Advokat Jovana Diljević | Sertifikovani DPO

PRAKTIČNI VODIČ KROZ ZAŠTITU LIČNIH PODATAKA U BIH (SL. GLASNIK BIH BR. 12/25)

2025

Novi instituti i poređenje sa starim zakonodavstvom

Praktični vodič kroz zaštitu ličnih podataka u BiH (Sl. Glasnik BiH br. 12/25)

NOVI INSTITUTI I POREĐENJE SA STARIM ZAKONODAVSTVOM

Advokat Jovana Diljević | Sertifikovani DPO

SADRŽAJ

INTRO

Zakon o zaštiti ličnih podataka Bosne i Hercegovine iz 2006. godine predstavljao je prvi korak ka normiranju obrade ličnih podataka u Bosni i Hercegovini. Obzirom na ubrzani razvoj zakonodavstva u oblasti Zaštite ličnih podataka na nivou Evropske unije, te usvajanju Opšte uredbe o zaštiti podataka Evrospke unije (GDPR Uredba) iz 2019. godine, postalo je evidentno da je postojeće zakonodavstvo zastarjelo, te da ne prati evropski razvoj zakonodavstva na polju zaštite ličnih podataka.

Iz tog razloga, došlo je i do inicijative za izradu sasvim novog Zakona o zaštiti ličnih podataka u BiH, koji je usvijen 30.01.2025. godine, a koji donosi značajne promjene, pogotovo u pogledu usklađenosti zakonskog teksta za GDPR Uredbom, kao i uvođenja novih obaveza kako za kontrolore tako i za obrađivače podataka.

Zakon o zaštiti ličnih podataka u BiH ("Sl. glasnik BiH", br. 49/2006, 76/2011 i 89/2011 - ispr.) vs Zakon o zaštiti ličnih podataka u BiH („Sl. Glasnik BiH“ br. 12/2025)

Ovim priručnikom staro i novo zakonodavno rješenje uporedićemo obrađujući deset najvažnijih kategorija, da bismo na što jednostavniji i slikovitiji način prikazali ključne razlike u zakonodavstvu, a pritom i ukazali na nove obaveze svih učesnika u osjetljivoj oblasti, kao što je zaštita ličnih podataka.

1. PREDMET I SVRHA ZAKONA

- **Zakon iz 2006. godine:** Cilj ovog zakona bio je osigurati zaštitu ljudskih prava i osnovnih sloboda u pogledu obrade ličnih podataka, uz osnivanje Agencije za zaštitu ličnih podataka.
- **Zakon iz 2025. godine:** Fokus zakonodavca je širi i uključuje usklađivanje s Opštom uredbom o zaštiti podataka (GDPR) EU u svim njenim oblastima, te dodatno precizira pravila za obradu podataka u svrhe sprječavanja i gonjenja krivičnih djela.

Ključna promjena: Novi zakon eksplicitno propisuje usklađivanje s GDPR-om i dodatno se fokusira na zaštitu ličnih podataka u svim pravosudnim procesima.

Obzirom da je Agencija za zaštitu ličnih podataka osnovana Zakonom iz 2006. godine, bitno je napomenuti da je usvajanjem novog Zakona Agencija obezbijedila proširenje nadležnosti.

Prema Zakonu o zaštiti ličnih podataka iz 2025. godine, Agencija za zaštitu ličnih podataka u BiH dobila je proširene nadležnosti kako bi se osigurala efektivna primjena zakona i usklađenost sa GDPR-om a koje su podijeljene u sljedeće kategorije:

1. Nezavisnost i nadzor

- Agencija djeluje kao potpuno nezavisan nadzorni organ u izvršavanju svojih funkcija, uključujući nadzor nad primjenom odredbi zakona od strane kontrolora i obrađivača podataka;
- Zaposleni u Agenciji su zaštićeni od spoljnog uticaja i dužni su obavljati svoje zadatke u skladu sa zakonom.

2. Provođenje inspekcijskih nadzora i izricanje kazni

- Agencija ima ovlaštenje za sprovođenje inspekcijskih nadzora nad kontrolorima i obrađivačima podataka, kao i za izricanje novčanih kazni za kršenje odredbi zakona
- Primenjuje se mehanizam prisilne naplate kazni preko poreznih organa ukoliko se kazne ne uplate u predviđenom roku.

3. Međunarodna saradnja

- Agencija preduzima mjere za međunarodnu saradnju u provođenju Zakona o zaštiti ličnih podataka, što uključuje razmjenu informacija i pružanje pomoći u istragama.
- Aktivno sarađuje sa međunarodnim organizacijama radi unaprjeđenja zakonodavstva u vezi s ličnim podacima.

4. Sertifikacija i kodeksi ponašanja

- Agencija preporučuje uspostavljanje postupaka sertifikacije zaštite podataka i odobrava kodekse ponašanja za kontrolore i obrađivače podataka;
- Pravno lice koje izrađuje kodeks ponašanja mora dobiti saglasnost Agencije kako bi se osigurala usklađenost sa zakonom.

5. Rješavanje prigovora i informisanje javnosti

- Agencija je dužna postupati po prigovorima nosilaca podataka koji smatraju da su njihova prava povrijeđena, pružajući pomoć u vezi s pravnim sredstvima.
- Podnosi redovne godišnje izvještaje Parlamentarnoj skupštini BiH i čini ih dostupnim javnosti.

6. Savjetovanje i preventivne mjere

- Agencija ima pravo na prethodno savjetovanje u vezi s obradama koje mogu nositi visok rizik za prava i slobode nosilaca podataka.
- Daje preporuke za mjere zaštite u postupcima obrade podataka.

Ove proširene nadležnosti omogućavaju Agenciji da se efikasno suoči sa izazovima savremenih tehnologija i poveća nivo zaštite ličnih podataka u BiH u skladu sa evropskim standardima.

