidentom, Procedura prvog odgovora na incident
Podrazumevana i ugrađena zaštita podataka o ličnosti	Implementirana *pseudonimizacija* i *minimizacija* vidljivosti podataka o ličnosti za implementaciju načela zaštite podataka o ličnosti, integracija neophodnih mera zaštite (ISMS, Zakon) u procese obrade. Ova kontrola se odnosi na količinu skupljanja podataka, obim obrade, period skladištenja i pristup podacima o ličnosti, Osigurati da podrazumevano podaci o ličnosti nisu dostupni fizičkim licima bez intervencije čoveka za neki neodređen broj lica koji traže pristup svojim podacima, pa je manuelna pomoć administratora neophodna.
Kontrola porudžbina, ugovora ili	Odgovarajuća instrukcija Kompanije za adekvatne tehničke i

sporazuma od rizika obrade podataka o ličnosti Kompanije kod treće strane (dobavljač, partner)	organizacione mere zaštite, jasan i nedvosmislen ugovor/sporazum, menadžement formalne porudžbine.