2. DEFINICIJE

- **Zakon iz 2006. godine:** Definisane su osnovne kategorije pojmova u vezi sa zaštitom ličnih podataka, poput: kontrolora, obrađivača, ličnih podataka i nosilaca podataka.
- **Zakon iz 2025. godine:** Uvedene su nove definicije poput pseudonimizacije, izrade profila, biometrijskih podataka i genetskih podataka, što je u skladu sa GDPR standardima.

Ključna promjena: Definicije su značajno proširene kako bi obuhvatile savremene izazove u obradi podataka.

Kao najvažniji iskorak novog Zakonodavstva, kada su u pitanju zakonske definicije, izdvajićemo tri ključna prava koja doprinose boljoj zaštiti nosilaca podataka i usklađenosti sa GDPR-om:

1. Pravo na brisanje („Pravo na zaborav“)

Nosilac podataka ima pravo zahtijevati od kontrolora podataka brisanje svojih ličnih podataka bez nepotrebnog odgađanja ako je ispunjen jedan od sljedećih uslova:

- Lični podaci više nisu potrebni za svrhe u koje su prikupljeni ili na drugi način obrađeni.
- Nosilac podataka je povukao saglasnost, a ne postoji drugi pravni osnov za obradu.

- Nosilac podataka je uložio prigovor na obradu podataka i ne postoje zakonski razlozi za nastavak obrade.
- Lični podaci su nezakonito obrađeni ili moraju biti obrisani radi poštovanja zakonske obaveze.

Izuzeci se primjenjuju kada je obrada podataka neophodna zbog slobode izražavanja, javnog zdravlja, istraživanja ili statistike, kao i za postavljanje, ostvarivanje ili odbranu pravnih zahtjeva.

2. Pravo na ograničenje obrade

Nosilac podataka ima pravo tražiti ograničenje obrade svojih podataka kada:

- Ospori tačnost ličnih podataka u roku dok kontrolor provjerava tačnost.
- Obrada je nezakonita, ali se nosilac protivi brisanju podataka i umjesto toga traži ograničenje njihove obrade.
- Kontroloru podataka podaci više nisu potrebni, ali ih nosilac zahtijeva radi postavljanja, ostvarivanja ili odbrane pravnih zahtjeva.

Dok je obrada ograničena, podaci se mogu obrađivati samo uz saglasnost nosioca ili za zaštitu pravnih interesa.

3. Pravo na prenosivost podataka

Nosilac podataka ima pravo preuzeti svoje lične podatke koje je dao kontroloru u strukturiranom, uobičajeno upotrebljavanom i mašinski čitljivom formatu. Takođe, nosilac ima pravo prenijeti te podatke drugom kontroloru bez ometanja od strane prvobitnog kontrolora podataka, ako je ispunjen jedan od sledećih uslova:

- Obrada je zasnovana na saglasnosti ili ugovoru.
- Obrada se vrši automatski.

Ovo pravo uključuje i direktan prenos podataka između kontrolora ako je tehnički izvodljivo.

Ove odredbe jasno usklađuju zakon sa GDPR standardima i pružaju veći stepen zaštite i kontrole nosiocima podataka.

3. NAČELA OBRADE PODATKA

- **Zakon iz 2006. godine:** Propisuje osnovna načela zakonitosti, pravičnosti i ograničenja svrhe obrade.

- **Zakon iz 2025. godine:** Dodata su načela transparentnosti, smanjenja obima podataka, tačnosti, ograničenja čuvanja i odgovornosti kontrolora.

Ključna promjena: Uvođenje načela transparentnosti i odgovornosti kontrolora.

4. PRAVA NOSILACA PODATAKA

- **Zakon iz 2006. godine:** Osnovna prava nosilaca podataka uključuju pravo na pristup i ispravku podataka.
- **Zakon iz 2025. godine:** Proširena prava uključuju pravo na brisanje („pravo na zaborav“), pravo na prenosivost podataka i pravo na ograničenje obrade.

Ključna promjena: Proširenje prava nosilaca podataka u skladu s GDPR-om.

5. SAGLASNOST ZA OBRADU PODATAKA

- **Zakon iz 2006. godine:** Obrada je dozvoljena uz saglasnost nosioca podataka koja mora biti izričita.
- **Zakon iz 2025. godine:** Saglasnost mora biti dobrovoljna, informisana i nedvosmislena, a predviđena je mogućnost njenog povlačenja.

Ključna promjena: Uvođenje strožijih standarda za davanje i povlačenje saglasnosti.

5.1 Saglasnost za obradu ličnih podataka djece

Kao ključnu novinu Zakona iz 2025. godine, izdvaja se zaštita podataka djece mlađe od 16 godina kao najosjetljivije kategorije za trgovinu ličnim podacima.

Prema novom Zakonu iz 2025. godine o zaštiti ličnih podataka u Bosni i Hercegovini, zaštita podataka djece definisana je kroz nekoliko ključnih odredbi:

1. Saglasnost roditelja

- Ako je dijete mlađe od 16 godina, obrada ličnih podataka djeteta zakonita je samo ako je saglasnost dao ili odobrio roditelj ili nosilac roditeljskog prava. Kontrolor podataka mora uložiti razumne napore da provjeri ko je u ime djeteta dao saglasnost..

2. Obrada podataka djece

- Obrada ličnih podataka djece mora biti u skladu s posebnim zaštitnim mjerama kako bi se osigurala bezbjednost i privatnost djeteta. Obrada podataka se ne smije koristiti na način koji negativno utiče na najbolje interese djeteta.

3. Transparentne informacije

- Kontrolori podataka moraju obezbijediti informacije o obradi podataka u razumljivom i lako dostupnom obliku koji je prilagođen djeci, koristeći jasan i jednostavan jezik.

4. Zaštita identiteta

- Obrada osjetljivih podataka djeteta, poput biometrijskih i zdravstvenih podataka, zahtijeva dodatne mjere zaštite kako bi se spriječile zloupotrebe ili povrede prava djeteta.

5. Zabrana automatizovanog donošenja odluka

- Automatske odluke koje imaju pravne ili slične značajne posljedice po dijete nisu dozvoljene bez posebnih mjera zaštite i saglasnosti nosioca roditeljskog prava.

Ove odredbe pokazuju značajan pomak u pravnoj regulativi, osiguravajući dodatnu zaštitu ličnih podataka djece u skladu sa GDPR standardima.

5.2 Davanje i povlačenje saglasnosti za obradu ličnih podataka

Prema novom Zakonu o zaštiti ličnih podataka iz 2025. godine, davanje i povlačenje saglasnosti za obradu podataka detaljno su uređeni kako bi se osigurala prava nosilaca podataka i usklađenost sa savremenim standardima zaštite podataka.

Da bismo na što jednostavniji način objasnili šta je to saglasnost za obradu ličnih podataka, te koje uslove ista mora ispunjavati da bi bila usklađena kako sa Zakonom tako i GDPR-om, osnovne karakteristike davanja i povlačenja saglasnosti podijelili smo u nekoliko kategorija:

Davanje saglasnosti

1. **Jasan i razumljiv način pružanja saglasnosti:**
    - Saglasnost se mora dati dobrovoljno, informisano i nedvosmisleno.
    - Ako se saglasnost daje u okviru pisanog dokumenta koji uključuje i druga pitanja, mora biti jasno odvojena i izražena jednostavnim jezikom.
2. **Obaveza kontrolora da dokaže postojanje saglasnosti:**

- Kontrolor podataka mora biti u mogućnosti da dokaže da je nosilac podataka dao saglasnost.

Povlačenje saglasnosti

1. **Jednostavnost povlačenja:**
    - Povlačenje saglasnosti mora biti jednako jednostavno kao i njeno davanje.
2. **Pravovremeno obavještavanje:**
    - Nosilac podataka mora biti informisan o pravu na povlačenje prije nego što da saglasnost.
3. **Uticaj povlačenja na obradu:**
    - Povlačenje saglasnosti ne utiče na zakonitost obrade koja je izvršena na osnovu saglasnosti prije njenog povlačenja.

Praktične implikacije/obaveze za kontrolore podataka

- Kontrolori moraju implementirati tehničke i administrativne procedure koje omogućavaju korisnicima da jednostavno daju i povuku saglasnost.
- Dokumentacija saglasnosti mora biti jasno organizovana i dostupna za nadzor.

Ove odredbe su usklađene sa GDPR-om, koji u članu 7 jasno definiše zahtjeve za saglasnost, ***uključujući dobrovoljnost, informisanost i pravo na povlačenje***. Pružaju se dodatne mjere zaštite za nosioce podataka i podstiče transparentno upravljanje saglasnostima od strane kontrolora.

6. OBRADA POSEBNIH KATEGORIJA PODATAKA

- **Zakon iz 2006. godine:** Zabranjena je obrada posebnih kategorija podataka, osim uz izričitu saglasnost ili u posebnim zakonskim okolnostima.
- **Zakon iz 2025. godine:** Proširenje izuzetaka za obradu posebnih kategorija podataka, uključujući medicinske, biometrijske i genetske podatke, uz odgovarajuće mjere zaštite.

Ključna promjena: Proširenje kategorija i uslova za zakonitu obradu.

Prema Zakonu iz 2025. godine, obrada posebnih kategorija ličnih podataka definisana je kroz striktne odredbe koje uključuju zabrane i izuzetke uz obavezu uvođenja odgovarajućih mjera zaštite. U nastavku predstavljamo osnovne karakteristike obrade posebnih kategorija ličnih podataka:

Zabrana obrade

- Obrada posebnih kategorija ličnih podataka je generalno zabranjena. Ove kategorije uključuju podatke koji otkrivaju:
    - Rasno ili etničko porijeklo
    - Politička mišljenja
    - Vjerska ili filozofska uvjerenja
    - Članstvo u sindikatu
    - Genetske i biometrijske podatke u svrhu jedinstvene identifikacije
    - Podatke o zdravlju, polnom životu ili seksualnoj orijentaciji.

Izuzeci od zabrane

Obrada je dozvoljena **samo ako su ispunjeni određeni uslovi**:

- **Saglasnost nosioca podataka:** Obrada je dozvoljena ako je nosilac podataka izričito dao saglasnost za obradu ovih podataka za jednu ili više konkretnih svrha, osim ako zakon zabranjuje obradu na osnovu saglasnosti.
- **Radno pravo i socijalna zaštita:** Obrada je neophodna za izvršavanje obaveza ili ostvarivanje posebnih prava kontrolora ili nosioca podataka u oblasti radnog prava i socijalne zaštite, pod zakonskim uslovima.
- **Zaštita životnih interesa:** Ako je obrada neophodna radi zaštite vitalnih interesa nosioca podataka ili drugog fizičkog lica kada nosilac nije u mogućnosti dati saglasnost.
- **Legitimne aktivnosti neprofitnih organizacija:** Obrada u okviru zakonitih aktivnosti fondacija, udruženja ili neprofitnih organizacija s političkim, filozofskim, vjerskim ili sindikalnim ciljevima, pod uslovom da se podaci ne otkrivaju izvan organizacije.
- **Javni interes i zdravstvo:** Obrada je dozvoljena u svrhe javnog zdravlja, preventivne medicine ili medicinske dijagnostike, pod uslovima koji uključuju zaštitu profesionalne tajne.

- **Objava od strane nosioca:** Ako je nosilac podataka očigledno učinio podatke javnim.
- **Pravni zahtjevi:** Obrada je dozvoljena za potrebe uspostavljanja, ostvarivanja ili odbrane pravnih zahtjeva.

Zaštitne mjere

Za sve dozvoljene obrade posebnih kategorija podataka, zakon propisuje obavezno uvođenje odgovarajućih zaštitnih mjera, uključujući pseudonimizaciju, ograničenje pristupa i tehničku zaštitu podataka.

Ovaj pristup jasno je usklađen sa GDPR standardima, osiguravajući stroge mjere zaštite prava nosilaca podataka i minimizaciju rizika prilikom obrade posebno osjetljivih podataka.

7. OBAVEZE KONTROLORA I OBRAĐIVAČA (PROCESORA) PODATAKA

- **Zakon iz 2006. godine:** Osnovne obaveze uključuju čuvanje podataka i sigurnost obrade.
- **Zakon iz 2025. godine:** Uvedene su nove obaveze, poput provođenja procjene uticaja na zaštitu podataka i imenovanja službenika za zaštitu podataka.

Ključna promjena: Proširenje obaveza u skladu sa GDPR standardima.

7.1 OBAVEZE KONTROLORA I OBRAĐIVAČA PODATAKA PREMA NOVOM ZAKONU

Nove obaveze kontrolora i obrađivača podataka koje su uvedene Zakonom iz 2025. godine u odnosu na Zakon iz 2006. godine uključuju sledeće ključne izmjene:

1. Imenovanje službenika za zaštitu podataka

- **Nova obaveza:** Kontrolori i obrađivači podataka koji obrađuju osjetljive ili velike količine podataka dužni su imenovati službenika za zaštitu podataka (Data Protection Officer - DPO).
- **Racionalizacija:** Cilj je da Službenik/DPO obezbijedi poštovanje propisa i zaštitu podataka u pravnom licu/organizaciji.

2. Provođenje procjene uticaja na zaštitu podataka (DPIA)

- **Nova obaveza:** Kontrolori podataka moraju provoditi procjenu uticaja na zaštitu podataka kada obrada može predstavljati visok rizik za prava i slobode pojedinaca.

- **Racionalizacija:** Ovaj zahtev omogućava identifikaciju i minimizaciju rizika prije početka obrade podataka.

U pogledu nove obaveze kontrolora a koja se odnosi na provođenje procjene uticaja na zaštitu podataka (DPIA) možemo reći da je ista detaljno uređena u skladu s GDPR-om i sadrži ključne odredbe za identifikaciju i minimizaciju rizika povezanih s obradom podataka.

U nastavku su ključni faktori vezani uz Provođenje procjene uticaja na zaštitu podataka (DPIA):

Obaveza sprovođenja DPIA

Kontrolor podataka mora izvršiti procjenu uticaja na zaštitu podataka prije obrade ako se očekuje visok rizik za prava i slobode fizičkih lica, posebno ako:

- se provodi sistematska i obimna procjena ličnih aspekata putem automatizovane obrade (uključujući profilisanje) koja može imati pravne ili značajne posljedice po nosioca podataka.
- Obrada uključuje velike količine posebnih kategorija ličnih podataka (poput zdravstvenih ili biometrijskih podataka) ili podataka o krivičnim presudama.
- Dolazi do sistematskog praćenja javno dostupnih područja u velikoj mjeri.

Elementi procjene uticaja

DPIA mora obuhvatiti najmanje:

- Sistematski opis predviđenih postupaka obrade i njihovih svrha.
- Procjenu nužnosti i proporcionalnosti obrade u odnosu na svrhe.
- Analizu rizika za prava i slobode nosilaca podataka.
- Predviđene mjere za rješavanje rizika, uključujući zaštitne i sigurnosne mjere te mehanizme za dokazivanje usklađenosti sa zakonom.

Uloga Agencije u sprovođenju i implementaciji DPIA rezultata

Agencija za zaštitu ličnih podataka ima ključnu ulogu u nadzoru sprovođenja DPIA:

- Uspostavlja i javno objavljuje spisak vrsta postupaka obrade koji zahtijevaju obavezno sprovođenje DPIA.
- Može uspostaviti spisak postupaka obrade za koje procjena nije potrebna.

- Kontrolori podataka dužni su se savjetovati s Agencijom ako procjena pokaže visok rizik za prava i slobode pojedinaca, a kontrolor ne preduzme mjere za ublažavanje rizika.

Prethodno savjetovanje

Ako procjena uticaja pokaže visok rizik, kontrolor podataka mora se savjetovati sa Agencijom prije početka obrade kako bi dobio smjernice o eventualnim dodatnim mjerama koje treba sprovesti.

Usklađenost s GDPR-om

Ove odredbe direktno odražavaju član 35 GDPR-a i pružaju snažan okvir za minimizaciju rizika u obradi ličnih podataka, uz transparentnost i obaveznu saradnju s nadzornim organom.

Koncept DPIA (Data Protection Impact Assessment) izvještaja sastoji se od nekoliko ključnih elemenata koji omogućavaju kontroloru podataka da procijeni i maksimalno umanji rizike u vezi s obradom ličnih podataka. Prema Zakonu iz 2025. godine i GDPR-u, DPIA je strukturisan na sledeći način:

Ključne komponente DPIA izvještaja

1. **Opis obrade i njenih svrha**
    - Objašnjenje tipova podataka koji će biti obrađeni.
    - Svrha obrade, uključujući ciljeve i koristi za organizaciju.
    - Kategorije nosilaca podataka (zaposleni, korisnici usluga, maloljetna lica).
    - Planirani rokovi za čuvanje podataka.
2. **Procjena nužnosti i proporcionalnosti obrade**
    - Pravna osnova za obradu podataka.
    - Objašnjenje zašto su podaci potrebni za ostvarenje definisanih svrha.
    - Analiza proporcionalnosti mjera zaštite u odnosu na svrhe obrade.
3. **Identifikacija i analiza rizika**

- Potencijalni rizici za prava i slobode nosilaca podataka, poput:
  - Neovlašćenog pristupa podacima.
  - Gubitka ili uništenja podataka.
  - Profilisanja ili donošenja automatizovanih odluka.
- Procjena vjerovatnoće i ozbiljnosti rizika.

4. **Mjere za smanjenje rizika**
   - Tehničke mjere (šifrovanje, pseudonimizacija, sigurnosne kopije).
   - Organizacione mjere (obuke zaposlenih, ograničenje pristupa).
   - Postavljanje jasnih procedura za postupanje u slučaju povrede podataka.
5. **Zaključak i preporuke**

3. Transparentnost i komunikacija s nosiocima podataka

- **Nova obaveza:** Kontrolori moraju pružiti jasne, sažete i lako dostupne informacije nosiocima podataka o svrsi i obimu obrade, pravnim osnovama, pravima nosilaca podataka i mogućnosti prigovora.
- **Racionalizacija:** Ovaj zahtev je dio obaveze transparentnosti prema GDPR-u.

4. Obezbeđenje prava na prenosivost podataka

- **Nova obaveza:** Kontrolori su dužni omogućiti nosiocima podataka preuzimanje svojih podataka u strukturisanom i mašinski čitljivom formatu.
- **Racionalizacija:** Omogućava lakše prebacivanje podataka između pružalaca usluga.

5. Prijava povrede ličnih podataka

- **Nova obaveza:** Kontrolori su dužni prijaviti povrede ličnih podataka Agenciji za zaštitu ličnih podataka u roku od 72 sata od otkrivanja povrede.
- **Racionalizacija:** Brzo reagovanje smanjuje potencijalnu štetu nosiocima podataka.

6. Izrada i sprovođenje tehničkih i organizacionih mjera zaštite

- **Nova obaveza:** Kontrolori i obrađivači moraju primijeniti odgovarajuće tehničke i organizacione mjere kako bi osigurali sigurnost podataka, uključujući enkripciju i pseudonimizaciju.

- **Racionalizacija:** Jačanje sigurnosnih mjera smanjuje rizik od zloupotrebe podataka.

7. Odgovornost i dokumentovanje usklađenosti

- **Nova obaveza:** Kontrolori moraju voditi evidenciju o obradi podataka i biti sposobni dokazati usklađenost sa zakonom (princip odgovornosti).
- **Racionalizacija:** Dokumentacija pomaže Agenciji u provjeri usklađenosti i olakšava interne procese.

Takođe, kao novinu u obavezama kontrolora i obrađivača podataka bitno je istaknuti obavezu odogovornosti za dokumentovanje podataka.

Prema Zakonu iz 2025. godine, odgovornost i dokumentovanje usklađenosti sa zakonodavstvom postavljaju se kao ključni principi koji dodatno jačaju povjerenje u obradu ličnih podataka. Zbog važnosti ovog pitanja u nastavku predstavljamo detaljni pregled ovog pitanja prema sljedećim kategorijama:

7.2 OBAVEZA DOKUMENTOVANJA PODATKA

1. Odgovornost kontrolora podataka

Kontrolor podataka je obavezan:

- Primijeniti odgovarajuće tehničke i organizacione mjere kako bi obezbijedio usklađenost s odredbama zakona i mogao dokazati tu usklađenost.
- Po potrebi, te mjere se moraju preispitati i ažurirati kako bi ostale u skladu s najboljim praksama.
- Poštovanje odobrenih kodeksa ponašanja ili sertifikacionih mehanizama može služiti kao dokaz za dosljednu primjenu zakonskih obaveza.

2. Dokumentovanje usklađenosti

Kontrolor i obrađivač podataka dužni su voditi evidenciju o aktivnostima obrade, koja mora sadržavati najmanje:

- Identifikaciju kontrolora i obrađivača.
- Svrhu obrade.
- Kategorije podataka i nosilaca podataka.
- Prenos podataka trećim stranama i zaštitne mjere.

3. Praćenje i provjera

Kontrolori su obavezni provoditi redovne interne provjere i usklađivanje aktivnosti obrade podataka sa zakonom, uključujući tehničke mjere kao što su pseudonimizacija i šifrovanje podataka.

4. Odgovornost obrađivača podataka

- Obrađivači podataka su obavezni da pomažu kontrolorima u ispunjavanju njihovih obaveza, uključujući odgovore na zahtjeve nosilaca podataka.
- Po završetku pružanja usluga, obrađivač mora obrisati ili vratiti kontroloru sve podatke osim ako postoji zakonska obaveza čuvanja.

5. Odgovornost za štetu

Ako obrada ličnih podataka prouzrokuje štetu nosiocu podataka, kontrolor i obrađivač snose odgovornost. Kontrolor može biti oslobođen odgovornosti ako dokaže da nije odgovoran za događaj koji je doveo do nastanka štete.

Usklađenost s GDPR-om

Ovi principi direktno odražavaju član 5 i član 24 GDPR-a, koji propisuju obavezu kontrolora podataka da osigura usklađenost sa zakonodavstvom i omogući dokazivanje te usklađenosti kroz dokumentaciju i praćenje procedura.

Ovaj okvir iz novog Zakona doprinosi jačanju odgovornosti i transparentnosti u zaštiti ličnih podataka, osiguravajući efikasnije upravljanje rizicima i poštovanje prava nosilaca podataka.

8. Kodeksi ponašanja i certifikacija

- **Nova obaveza:** Podstiče se usvajanje kodeksa ponašanja i učestvovanje u programima sertifikacije kako bi kontrolori i obrađivači pokazali usklađenost sa zakonskim zahtjevima.

Ove promjene značajno povećavaju odgovornost i obaveze kontrolora i obrađivača podataka, postavljajući strože standarde koji su u skladu s GDPR-om.

7.3 BANKE KAO POSEBNE KATEGORIJE KONTROLORA PODATAKA

Prema Nacrtu zakona iz 2025. godine, banke kao kontrolori i obrađivači ličnih podataka imaju niz specifičnih obaveza koje uključuju tehničke, organizacione i proceduralne mjere zaštite podataka kako bi bile u skladu sa zakonskim zahtjevima i GDPR-om:

1. Primjena tehničkih i organizacionih mjera

Banke su obavezne da uvedu tehničke i organizacione mjere kako bi osigurale zaštitu ličnih podataka, uzimajući u obzir prirodu, obim i svrhu obrade, kao i rizike za prava i slobode pojedinaca:

- Primjena šifriranja podataka.
- Pseudonimizacija ličnih podataka.
- Redovne sigurnosne provjere i ažuriranja sistema za zaštitu podataka.

2. Upravljanje saglasnošću nosilaca podataka

- Banke moraju osigurati da lični podaci budu obrađeni samo uz izričitu saglasnost nosioca podataka ili na osnovu zakonskih osnova predviđenih zakonom.
- Posebna pažnja se posvećuje osjetljivim podacima, uključujući biometrijske i finansijske informacije.

3. Evidencija aktivnosti obrade

- Banke su dužne voditi evidenciju svih aktivnosti obrade podataka, uključujući svrhe obrade, kategorije podataka, primaoce i eventualne prenose podataka u treće zemlje.
- Ova evidencija mora biti dostupna Agenciji za zaštitu ličnih podataka na zahtjev.

4. Obaveza obavještavanja o povredi podataka

- Banke su dužne da prijave povredu sigurnosti podataka Agenciji za zaštitu ličnih podataka u roku od 72 sata od saznanja o incidentu.
- Ako povreda može imati ozbiljne posljedice po nosioce podataka, banke su dužne da obavijeste i same nosioce podataka.

5. Prenos podataka u treće zemlje

- Banke mogu vršiti prenos podataka izvan Bosne i Hercegovine samo ako su ispunjeni strogi uslovi zaštite podataka, uključujući odgovarajuće pravne osnove i tehničke mjere zaštite.

6. Imenovanje službenika za zaštitu podataka

- Banke koje obrađuju velike količine ličnih podataka ili osjetljive podatke dužne su imenovati službenika za zaštitu podataka (DPO) koji će nadzirati usklađenost sa zakonom.

Usklađenost sa GDPR-om

Navedene obaveze direktno su u skladu s GDPR-om koji zahtijeva:

- Dokumentovanje obrade podataka (član 30 GDPR-a).
- Provođenje procjena uticaja na zaštitu podataka (član 35 GDPR-a).
- Osiguranje tehničke i organizacione mjere zaštite podataka (član 32 GDPR-a).
- Obavezu obavještavanja o povredi podataka (član 33 GDPR-a).
- Imenovanje službenika za zaštitu podataka (član 37 GDPR-a).

Ove mjere osiguravaju da banke preuzmu veću odgovornost za obradu podataka i zaštitu privatnosti svojih klijenata u skladu sa savremenim zakonskim i tehnološkim zahtjevima.

8. SLUŽBENIK ZA ZAŠTITU LIČNIH PODATAKA (DATA PROTECTION OFFICER – DPO)

Prema novom Zakonu iz 2025. godine i u skladu s GDPR-om, imenovanje službenika za zaštitu ličnih podataka (Data Protection Officer - DPO) je obavezno pod određenim uslovima, a definisani su kriterijumi za njihovu kvalifikaciju, dužnosti i nezavisnost.

8.1 IMENOVANJE DPO-A, KVALIFIKACIJE I DUŽNOSTI

1. Obaveza imenovanja DPO-a

Prema zakonu, DPO mora biti imenovan kada:

- Obrada uključuje redovno i sistematsko praćenje nosilaca podataka u velikom obimu.
- Obrada obuhvata posebne kategorije ličnih podataka, uključujući biometrijske i genetske podatke.
- Obradu vrši javni organ ili tijelo.

2. Kvalifikacije DPO-a

- Lice mora imati stručno znanje o zakonodavstvu i praksi zaštite podataka, kao i sposobnost da savjetuje kontrolore i obrađivače u vezi sa zakonskim obavezama.
- Potrebne su kompetencije u vezi s procjenom rizika i sprovođenjem sigurnosnih mjera.

3. Dužnosti DPO-a

DPO je odgovoran za:

- Informisanje i savjetovanje kontrolora, obrađivača i zaposlenih o njihovim obavezama prema zakonu.
- Praćenje usklađenosti s odredbama zakona i politikama zaštite podataka.
- Pružanje savjeta u vezi s procjenama uticaja na zaštitu podataka (DPIA).
- Saradnju s Agencijom za zaštitu ličnih podataka i posredovanje između Agencije i kontrolora podataka.

4. Nezavisnost DPO-a

- DPO mora djelovati nezavisno i ne smije biti razriješen ili kažnjen/sankcionisan zbog obavljanja svojih dužnosti.
- Direktna nezavisnost od izvršnog menadžmenta organizacije omogućava mu neometan rad.

Usklađenost sa GDPR-om

Ovi zahtjevi direktno su usklađeni s GDPR-om, koji u članu 37 propisuje obavezno imenovanje DPO-a pod istim uslovima, dok član 38 definiše njegovu nezavisnost i zaštitu od sankcija. Propisi iz novog zakona obezbjeđuju strogu usklađenost sa evropskim standardima i dodatno jačaju institucionalne kapacitete za zaštitu ličnih podataka.

8.2 KODEKS I SERTIFIKACIJA

Angažman DPO-a uključuje i pripremu kodeksa ponašanja kao i sertifikacije.

Prema Zakonu iz 2025. godine, kodeks ponašanja i sertifikacija definisani su kao ključni mehanizmi za povećanje usklađenosti sa zakonom i obezbeđivanje povjerenja javnosti u obradu ličnih podataka.

Kodeks ponašanja

Kodeksi ponašanja omogućavaju prilagođavanje zakonskih pravila specifičnostima različitih sektora. Prema Zakonu iz 2025. godine, kodeks ponašanja može obuhvatiti sledeće aspekte:

- Pravična i transparentna obrada podataka.
- Informisanje nosilaca podataka i zaštitu djece.
- Pseudonimizaciju i druge sigurnosne mjere za obradu podataka.
- Informisanje javnosti o pravima i postupanju s podacima.
- Postupke u vezi sa prijenosom podataka trećim zemljama i međunarodnim organizacijama.

Postupak izrade i odobravanja kodeksa

- Udruženja i subjekti koji predstavljaju kontrolore i obrađivače podataka mogu izraditi ili modifikovati kodeks ponašanja.

- Agencija za zaštitu ličnih podataka odobrava nacrt kodeksa ponašanja nakon što utvrdi da obezbjeđuje odgovarajuće zaštitne mjere.
- Nakon odobrenja, kodeks se registruje i objavljuje.

Praćenje primjene kodeksa ponašanja

- Agencija akredituje pravna lica koja prate usklađenost sa kodeksom ponašanja.
- Ta pravna lica moraju dokazati svoju nezavisnost i stručnost, uspostaviti postupke za ocjenu kontrolora i obrađivača te imati mehanizme za rješavanje prigovora.

Sertifikacija

Sertifikacija se uvodi kao dodatni mehanizam za dokazivanje usklađenosti sa zakonom:

- Postupak sertifikacije zaštite ličnih podataka je dobrovoljan i otvoren za kontrolore i obrađivače podataka.
- Sertifikaciona tijela, koja akredituje Agencija, provode sertifikaciju i imaju obavezu prijavljivanja izdatih i obnovljenih sertifikata Agenciji.

Postupak i trajanje sertifikacije

- Sertifikacija se izdaje na period do tri godine, uz mogućnost obnove pod istim uslovima.
- Kontrolor podataka ili obrađivač mora omogućiti pristup svim relevantnim informacijama kako bi sertifikaciono tijelo sprovelo postupak.

Oduzimanje sertifikata

- Ako se ne ispune zahtjevi sertifikacije ili dođe do kršenja, sertifikaciono tijelo ili Agencija imaju pravo oduzeti sertifikat.

Usklađenost sa GDPR-om

Navedeni mehanizmi kodeksa ponašanja i sertifikacije direktno su usklađeni s GDPR-om:

- Članovi 40 i 41 GDPR-a propisuju izradu kodeksa ponašanja za olakšanje usklađenosti sa zakonodavstvom i promovisanje dobre prakse.
- Član 42 GDPR-a definiše sertifikaciju kao mehanizam kojim kontrolori i obrađivači dokazuju usklađenost sa zakonskim zahtjevima.

Ovi mehanizmi jačaju povjerenje javnosti u postupke obrade ličnih podataka i omogućavaju fleksibilno sprovođenje zakonskih odredbi kroz prilagođene kodekse i sertifikacione standarde.

8.3 DOKUMENTACIJA KODEKSA

Dokumentacija koja čini kodeks zaštite ličnih podataka obuhvata sljedeće dokumente:

1. Politika privatnosti

- Precizan i transparentan dokument koji opisuje način prikupljanja, obrade, čuvanja i dijeljenja ličnih podataka.
- Mora uključivati:
    - Svrhe obrade podataka.
    - Prava nosilaca podataka.
    - Informacije o prenosu podataka trećim stranama ili u treće zemlje.
    - Kontakt informacije službenika za zaštitu podataka (DPO), ako postoji.

2. Ugovori sa obrađivačima podataka (Data Processing Agreements - DPA)

- Pravni dokument između kontrolora i obrađivača koji definiše:
    - Svrhu i način obrade podataka.
    - Tehničke i organizacione mjere zaštite podataka.
    - Obaveze obrađivača, uključujući prijavu povrede podataka.
    - Procedure povrata ili brisanja podataka nakon završetka usluge.

3. Saglasnost za obradu ličnih podataka

- Dokument kojim korisnik eksplicitno daje saglasnost za obradu svojih podataka.
- Mora biti:
    - Jasno definisan i lako razumljiv.
    - Dobrovoljan, informisan i konkretan.
    - Sa mogućnošću povlačenja saglasnosti.

4. Interna politika za zaštitu ličnih podataka

- Dokument koji definiše interne procedure za obradu podataka u skladu sa zakonom.
- Treba da sadrži:
    - Pravila za prikupljanje, čuvanje i brisanje podataka.
    - Procedure za prijavu povrede podataka.
    - Smjernice za obuku zaposlenih.

5. Evidencija aktivnosti obrade (Records of Processing Activities - ROPA)

- Obavezna dokumentacija koja uključuje:
    - Kategorije podataka.
    - Svrhe obrade.
    - Kategorije nosilaca podataka i primalaca.
    - Rokove za čuvanje podataka.
    - Opis tehničkih i organizacionih mjera zaštite podataka.

6. DPIA izvještaj (Procjena uticaja na zaštitu podataka)

- Obavezan za aktivnosti obrade koje nose visok rizik za prava i slobode nosilaca podataka.
- Mora sadržavati procjenu rizika i predložene mjere za smanjenje tih rizika.

7. Ugovori o povjerljivosti (Non-Disclosure Agreements - NDA)

- Ugovori za zaposlene i partnere koji regulišu povjerljivost informacija, uključujući lične podatke.

8. Plan postupanja u slučaju povrede podataka (Incident Response Plan)

- Dokument koji definiše korake za prijavu i upravljanje povredama podataka, uključujući komunikaciju sa nadležnim organima i nosiocima podataka.

9. Politika pristupa podacima

- Dokument koji definiše ko ima pravo pristupa ličnim podacima i na koji način se taj pristup kontroliše.

10. Kodeks ponašanja ili sertifikacioni dokument (opciono)

- Dokument kojim firma dokazuje usklađenost s GDPR-om i zakonskim propisima putem odobrenih kodeksa ponašanja ili sertifikacija.

9. PRENOS LIČNIH PODATAKA U TREĆE ZEMLJE

- **Zakon iz 2006. godine:** Minimalne odredbe o prenosu podataka izvan BiH.
- **Zakon iz 2025. godine:** Detaljno regulisan prenos podataka, uz obavezu primjene odgovarajućih zaštitnih mjera.

Ključna promjena: Strožiji uslovi za prenos podataka izvan zemlje.

Prema Zakonu iz 2025. godine, definicija i uslovi za prenos ličnih podataka u treće zemlje precizno su uređeni u skladu sa GDPR-om, sa fokusom na obezbeđenje odgovarajuće zaštite podataka.

1. Opšta načela prenosa podataka

Prenos ličnih podataka u drugu državu ili međunarodnu organizaciju može se vršiti samo pod sledećim uslovima:

- Država ili međunarodna organizacija mora obezbjediti adekvatan nivo zaštite ličnih podataka.
- Prenos podataka mora biti u skladu s odredbama zakona i uključivati dalji prenos podataka pod istim uslovima.

2. Prenos na osnovu adekvatnog nivoa zaštite

- Prenos je dozvoljen ukoliko je potvrđeno da država, dio njene teritorije ili određeni sektor u toj državi, ili međunarodna organizacija, osigurava adekvatan nivo zaštite ličnih podataka.
- Odluku o adekvatnosti nivoa zaštite donosi Vijeće ministara Bosne i Hercegovine na prijedlog Agencije za zaštitu ličnih podataka.

3. Prenos na osnovu odgovarajućih zaštitnih mjera

- Ako ne postoji odluka o adekvatnosti, prenos se može izvršiti ukoliko postoje pravno obavezujuće zaštitne mjere.
- Te mjere uključuju sporazume između kontrolora ili obrađivača podataka u Bosni i Hercegovini i trećih zemalja ili međunarodnih organizacija.

4. Odstupanja u posebnim slučajevima

Prenos podataka može se izuzetno izvršiti bez odluke o adekvatnosti ili odgovarajućih zaštitnih mjera ako je ispunjen jedan od sledećih uslova:

- Postoji izričita saglasnost nosioca podataka nakon što je upoznat sa rizicima prenosa.
- Prenos je neophodan za izvršenje ugovora ili pravne zahtjeve.
- Prenos je od vitalnog značaja za zaštitu životnih interesa nosioca podataka.
- Prenos je neophodan zbog važnih razloga javnog interesa ili sprečavanja ozbiljnih prijetnji javnoj sigurnosti.

5. Uloga Agencije za zaštitu ličnih podataka

Agencija ima ključnu ulogu u:

- Davanju preporuka o adekvatnosti nivoa zaštite.
- Nadgledanju prenosa i sprovođenju odgovarajućih zaštitnih mjera.
- Utvrđivanju lista država i organizacija koje ne ispunjavaju kriterijume adekvatne zaštite.

Ove odredbe predstavljaju značajan napredak u regulaciji međunarodnog prenosa podataka u skladu sa GDPR-om, garantujući visok nivo zaštite ličnih podataka i transparentnost procedura.

10. KAZNENE ODREDBE

- **Zakon iz 2006. godine:** Relativno niske kazne za prekršaje.
- **Zakon iz 2025. godine:** Značajno povećanje kazni koje mogu dosegnuti maksimalne pragove, slično GDPR-u.

Ključna promjena: Uvođenje visokih kazni kao instrumenata obezbjeđenja dosljedne primjene Zakona.

Prema Zakona iz 2025. godine, kaznene odredbe su značajno proširene kako bi se povećala odgovornost kontrolora i obrađivača podataka te osigurala stroga primjena zakona u skladu s evropskim standardima.

1. Vrste kazni

Novi zakon predviđa različite vrste kazni, uključujući:

- **Upravne novčane kazne:** Izriču se za teža kršenja zakonskih odredbi, pri čemu iznosi variraju u zavisnosti od prirode i težine povrede.
- **Krivične sankcije:** Krivični zakoni propisuju kazne za protivpravnu obradu podataka u slučaju grubih povreda odredbi zakona.
- **Kazne za kontrolore i obrađivače:** Propisane su posebne kazne za odgovorna lica unutar organizacija koje ne primjenjuju zakonske odredbe.

2. Izračunavanje visine novčanih kazni

Visina novčanih kazni zavisi od:

- **Težine povrede:** Kršenje osnovnih principa obrade podataka, prava nosilaca podataka ili neispunjavanje obaveza u vezi s prenosom podataka trećim zemljama.
- **Prirode obrade:** Posebna pažnja posvećena je obradama koje uključuju osjetljive podatke ili profilisanje.
- **Usklađenosti:** Prilikom izricanja kazne uzima se u obzir da li je kontrolor prethodno preduzeo mjere za postizanje usklađenosti.

3. Oslobađanje i umanjenje kazni

Zakon predviđa mogućnost oslobađanja ili umanjenja kazni ako:

- Kontrolor dokaže da je povreda nastala zbog vanrednih okolnosti.
- Kontrolor pokaže da je preduzeo sve razumne mjere za sprječavanje povrede.
- Kazna bi izazvala značajne ekonomske poteškoće za subjekat, pri čemu je moguće izvršenje kazne u više manjih dijelova.

4. Uloga Agencije za zaštitu ličnih podataka

- Agencija ima pravo izricanja upravnih kazni i nadzora nad njihovom naplatom.
- Može odlučiti o postepenoj naplati kazni kako bi izbjegla negativne ekonomske posljedice po kontrolora.

Usklađenost sa GDPR-om

Ove kaznene odredbe su usklađene s GDPR-om koji predviđa visoke kazne u iznosu do 20 miliona eura ili 4% ukupnog godišnjeg prihoda za ozbiljna kršenja (kao što je predviđeno I novim Zakonom iz 2025. godine). Norme novog zakona postavljaju stroga pravila i visoke kazne kao sredstvo odvraćanja i osiguravaju da kontrolori i obrađivači podataka ozbiljno pristupe zaštiti ličnih podataka.

ZAKLJUČAK

Ovaj Priručnik služi svim zainteresovanim fizičkim i pravnim licima, kao i svim kontrolorima i obrađivačima podataka, da se na što jednostavniji i slikovitiji način upute u najvažnije novine i institute novog Zakona o zaštiti ličnih podataka u BiH. Takođe, isti predstavlja objedinjeni komparativni prikaz starog i novog zakonodavnog rješenja u polju Zaštite ličnih podataka, kao i njegovu usklađenost sa GDPR Uredbom.

Mart 2025

Jovana Diljević, advokat